



**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# Adapting to GNSS Signal Interference - Challenges and Opportunities

[Prof. Zahidul Bhuiyan](#)

**Finnish Geospatial Research Institute**

Keynote@NKG Summer School

August 28, 2025, Tartu, Estonia

# Speaker Introduction



Prof. Zahidul Bhuiyan

## Current Professional Roles

- ⇒ **Full Professor** – Finnish Geospatial Research Institute
- ⇒ **Group Leader** – Resilient PNT, FGI-NLS
- ⇒ **Technical Expert** – European Commission
- ⇒ **Adjunct Professor (Satellite and Radio Navigation)** – Tampere University
- ⇒ **Editorial board member**, GPS Solutions
- ⇒ **Member** – EU Workgroups:
  - *Galileo High Accuracy and Authentication*
  - *European GNSS Interference Task Force*

## Key Skills

- ⇒ **Resilient PNT** (Positioning, Navigation, and Timing)
- ⇒ **LEO-PNT** user receiver development
- ⇒ **GNSS** Technologies
- ⇒ **Cross-domain experience**: **Road, Aviation, Maritime, and Mass-market**

Keynote @NKG Summer School,  
9:15 – 10:45; August 28, 2025, Tartu, Estonia

# 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
- 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
  - => regional conflicts to protect critical infrastructures/air space from unauthorized entities**

# Understanding GNSS Vulnerabilities

- **GNSS is working as designed:** The system continues to function correctly and deliver accurate data under normal conditions.
- **The degradation in performance is not a failure of GNSS itself,** but a consequence of external, intentional interference in specific regions.
- **Civilian GNSS signals were not designed to resist hostile threats,** causing service degradation in conflict areas.
- **During conflict situations,** the consequence is compromised availability of GNSS services for civilians in affected areas.



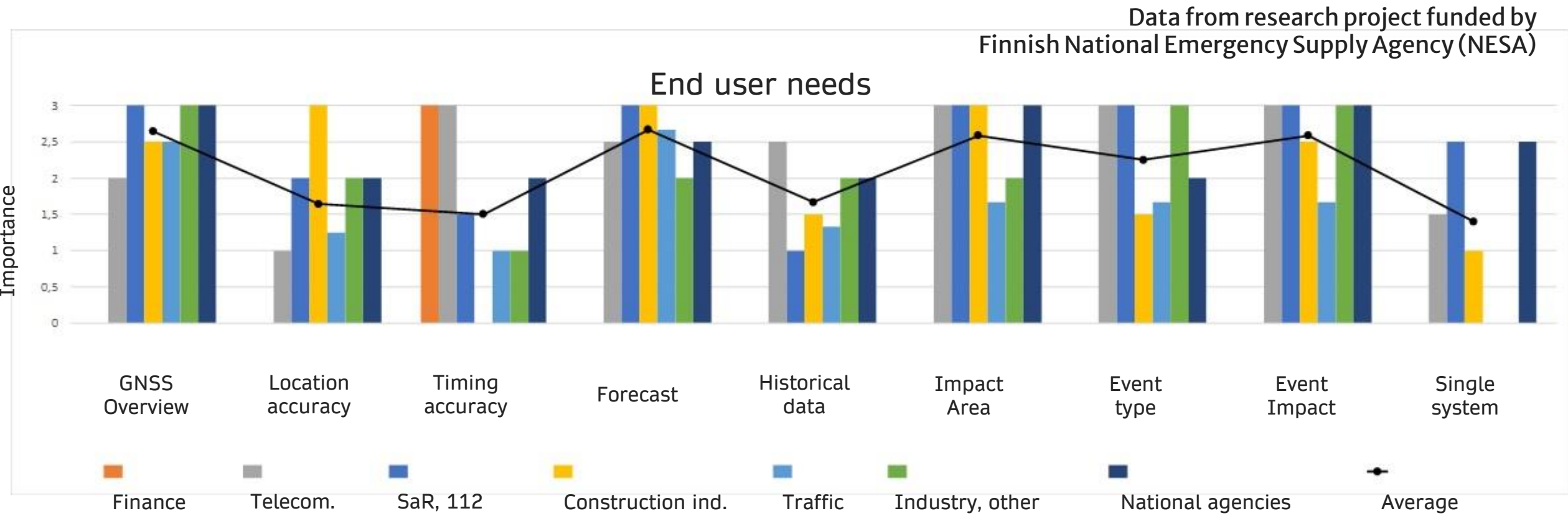
# GNSS Performance Requirements for Different Industries



Investigation  
of GNSS end  
user needs  
and  
requirements  
funded by  
NESAs 2021

Industry	Users	Positioning	Timing
Telecom	Telecom providers, data transfer	-	100 ns - 1 $\mu$ s
Finance	Banks, stock exchange	-	100 ns - 1 $\mu$ s
Electricity	Digital electricity stations	-	1 $\mu$ s
Aviation	Civil aviation	$\sim$ 1 m	-
Maritime	Shipping industry	1 - 10 m	2 s
Road users	Navigation, autonomous driving	10 cm - 1 m	-
Rail roads	Civil transportation, rail transport	1 - 10 m	-
Agriculture	Precision agriculture, forestry	1 cm - 1 m	-
Construction	Construction sites	1 cm - 1 m	-

# Increasing Need for Auxiliary Information

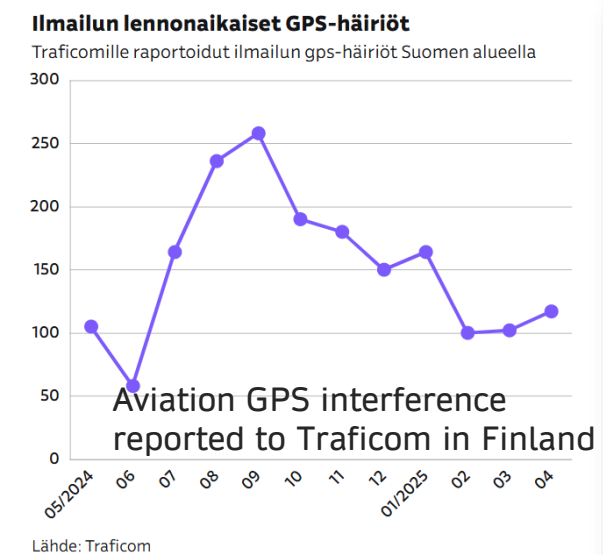
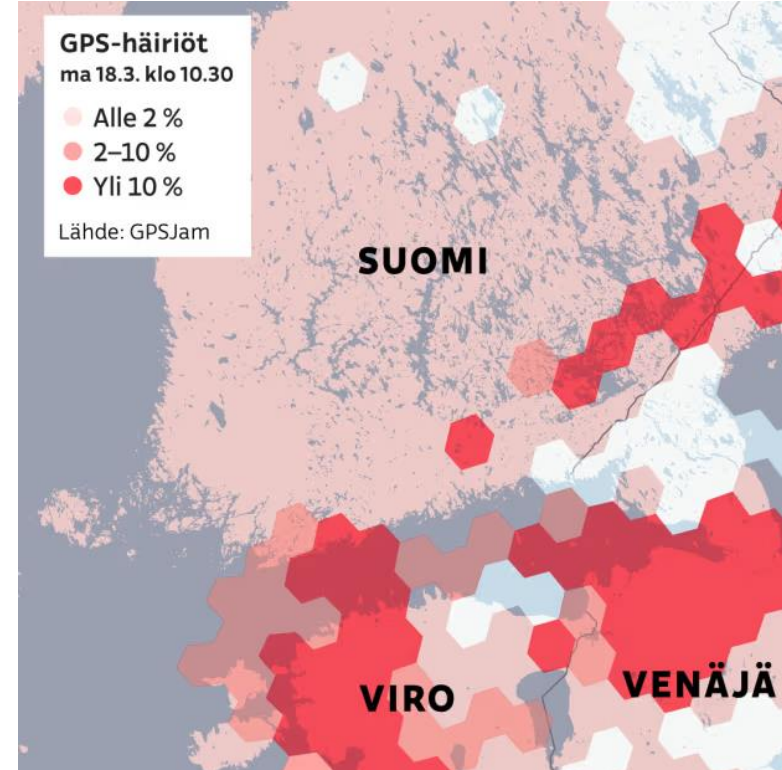


**Accuracy + Availability + Reliability**

**Users now expect a sense of reliability, achieved by building resilience into the system.**

# GNSS Interference in Finland

- **Severe interference detected during 2024-2025**
- High impact on air traffic
- Cancelled flights
  - Mostly to eastern Finland
- Reports of jamming and spoofing from the Gulf of Finland
- Limited effect on land



29.04.2024

**Finnair temporarily suspends flights between Helsinki and Tartu**

Finnair has announced that it is suspending its flights between Helsinki and Tartu from 29 April-31 May due to interference with GPS signals. The airline itself will contact all passengers who have purchased flight tickets for this period via SMS or e-mail.

Liikenne

**Kaksi Finnairin konetta joutui palaamaan Virosta takaisin Suomeen GPS-häirinnän takia**

GPS-häirintä on yleistä, mutta useimmiten se ei aiheuta lentojen kääntymistä takaisin, kertoo Finnairin viestintäjohtaja.

Tartun lentokenttä on erityisen altis GPS-häirinnälle, sillä siellä lähestyminen vaatii GPS-signaalia. Arkistokuva. Kuva: Sami Jumppanen / Korpipaja

LAURA KANGAS  
27.4. 9:15 · Päivitetty 27.4. 10:05





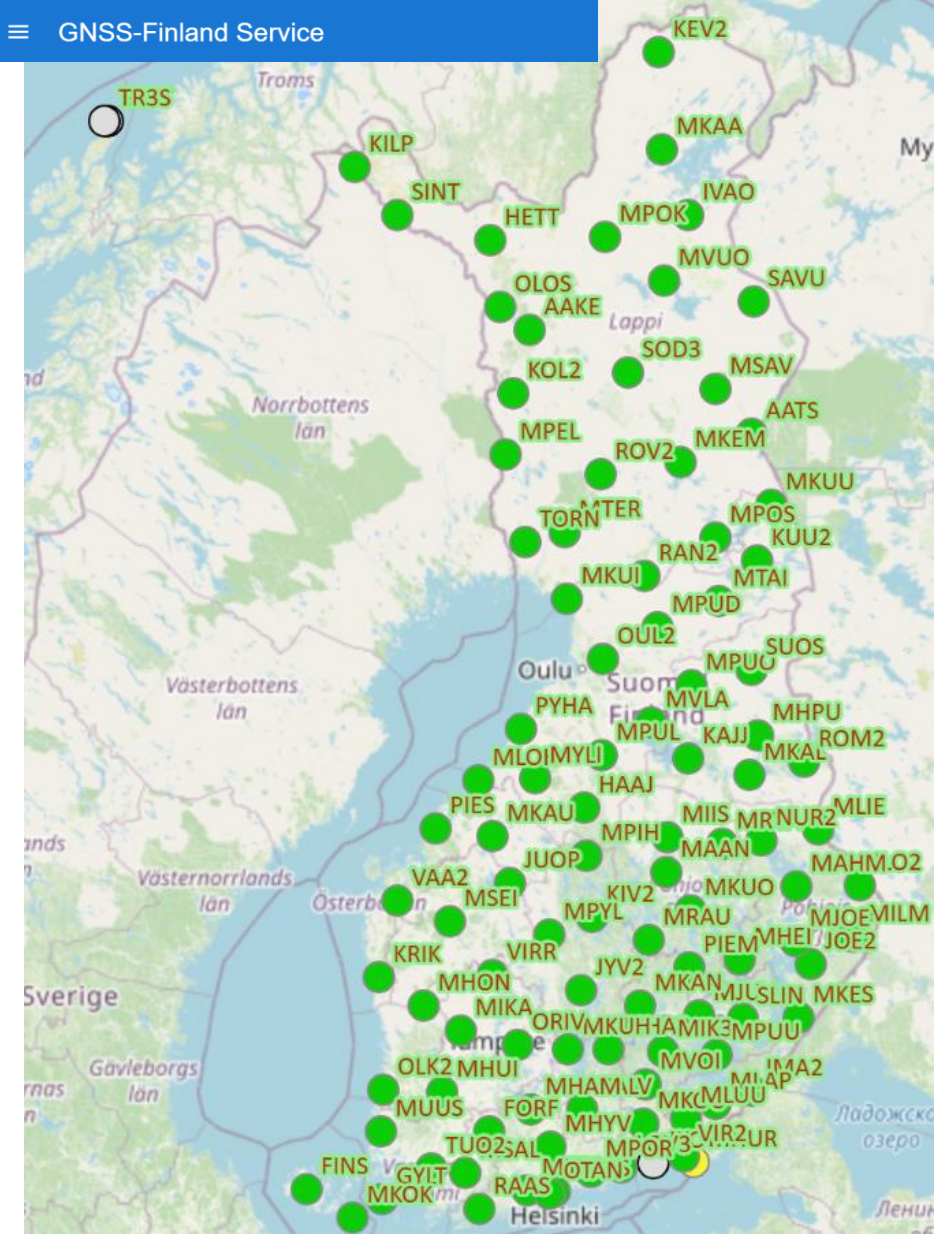
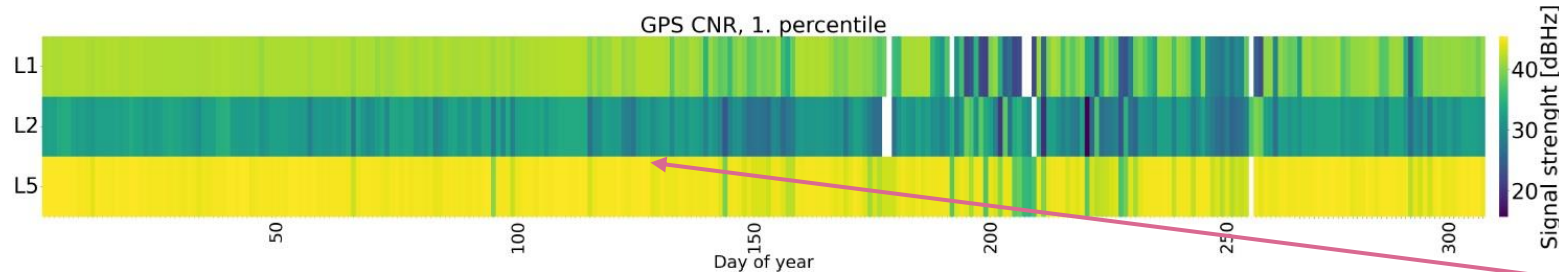
**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# Effects of Prolonged GNSS Jamming on a Continuously Operating Monitoring Station

# GNSS-Finland and the Availability of Satellite Navigation Systems

## Realtime monitoring of navigation signals with FinnRef monitoring station network

- Server and traffic light (web-site) interface for fault notifications
- Based on the monitoring station network maintained by the NLS (~100 stations)
- Public service started in 2021:  
<https://gnss-finland.nls.fi>
- Example of interference events detected at one of the monitoring stations



Lowest 1 percentile average  $C/N_0$  for the GPS L1, L2, and L5 signals

# Effects of Interference on a Monitoring Station (1/3)

Example case:

- **Extended jamming attack against a modern Multi-Constellation, Multi-Frequency (MCMF) GNSS receiver**

- ❖ All available constellations
- ❖ All available signals

- Jamming targeting upper L-band

- ❖ L1, E1, B1, G1

- PNT from lower L-band

- ❖ E5, L5, B3, G2

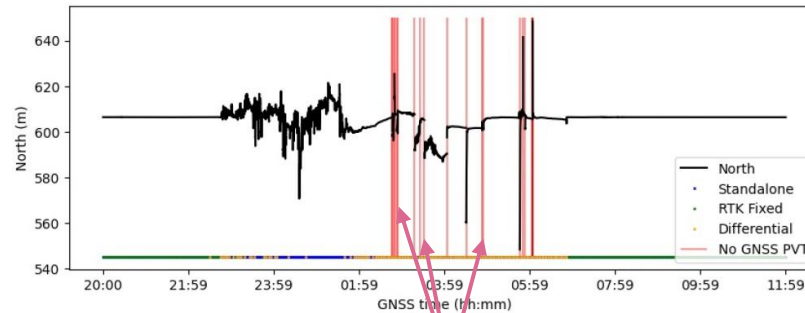
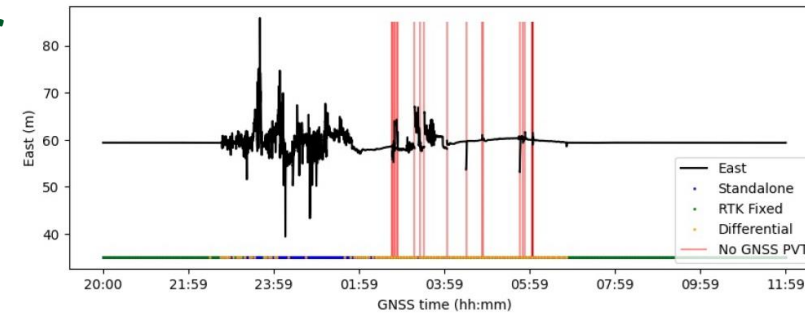
Effects:

- **Positioning accuracy degraded**

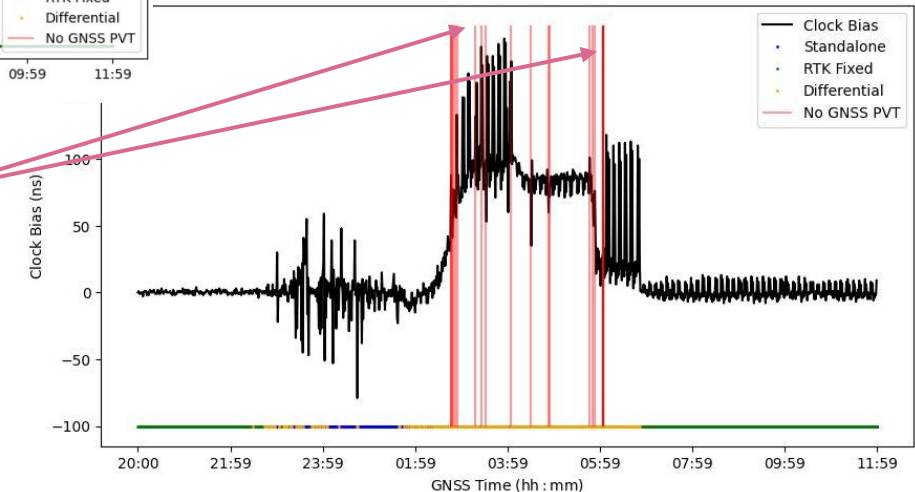
- ❖ Nominal: centimetre level
- ❖ **Under jamming: ~10 m or more**

- **Time synchronisation**

- ❖ Clock bias increased by up to 180 ns



PNT LOST!





# Effects of Interference on a Monitoring Station (2/3)

Example case:

➤ **Extended jamming attack against a modern Multi-Constellation, Multi-Frequency (MCMF) GNSS receiver**

- ❖ All available constellations
- ❖ All available signals

➤ Jamming targeting upper L-band

- ❖ L1, E1, B1, G1

➤ PNT from lower L-band

- ❖ E5, L5, B3, G2

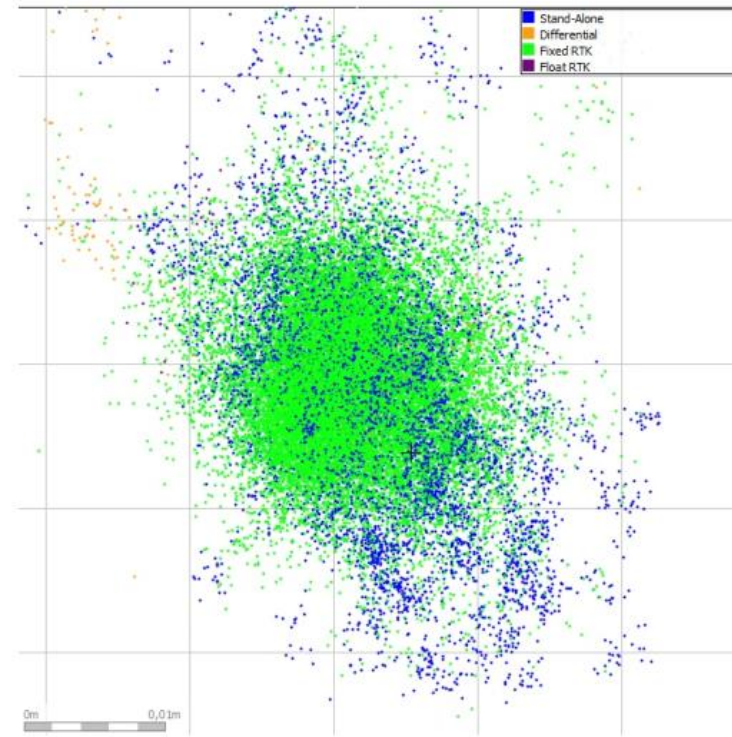
Effects:

➤ Positioning accuracy degraded

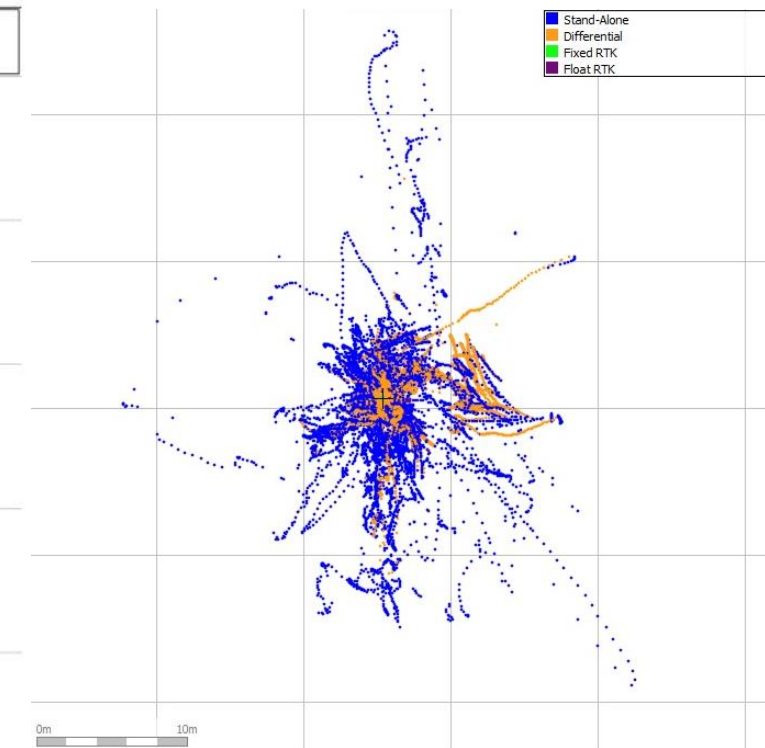
- ❖ Nominal centimetre level
- ❖ **Under jamming ~10 m or more**

➤ Time synchronisation

- ❖ Clock bias increased by up to 180 ns



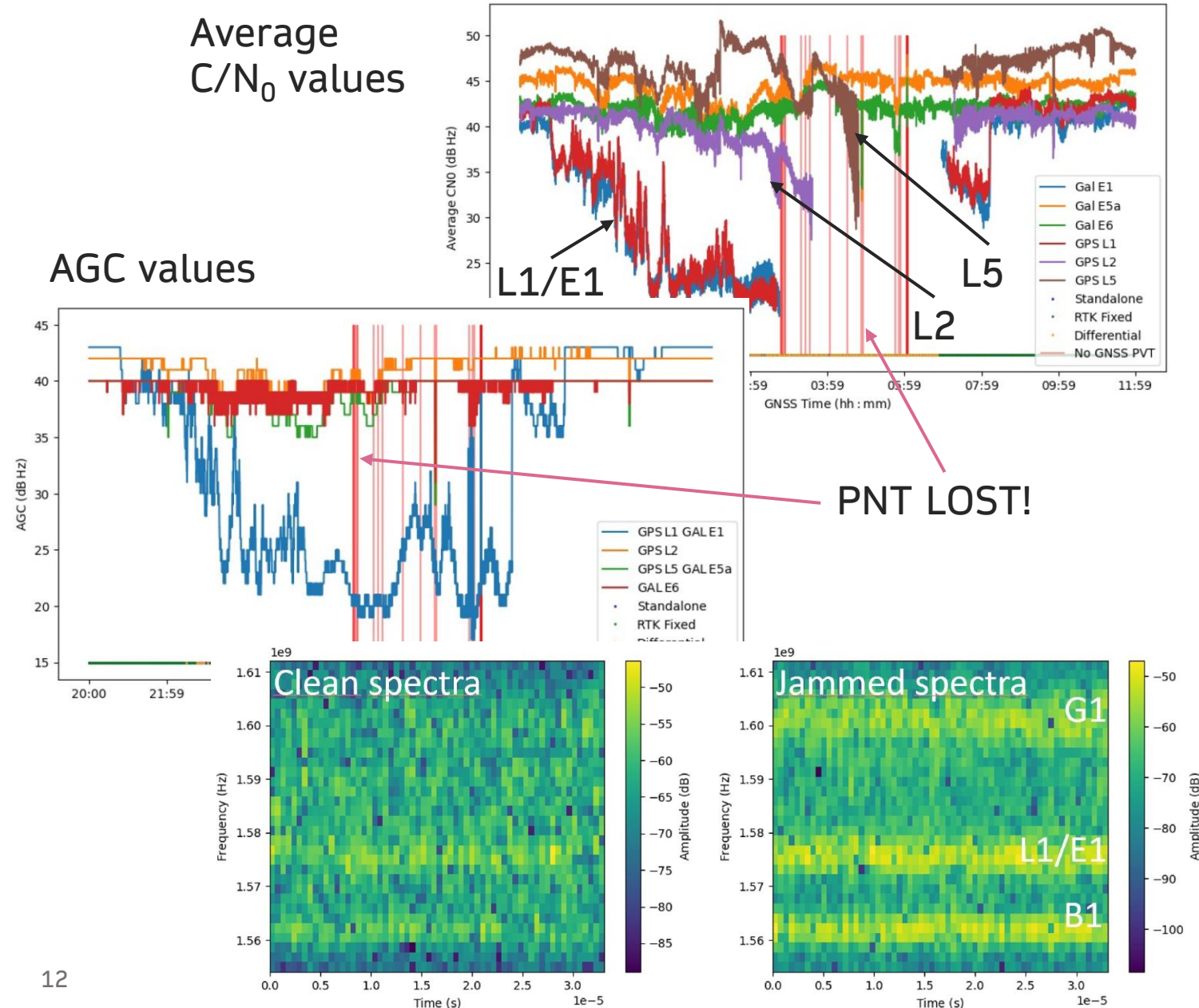
Nominal Operational condition



16-hour measurement period

# Effects of Interference on a Monitoring Station (3/3)

- Interference was strong enough to completely deny use of upper L-band!
- GPS L2 and L5 signals were lost, but Galileo E5a and E6 were working fine.
- Receiver could still operate by utilising lower L-band
- **PNT solution was completely lost only for ~ 24 seconds in total**
- Recommendation: **To ensure the resilience of critical infrastructures or critical services, the use of MCMF receivers is encouraged!**





**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# GNSS Interference Detection: A Largely Solved Problem

# Interference Detection Techniques\*

- **‘Interference’** in this context defined as: intentional/unintentional presence of **interference in the form of either ‘jamming’ or ‘spoofing’**
- Following techniques are presented:
  - Automatic Gain Control (AGC) based technique
  - Running Digital Sum (RDS) based technique
  - Carrier-to-Noise density ratio ( $C/N_0$ ) based technique
  - Proposed Chi-Square Test based technique

\*Mohammad Zahidul H. Bhuiyan, Muwahida Liaquat, Saiful Islam et al. Implementation and Performance Analysis of a Chi-square Test based GNSS Signal Anomaly Detection, 03 June 2025, PREPRINT (Version 1) available at Research Square [<https://doi.org/10.21203/rs.3.rs-6750861/v1>]



# Chi-Square Test based Interference Detection Technique (1/2)

- The Chi-Square Test is a statistical hypothesis test that compares the distribution between observed and expected data and generates a metric for distribution similarity.
- The Chi-Square Test is applied on **digitized IF data samples** at the **receiver tracking stage** just before the actual signal correlation

$$\text{Chi-Square Test metric: } \tau_x = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i}$$

$$\text{Chi-Square Test metric in dB: } \tau_{x_{dB}} = 10 \log_{10}(\tau_x)$$

$$\text{Detection threshold in dB: } \tau_{\alpha_{dB}} = 10 \log_{10}(\mu_m + \sqrt{2\sigma_m^2} \operatorname{erfc}^{-1}(1 - P_{fa}))$$

$$\text{Hypothesis definition: } \tau_{x_{dB}} < \tau_{\alpha_{dB}} \rightarrow H_0, \text{Nominal}$$

$$\tau_{x_{dB}} \geq \tau_{\alpha_{dB}} \rightarrow H_1, \text{Anomaly}$$

$$\text{Expected impact under H1: } \bar{\alpha}_{dB} \Big|_{H_1} = \sum_{i=1}^N \frac{\tau_{x_{dB}}(i) - \tau_{\alpha_{dB}}(i)}{N} \Big|_{H_1}$$

Digitized signal samples with AWGN at IF:  $y[n] = S_{IF}[n] + w[n]$

Digitized signal samples in the presence of interference:  $x[n] = y[n] + vq[n]$

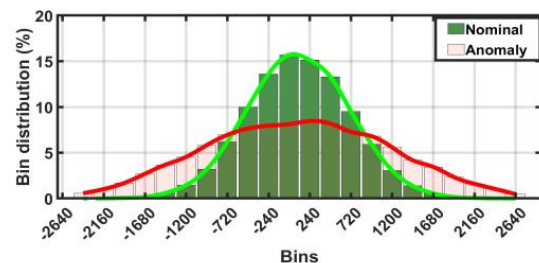
$$\text{Expected samples: } E[k] = \frac{1}{N} \sum_{i=1}^k y_i$$

$$\text{Observed samples: } O[k] = \frac{1}{N} \sum_{i=1}^k x_i$$

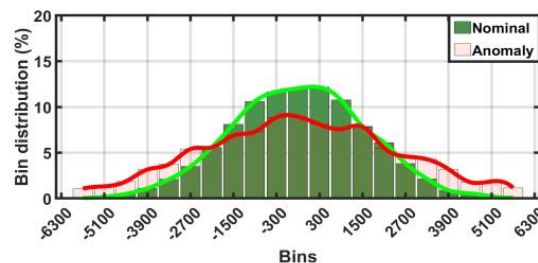
$q[n]$  is the interference signal and  $v$  is the amplitude factor

# Chi-Square Test based Interference Detection Technique (2/2)

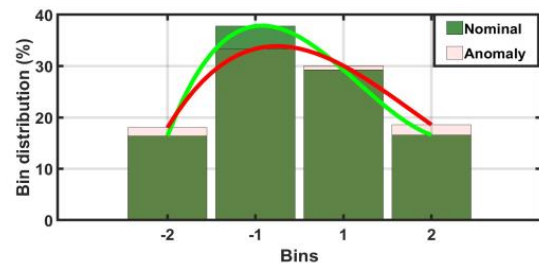
- Distribution of digitized samples under different scenarios:



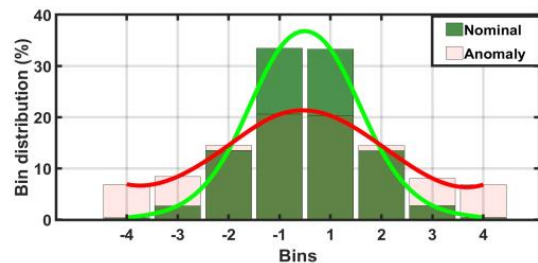
(a)



(b)

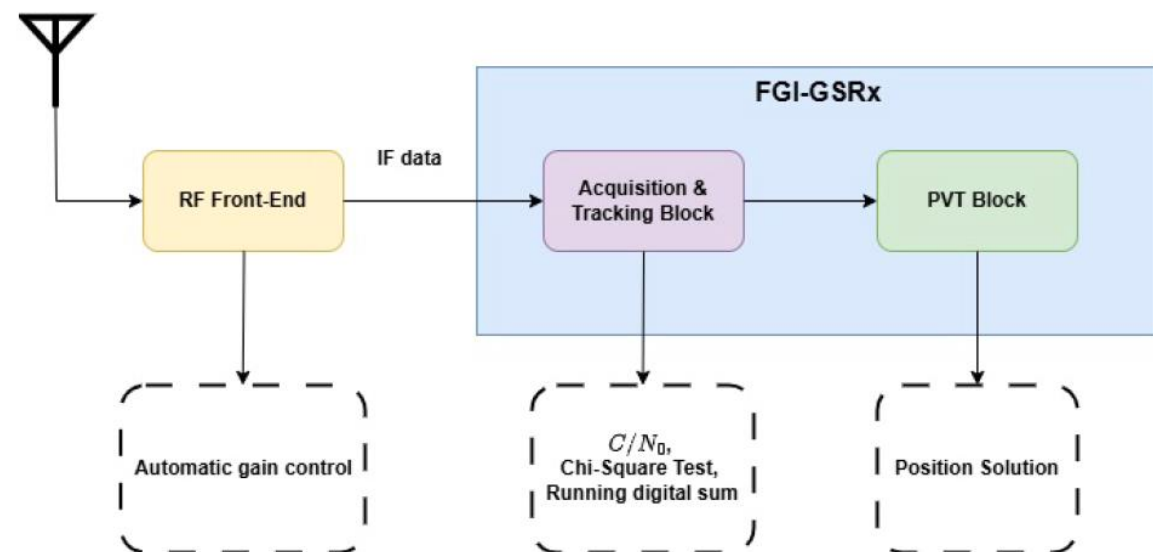


(c)



(d)

(a)TEXBAT ds2 (b) OAKBAT os2 (c) FGI-SpoofRepo TG-DFMC, (d) JammerTest JT-17.1.6



Generic functional block diagram of a GNSS receiver



# Datasets Selection (1/2)

- Publicly available datasets and real-world jammer test campaign data are used for testing and evaluation.

Scenario identifier	Description	Impact	Power advantage (dB)	Duration (s)	Onset (s)
ds0	Clean static	N/A	N/A	450	N/A
ds2	Static overpowered spoofing	Time push	10	450	110
ds3	Static matched power spoofing	Time push	1.3	450	120
ds4	Static matched power spoofing	Position push	0.4	400	114
ds7	Static matched power spoofing	Time push	1.3	450	120
ds8	Static matched power spoofing	Time push	1.3	450	120

TEXBAT datasets

<https://radionavlab.ae.utexas.edu/texbat/>

Scenario identifier	Scenario description	Impact	Power advantage (dB)	Duration (s)	Onset (s)
os0	Clean static	N/A	N/A	240	N/A
os2	Static overpowered spoofing	Time push	10	240	115
os3	Static matched power spoofing	Time push	1.3	240	119
os4	Static matched power spoofing	Position push	0.4	240	119

OAKBAT datasets

<https://doi.ccs.ornl.gov/dataset/d21dfe58-3af9-5ed8-9c97-693c12045aee>

# Datasets Selection (2/2)

- Publicly available datasets and real-world jammer test campaign data are used for testing and evaluation.

Scenario identifier	Scenario description	Duration (s)	Onset (s)
TG-DFMC	Targeted overpowered dynamic spoofing attack	370	138
UT-DFMC	Untargeted spoofing attack with asynchronous positioning and timing	370	135
Meaconing	Meaconing attack with asynchronous timing	400	155

FGI-SpoofRepo datasets

<https://doi.org/10.23729/7a648509-2ca8-4a7d-8223-0b429182f857>

Scenario identifier	Scenario description	Power transmission (dBm)	Duration (s)	Onset (s)
JT23-4.1.5	Continuous high powered pseudo-random noise jamming	43	300	259
JT23-16.1.1	Incoherent overpowered using broadcast (true) ephemerides	33	300	150
JT23-17.1.6	Coherent spoofing from stationary spoofer using broadcast (true) ephemerides	25	500	226

JammerTest 2023 datasets

<https://doi.org/10.23729/fd-06d27736-45cb-3ca2-aff8-725d42c6caeb>

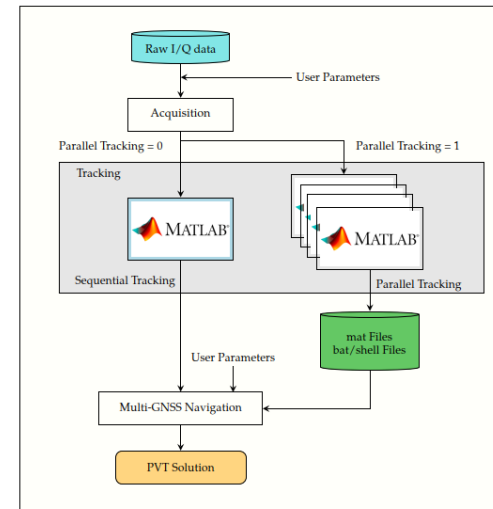
# Experimental Setup: Research Tools

- Various Front-Ends are used to capture raw GNSS data samples for different datasets

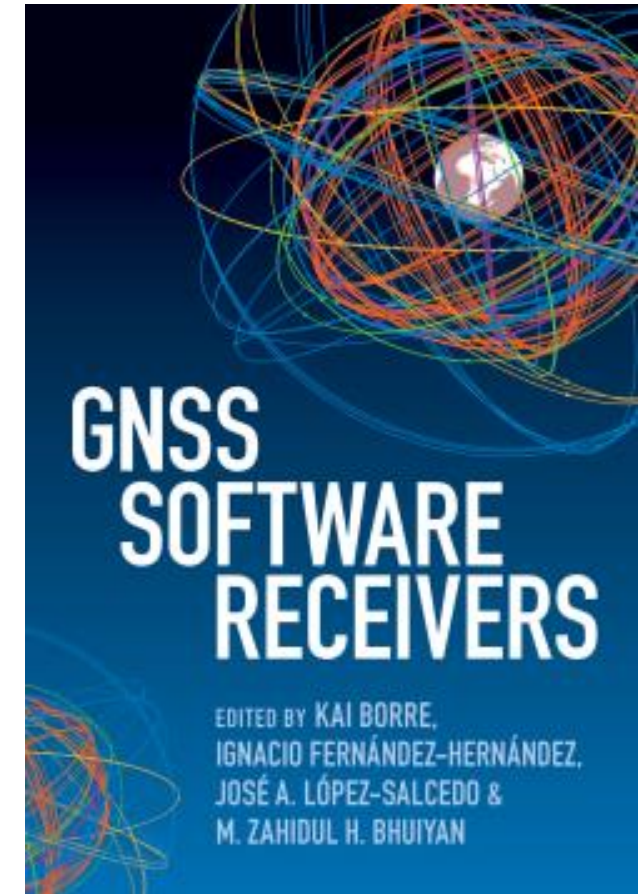
Front-ends	Received signal bandwidth (MHz)	Down-converted intermediate frequency (MHz)	Sampling rate (Mpsps)	ADC bits	Bits per sample	Data type
LabSat 3 wideband	30	0	30.69	3	8	Complex
Stereo v2 (MAX2769B)	4.2	6.39	26	2	8	Real
NI's PXIe-5673E	25	0	25	16	16	Complex
USRP X310	5	0	5	14	16	Complex

List of Front-Ends with key configuration parameters

- FGI-GSRx software-defined receiver is configured in accordance with the associated front-ends:  
<https://github.com/nlsfi/FGI-GSRx>

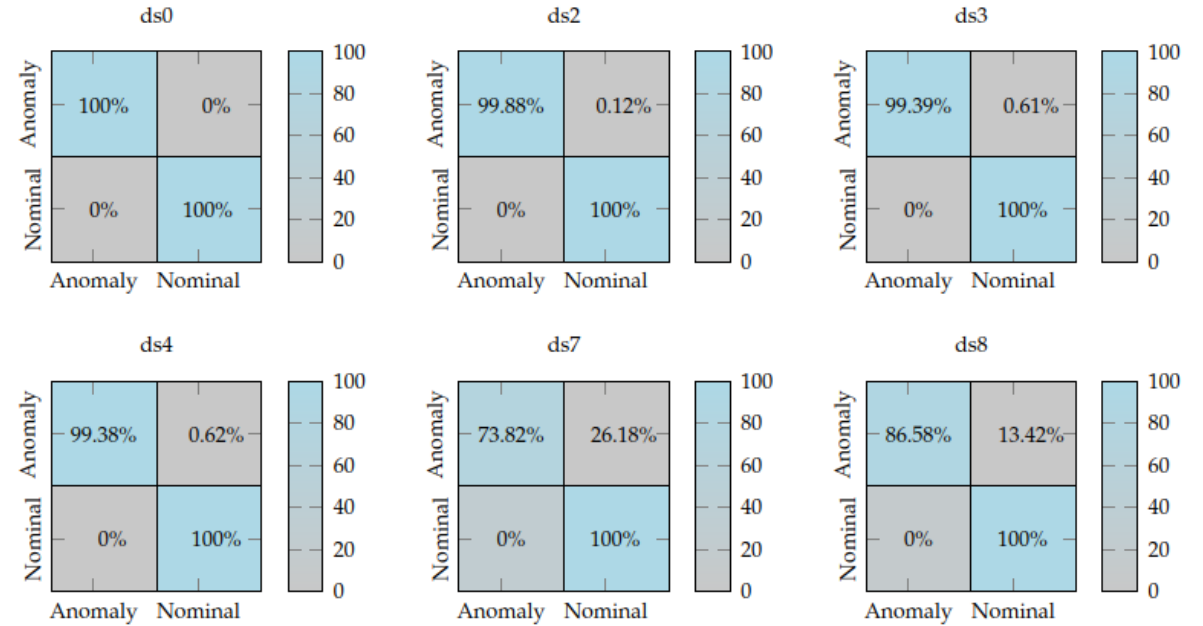
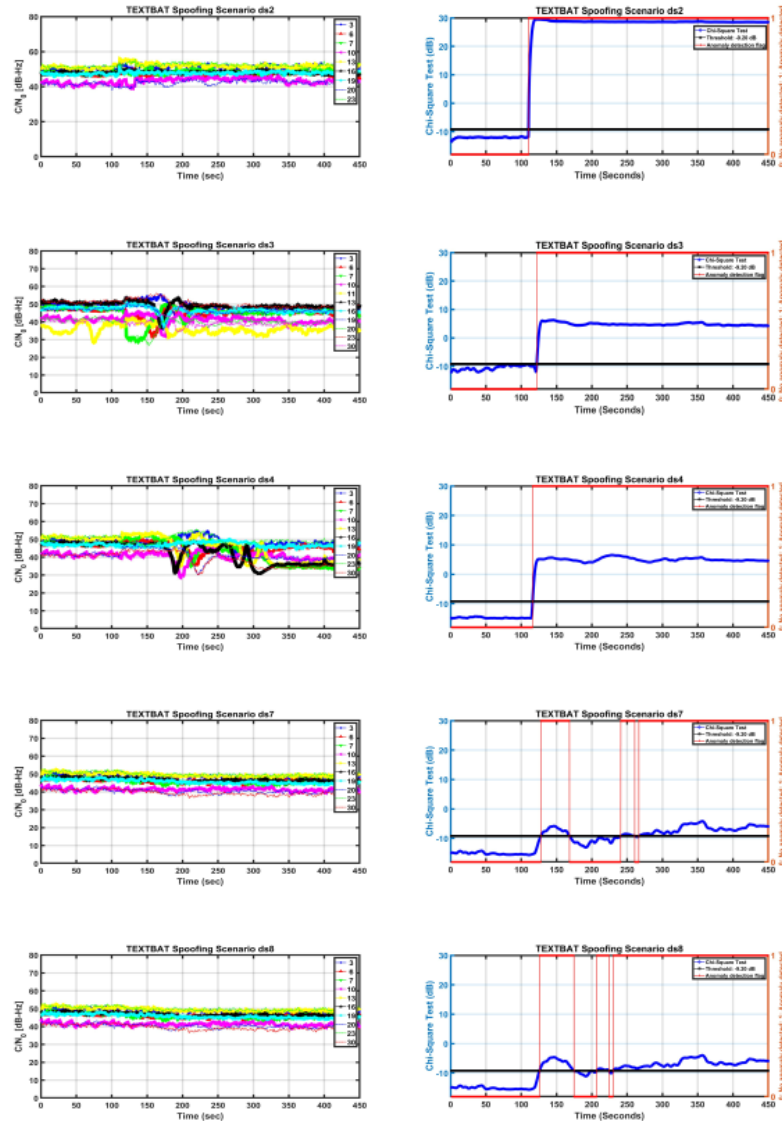


FGI-GSRx-v2.0.0 Receiver Architecture



<https://doi.org/10.1017/9781108934176>

# Results and Analysis: TEXBAT



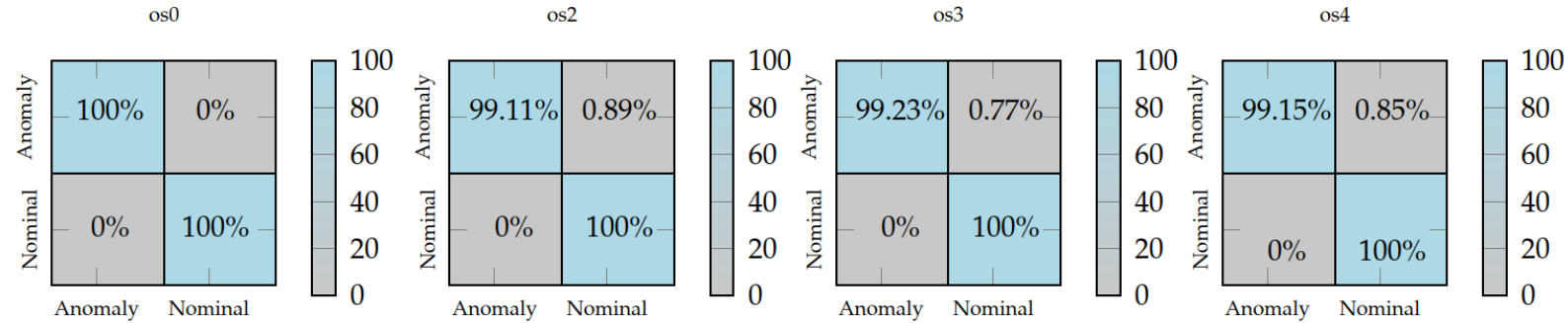
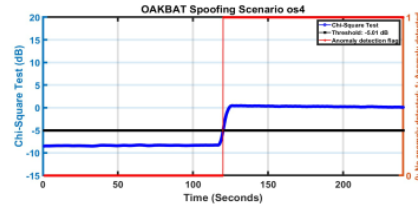
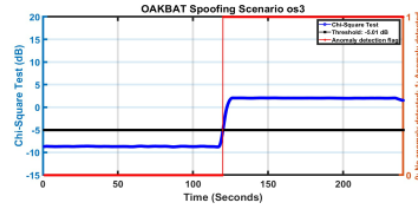
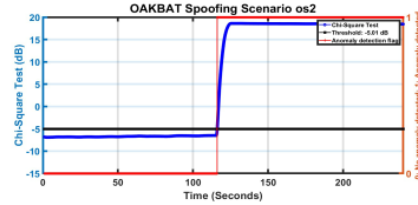
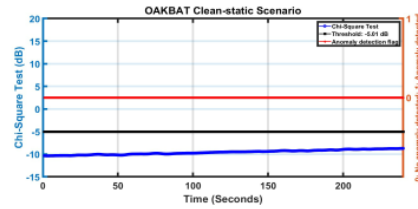
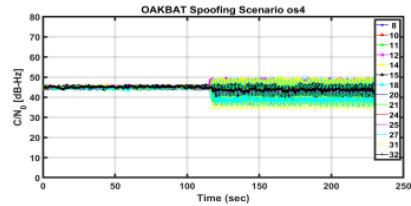
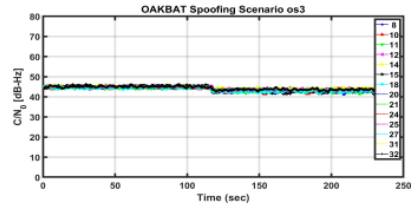
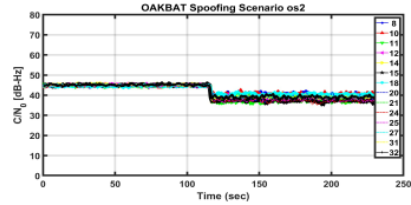
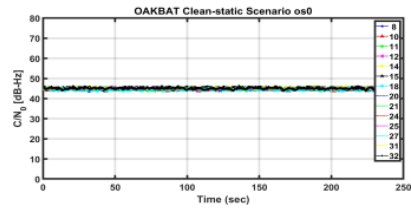
Confusion matrix for TEXBAT datasets

Scenario Identifier	Accuracy	Precision	Recall	FAR	Threshold $\tau_{\alpha_{dB}}$ (dB)	Expected impact $\bar{\alpha}_{dB}$ (dB)
ds0	100%	100%	100%	0%	-9.2	N/A
ds2	99.94%	100%	99.88%	0%		37.8
ds3	99.69%	100%	99.39%	0%		13.8
ds4	99.68%	100%	99.37%	0%		14.0
ds7	86.90%	100%	73.81%	0%		1.2
ds8	93.29%	100%	86.58%	0%		2.0

Detection performance of the Chi-Square Test for TEXBAT datasets

(Left) C/N<sub>0</sub> of GPS satellites; (Right) Anomaly detection based on the Chi-Square Test metric

# Results and Analysis: OAKBAT



Confusion matrix for OAKBAT datasets

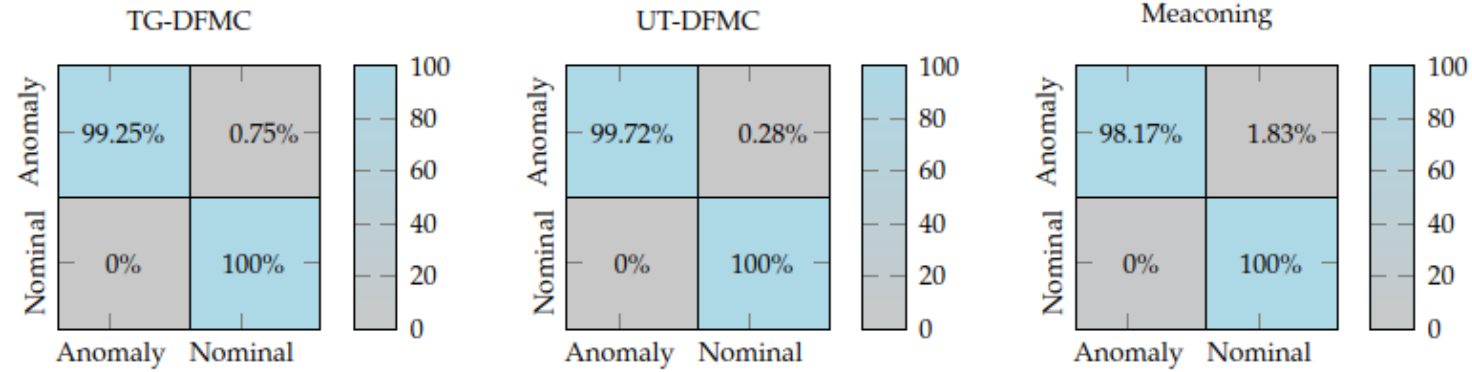
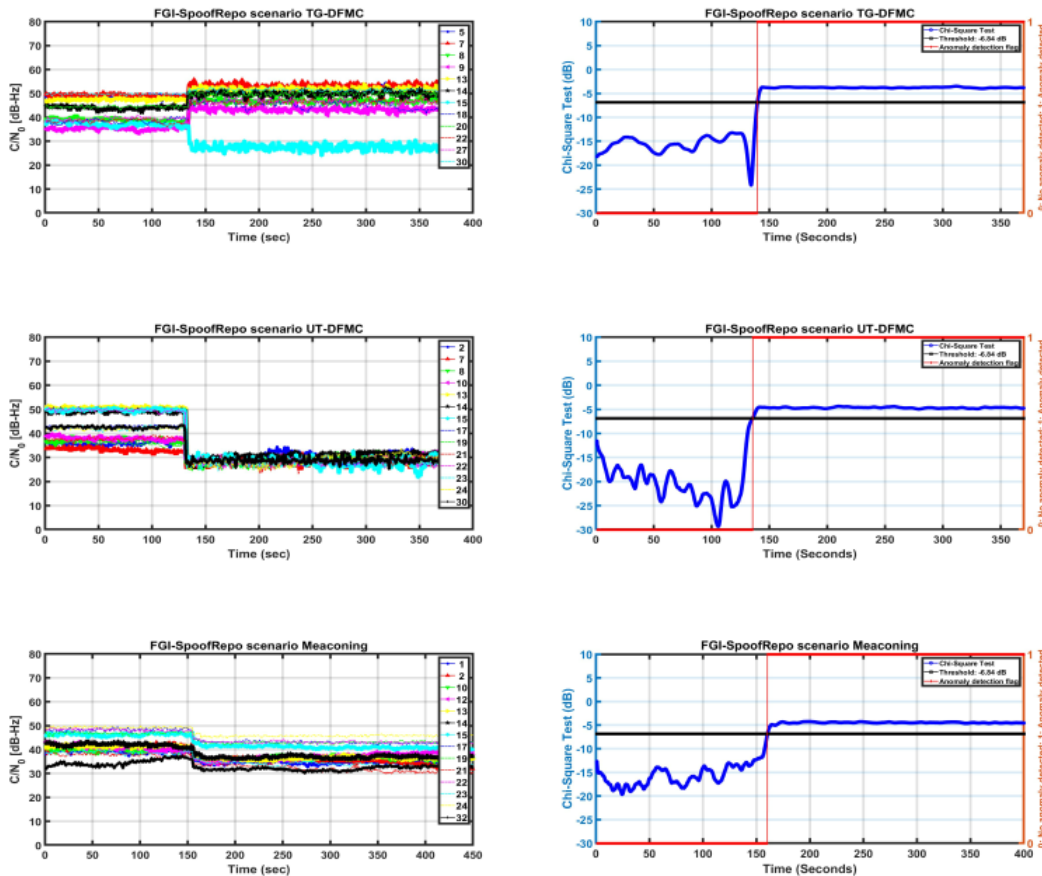
Scenario identifier	Accuracy	Precision	Recall	FAR	Threshold $\tau_{\alpha_{dB}}$ (dB)	Expected impact $\bar{\alpha}_{dB}$ (dB)
os0	100%	100%	100%	0%	-5.01	N/A
os2	99.55%	100%	99.11%	0%		12.8
os3	99.61%	100%	99.23%	0%		3.2
os4	99.57%	100%	99.14%	0%		4.8

Detection performance of the Chi-Square Test for OAKBAT datasets

(Left)  $C/N_0$  of GPS satellites; (Right) Anomaly detection based on the Chi-Square Test metric



# Results and Analysis: FGI-SpoofRepo



Confusion matrix for FGI-SpoofRepo datasets

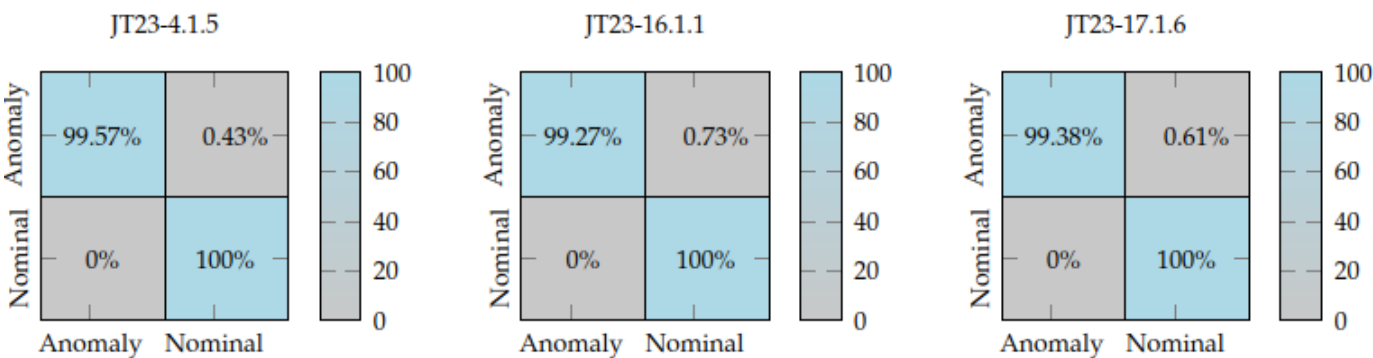
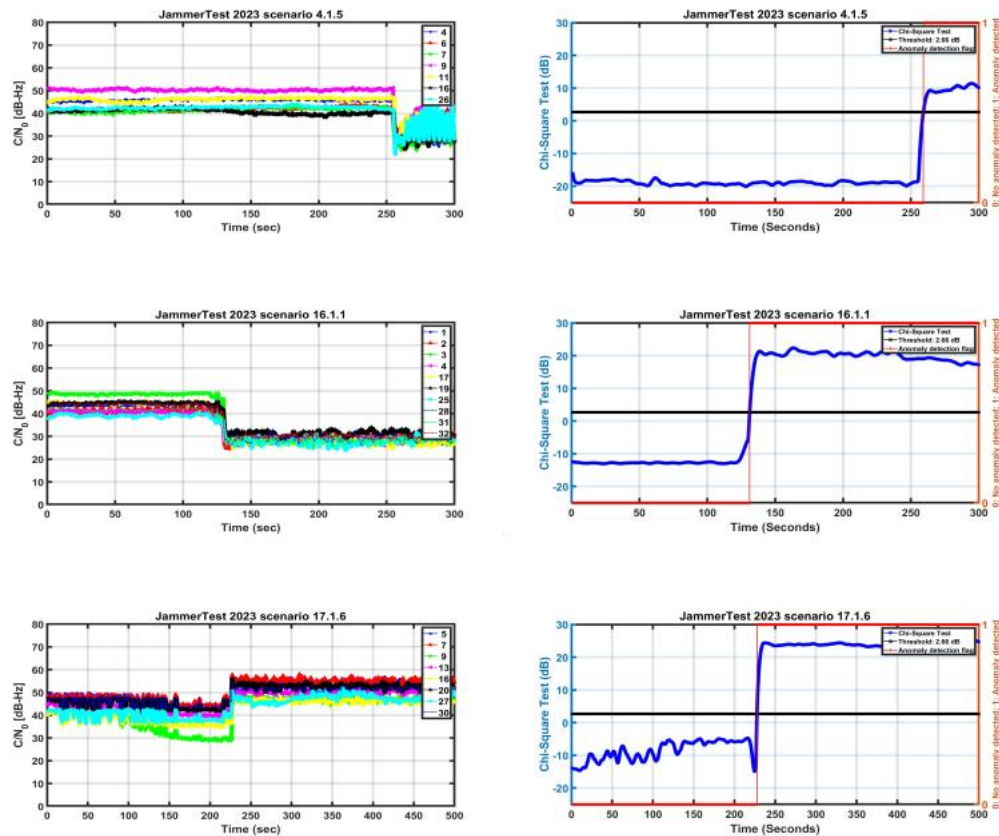
Scenario identifier	Accuracy	Precision	Recall	FAR	Threshold $\tau_{\alpha_{dB}}$ (dB)	Expected impact $\bar{\alpha}_{dB}$ (dB)
TG-DFMC	99.62%	100%	99.25%	0%	-6.84	2.2
UT-DFMC	99.86%	100%	99.72%	0%		1.3
Meaconing	99.08%	100%	98.16%	0%		1.4

Detection performance of the Chi-Square Test for FGI-SpoofRepo datasets

(Left) C/N<sub>0</sub> of GPS satellites; (Right) Anomaly detection based on the Chi-Square Test metric



# Results and Analysis: JammerTest 2023



Confusion matrix for JammerTest 2023 datasets

Scenario identifier	Accuracy	Precision	Recall	FAR	Threshold $\tau_{\alpha_{dB}}$ (dB)	Expected impact $\bar{\alpha}_{dB}$ (dB)
JT23-4.1.5	99.78%	100%	99.57%	0%	2.66	6.9
JT23-16.1.1	99.63%	100%	99.27%	0%		17.1
JT23-17.1.6	99.69%	100%	99.38%	0%		21.1

Detection performance of the Chi-Square Test for JammerTest 2023 datasets

(Left) C/N<sub>0</sub> of GPS satellites; (Right) Anomaly detection based on the Chi-Square Test metric

# Comparison against the Most Promising ML Techniques

⇒ Chi-Square Test outperforms ML-based methods for TEXBAT and OAKBAT scenarios except for ds7 and ds8

⇒ Datasets ds7 and ds8 assume carrier-phase alignment and also power-matched with the authentic signal which is impossible to achieve without precise information of PVT of the victim receiver

Method	KPI	ds0	ds2	ds3	ds4	ds7	ds8
ZDD [19]	Accuracy	99.7%	99.7%	99.6%	100%	89.7%	-
	FAR	0.30	1.01%	1.44%	0%	2.61%	-
TSVAE [20]	Accuracy	-	99.4%	99.4%	99.7%	99%	99.3%
	FAR	-	2.1%	1%	1%	1.7%	1.4%
Chi-Square Test	Accuracy	100%	99.94%	99.69%	99.68%	86.90%	93.29%
	FAR	0%	0%	0%	0%	0%	0%

Comparison of detection performance of a few reported ML Techniques and the proposed Chi-Square Test for TEXBAT datasets

Method	KPI	os0	os2	os3	os4
TSVAE [20]	Accuracy	-	99.4%	99.1%	99.7%
	FAR	-	2.1%	2.1%	1%
Chi-Square Test	Accuracy	100%	99.55%	99.61%	99.57%
	FAR	0%	0%	0%	0%

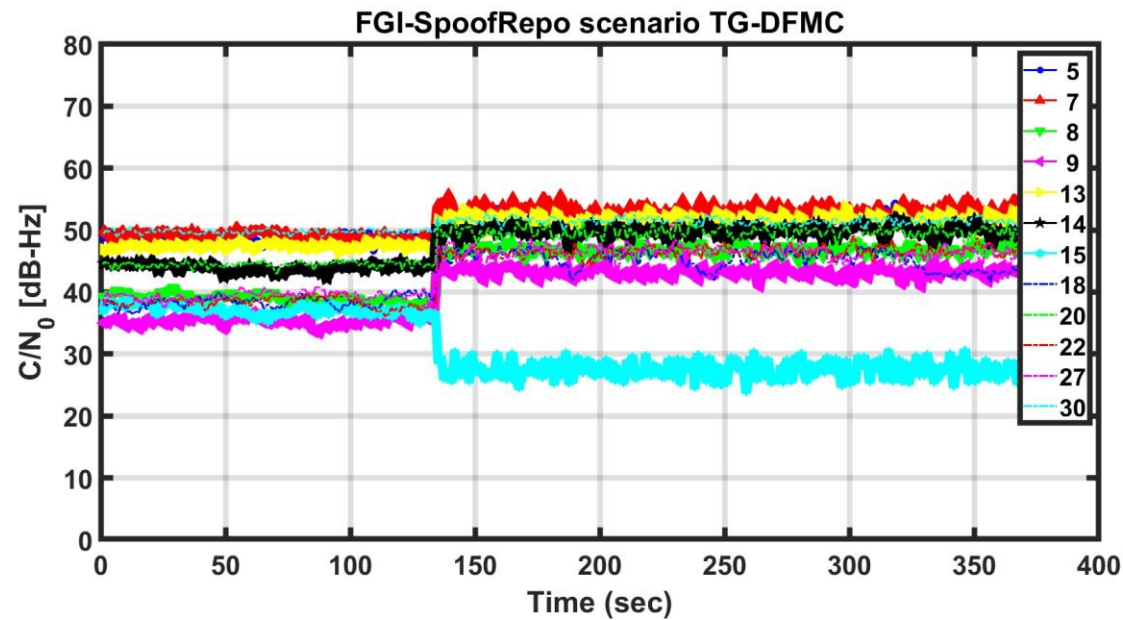
Comparison of detection performance of one reported ML Technique and the proposed Chi-Square Test for OAKBAT datasets

# Conclusion

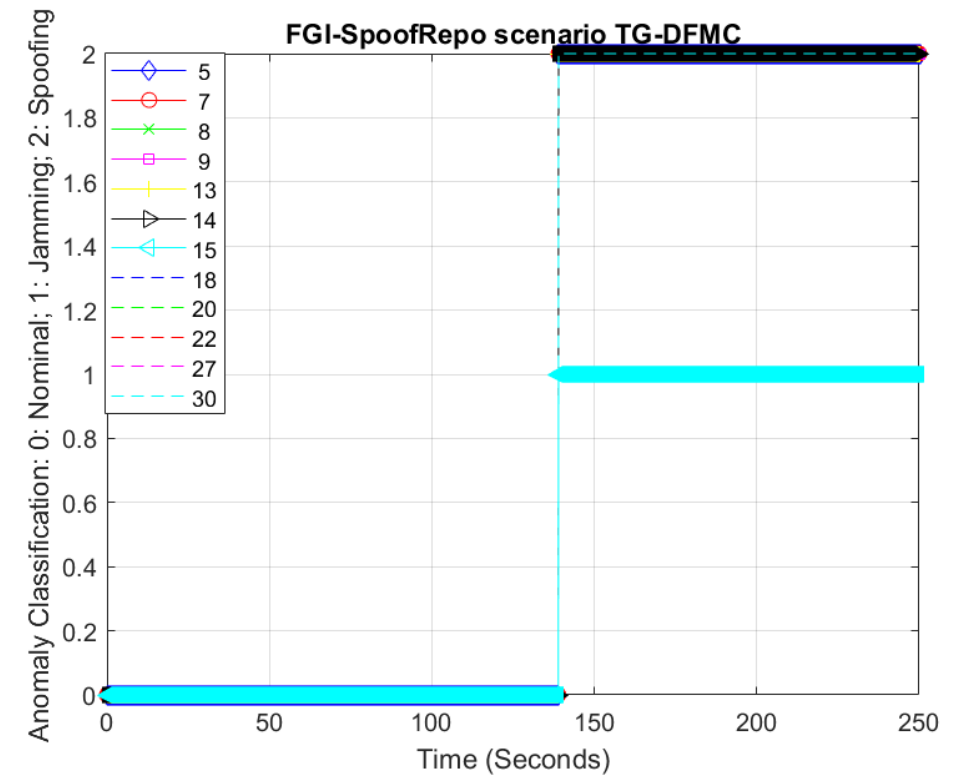
- The proposed **Chi-Square Test** technique is effective for GNSS signal anomaly detection with a detection accuracy greater than 99% and no false alarm under a realistic signal propagation environment.
- Datasets from **JammerTest 2023** campaign is publicly shared to promote open data policy.
- The **FGI-GSRx receiver** along with the configuration files are also publicly shared that can be used together with the datasets to benchmark any new PNT resilience techniques.
- The authors made **one of the first attempts to present anomaly detection performance across various public and real-world datasets**, hence offering a benchmark for future studies on similar topics.

# Interference Classification: FGI-SpoofRepo Dataset (1/4)

- Utilizes **Chi-Square Test metric**, **receiver's estimated  $C/N_0$**  and **satellite elevation angle** for classification into the following 3 classes:
  - Class 0: Nominal
  - Class 1: Jamming
  - Class 2: Spoofing



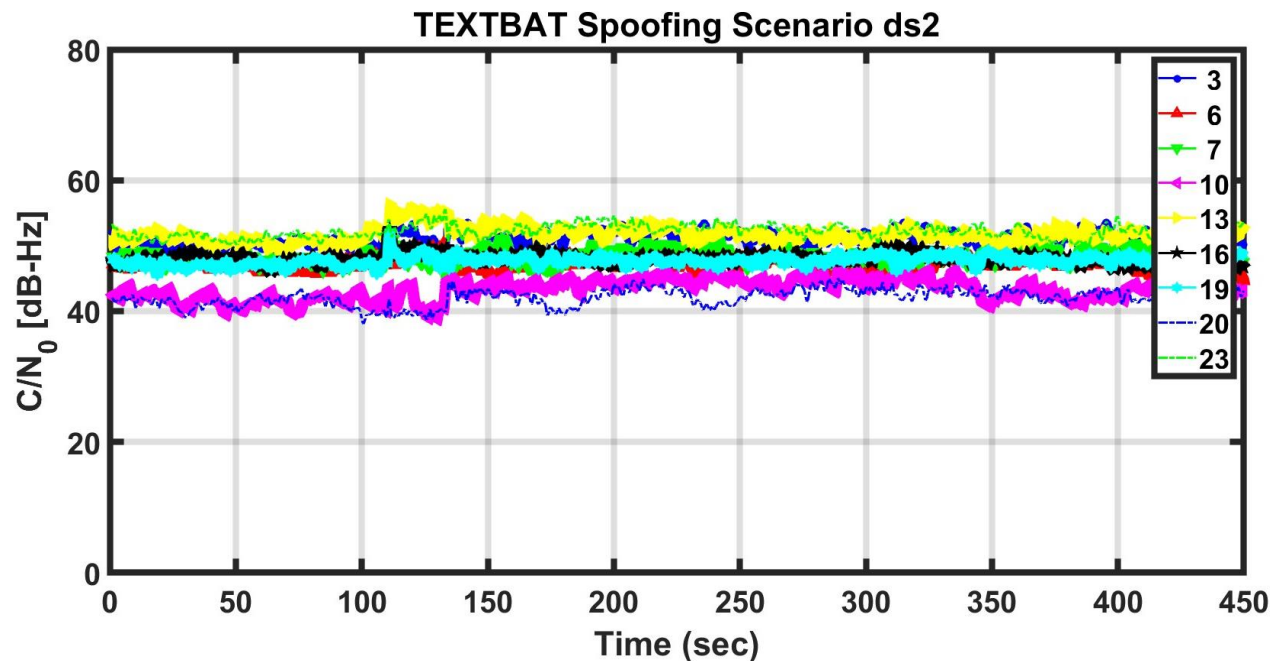
$C/N_0$  for scenario TG-DFMC



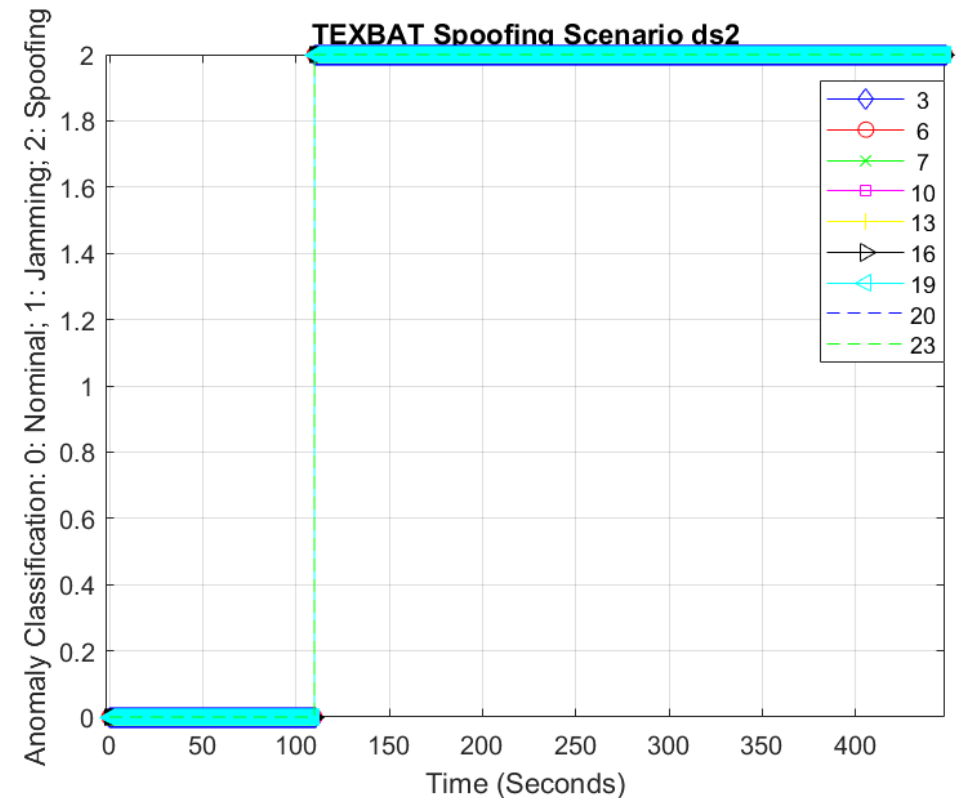
Anomaly classification result for TG-DFMC

# Interference Classification: TEXTBAT ds2 Spoofing Scenario (2/4)

- Utilizes **Chi-Square Test** metric, receiver's estimated  $C/N_0$  and **satellite elevation angle** for classification into the following 3 classes:
  - Class 0: Nominal
  - Class 1: Jamming
  - Class 2: Spoofing



$C/N_0$  for scenario TEXTBAT ds2

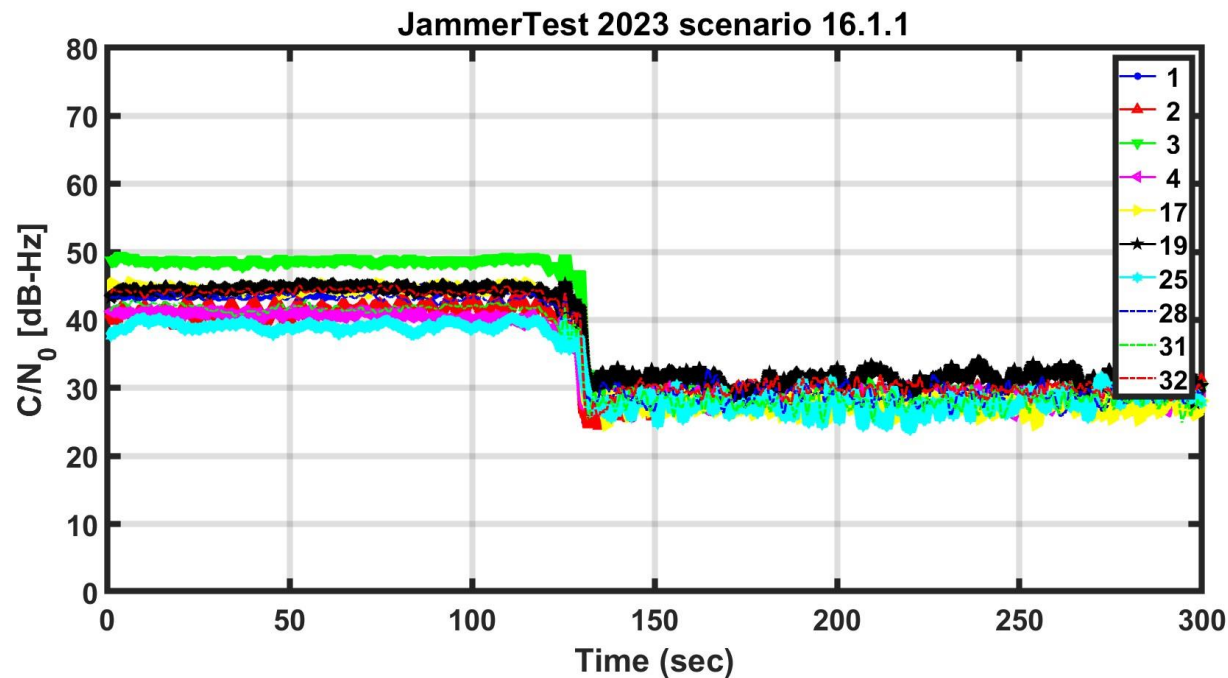


Anomaly classification result for TEXTBAT ds2

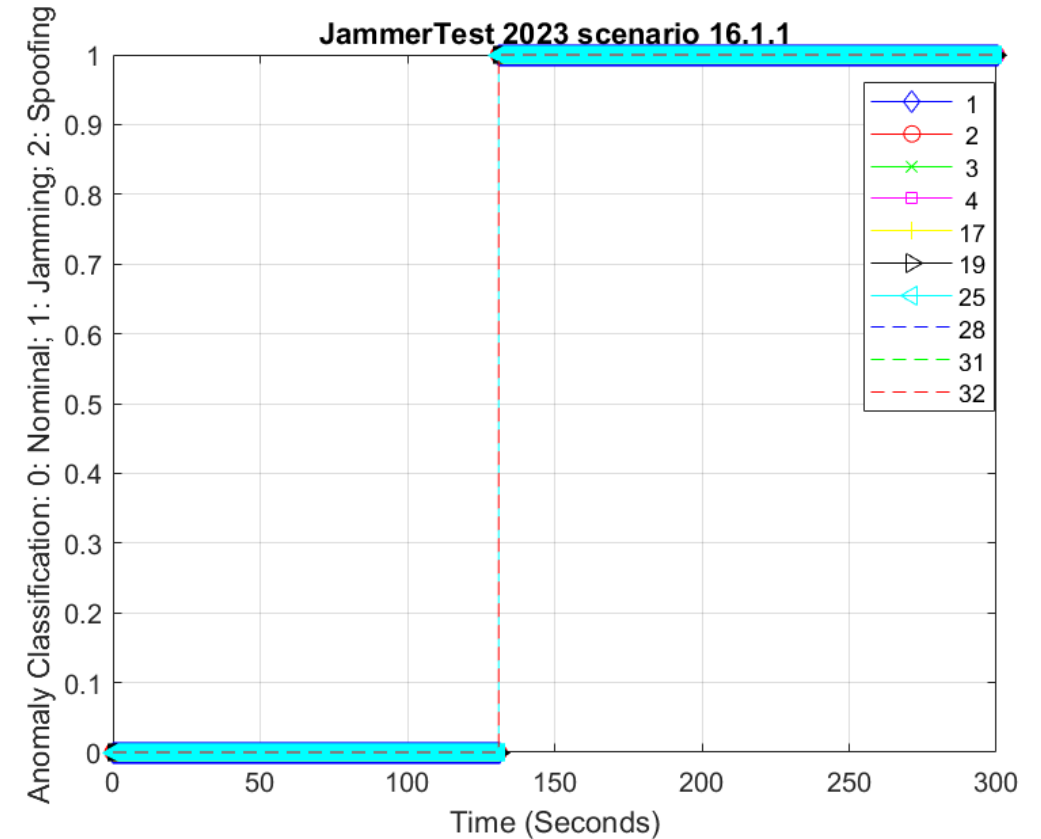


# Interference Classification: JammerTest2023 Incoherent Spoofing Scenario 16.1.1 (3/4)

- Utilizes **Chi-Square Test metric**, receiver's estimated  $C/N_0$  and **satellite elevation angle** for classification into the following 3 classes:
  - Class 0: Nominal
  - Class 1: Jamming
  - Class 2: Spoofing



$C/N_0$  for scenario JammerTest 2023 scenario 16.1.1

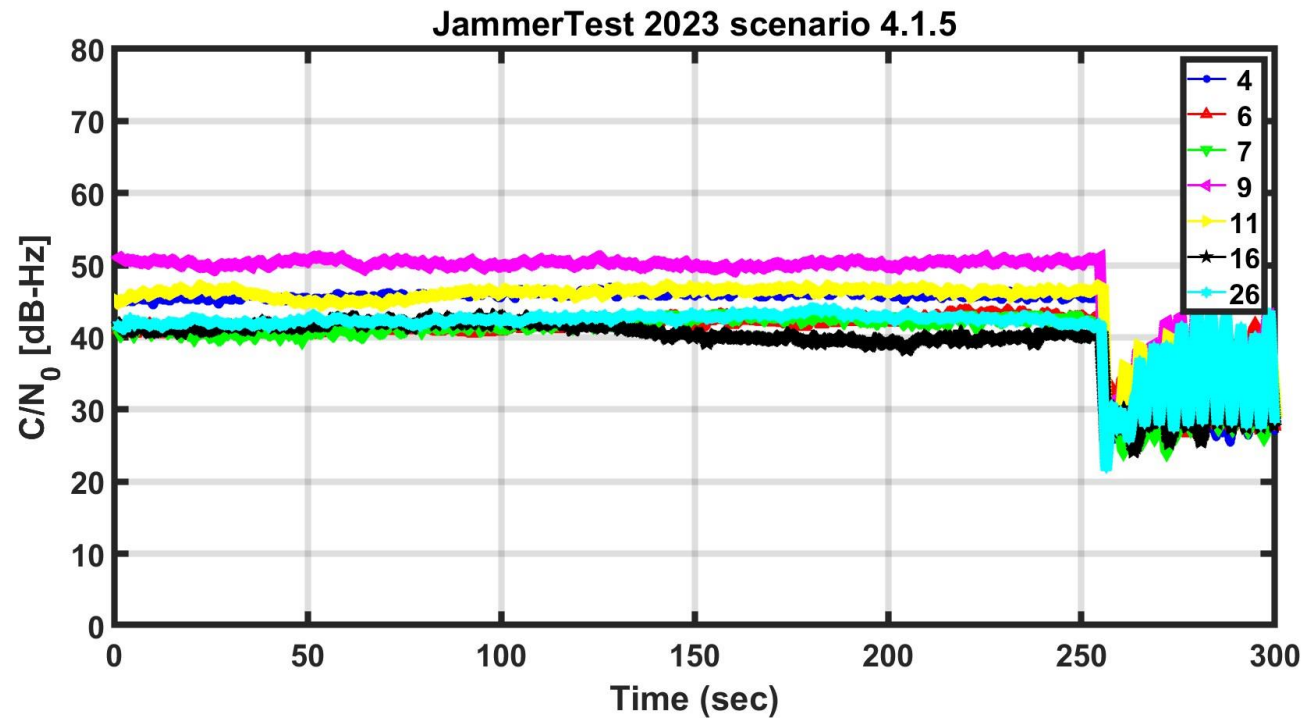


Anomaly classification result for JammerTest 2023 scenario 16.1.1

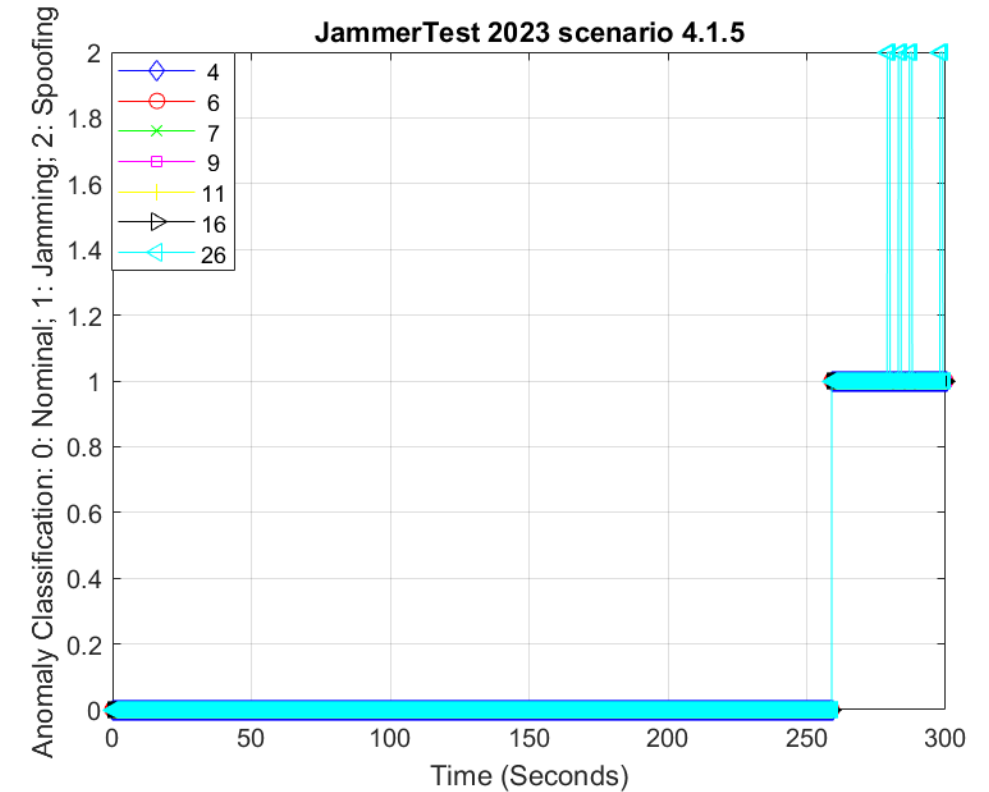


# Interference Classification: JammerTest2023 Jamming Scenario 4.1.5 (4/4)

- Utilizes **Chi-Square Test** metric, receiver's estimated  $C/N_0$  and **satellite elevation angle** for classification into the following 3 classes:
  - Class 0: Nominal
  - Class 1: Jamming
  - Class 2: Spoofing



$C/N_0$  for scenario JammerTest 2023 scenario 4.1.5



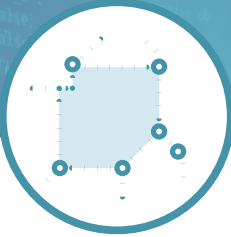
Anomaly classification result for JammerTest 2023 scenario 4.1.5



**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# GNSS Interference Mitigation: Emerging Technologies Paving the Way to Ultimate Resilience

# Suggested way forward



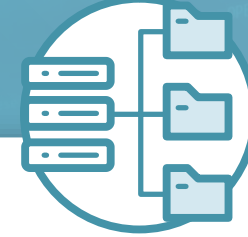
## Multi-Frequency Multi-Constellation Receivers

Increased resilience  
against both jamming and  
spoofing attacks



## Backup/Alternative Systems and Sensor Fusion

Securing critical  
infrastructure and  
safety of operations



## Monitoring GNSS Frequency Spectrum

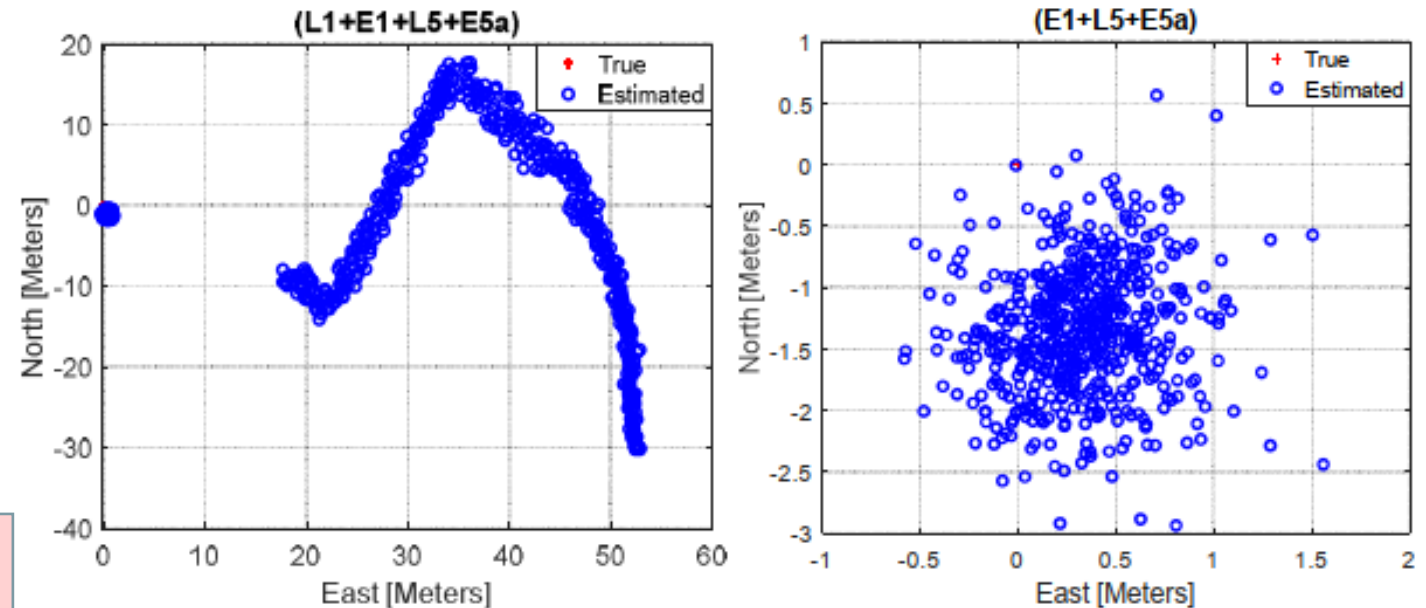
Improved  
understanding of  
threat space

# 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	$\epsilon_{3D}$	$\epsilon_H$	$\sigma_H$	$\epsilon_V$	$\sigma_V$	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



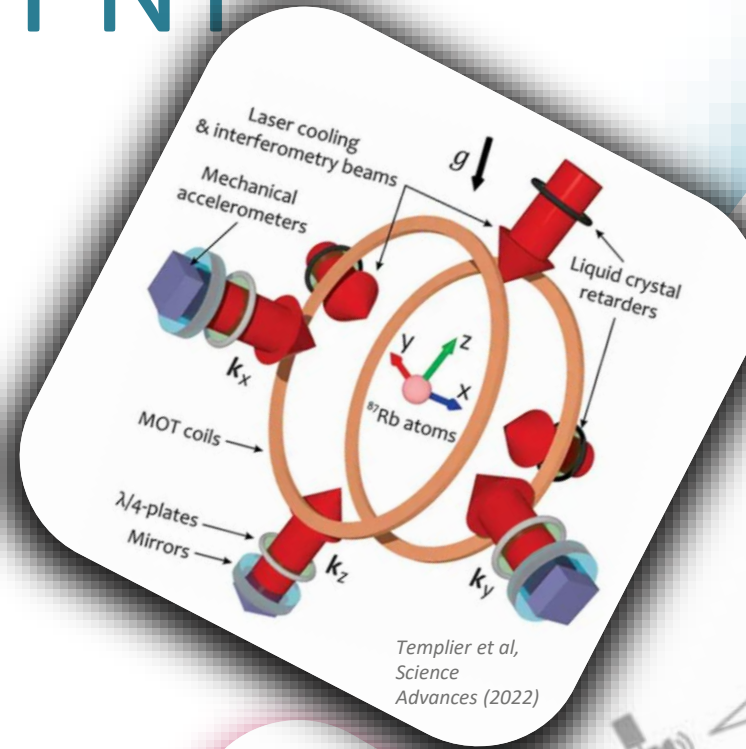
(Left): Position solution with all available constellations,  
(Right): Spoofing detection-based constellation selection for position solution with FGI-GSRx

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



# Future Trends for PNT

- GNSS still is an excellent system!
  - Ease of use
  - Cost efficiency
  - Precision
- Authentication services
  - **OSNMA**
  - PRS
  - Chimera
- Sensor fusion and system of systems approach
- **Low Earth Orbit (LEO)** constellations
  - Dedicated PNT system
  - Augmenting GNSS
- Quantum Navigation







**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# PNT Authentication with Galileo Constellation



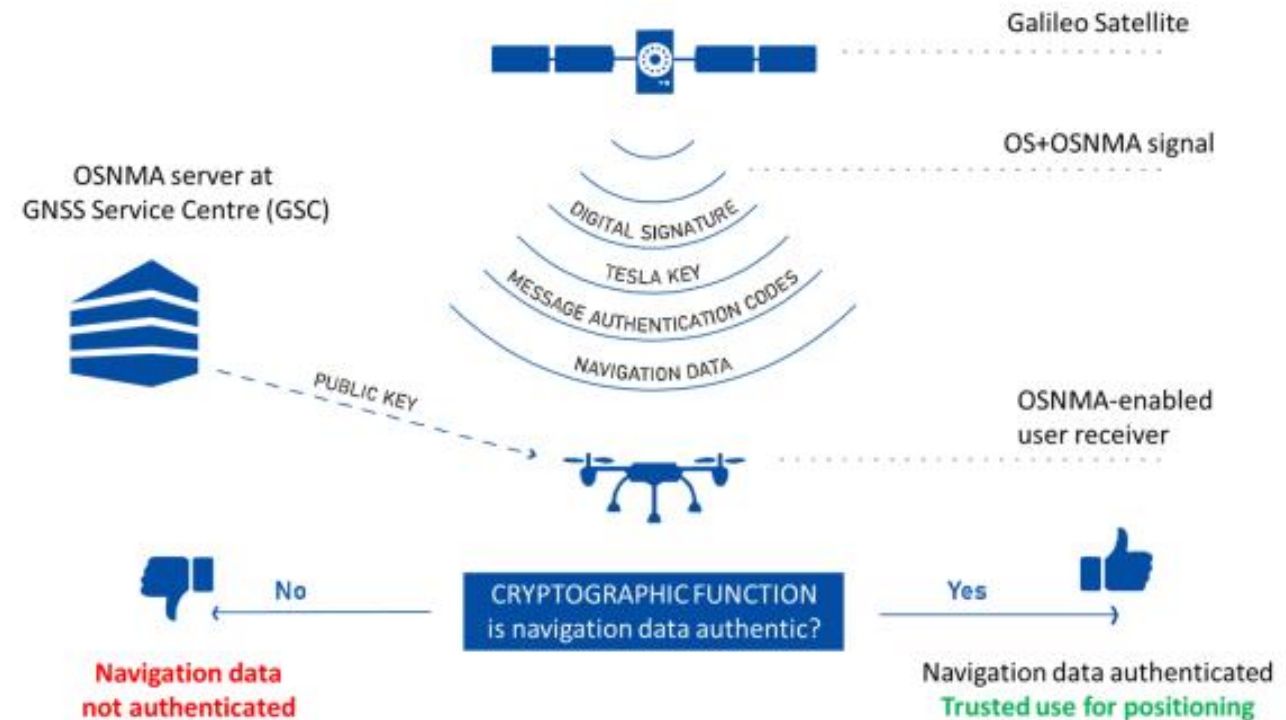
## European Galileo



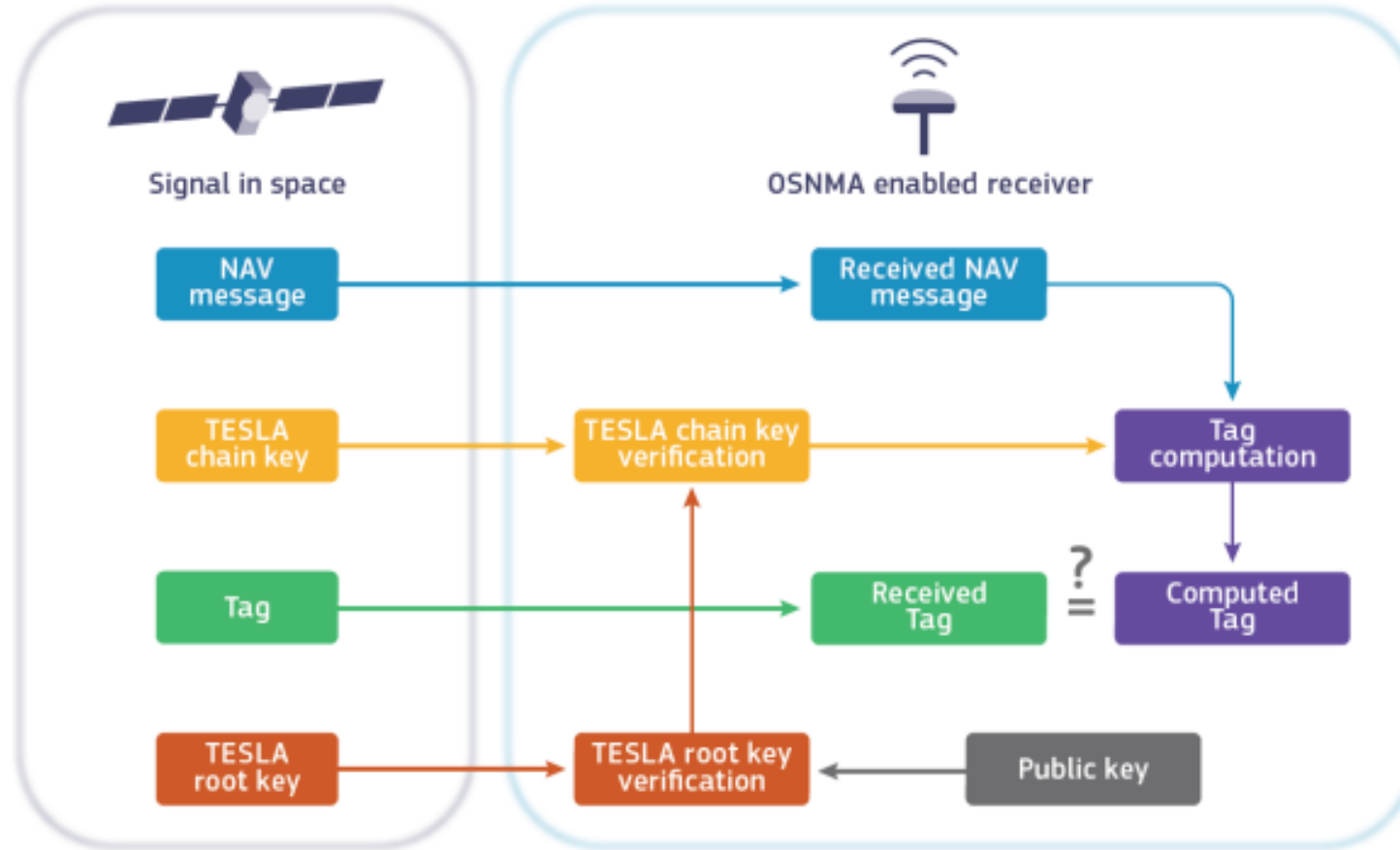
A constellation of 30 GSTB-V2 satellites (27 active and 3 spares) and their ground stations.

# Galileo Open Service Navigation Message Authentication (OSNMA)

- A new feature of the Galileo Open Service which enables users to verify that the navigation data at the receiver.
- OSNMA relies on the transmission of cryptographic information I/NAV message on E1B component.
- **OSNMA initial service was declared operational on the 24<sup>th</sup> of July 2025.**
- Galileo currently is the only constellation that offers possibility for position authentication.



# OSNMA Principle



- Navigation data are verified through the computation of a truncated Message Authentication Code (MAC), named tag, which is compared against a received tag.
- The tag is computed with a key, released after the tag. To ensure the timely reception of OSNMA data, time synchronization to GST is required.
- The key is part of a TESLA chain, and can be used to derive previous keys, as the TESLA root key.
- The TESLA root key is verified with a public key through a digital signature algorithm.

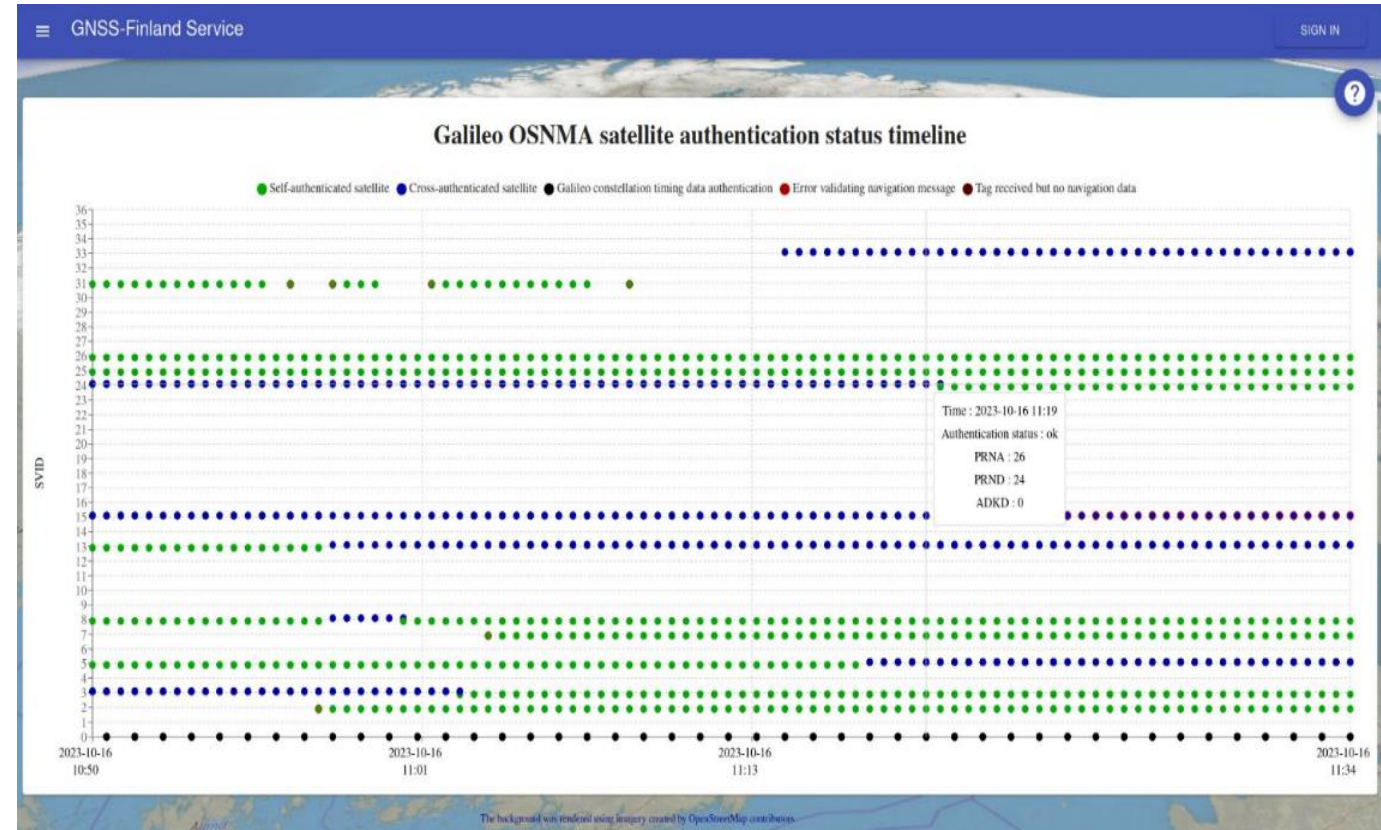


# FGI-OSNMA

FGI has made an open source OSNMA implementation called FGI-OSNMA.

The goal of FGI-OSNMA is to serve as a flexible and easily integrable OSNMA implementation, usable in both research tasks and production server environments.

FGI-OSNMA in GNSS-Finland service and utilization of FGI-OSNMA with RTKLIB to perform authenticated positioning.



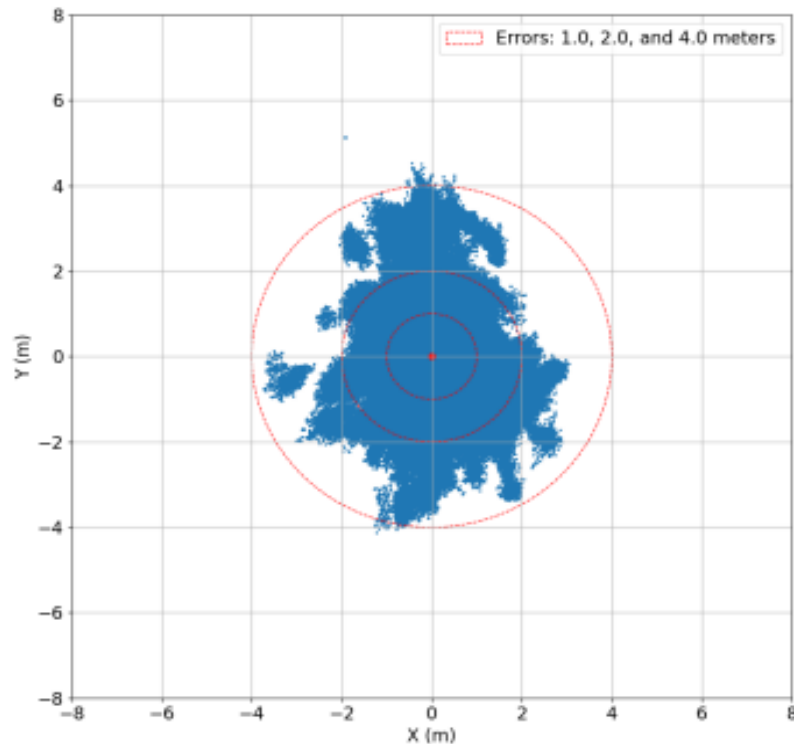
OSNMA authentication timeline in GNSS-Finland Service

Hammarberg, Toni, García, José M. Vallet, Alanko, Jarno N., Bhuiyan, M. Zahidul H., "FGI-OSNMA: An Open Source Implementation of Galileo's Open Service Navigation Message Authentication," Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023), Denver, Colorado, September 2023, pp. 3774-3785. <https://doi.org/10.33012/2023.19348>

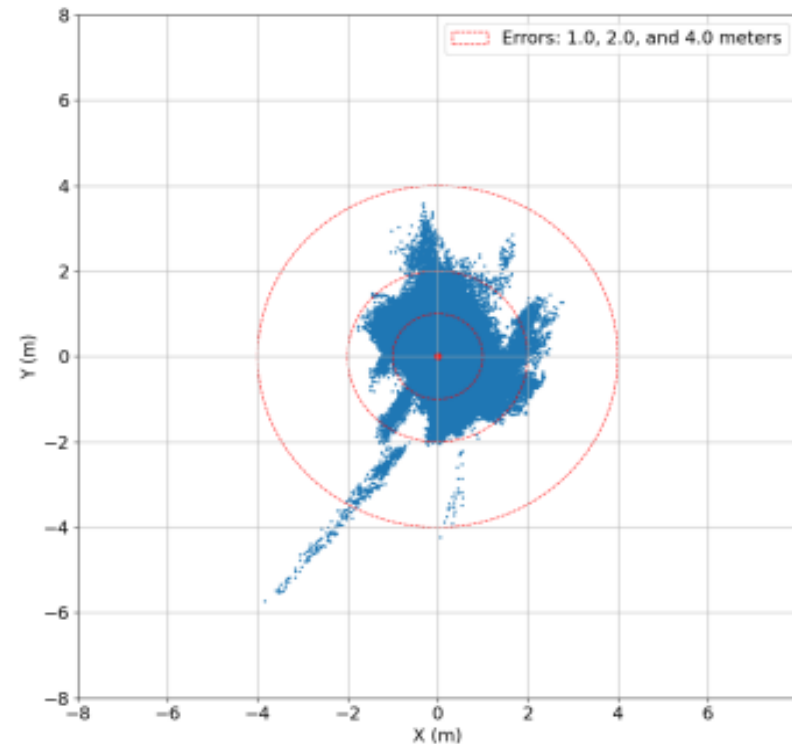
# Authenticated positioning using FGI-OSNMA

To make full use of the authentication, only Galileo E1b signal is used to compute the PVT.

The OSNMA processing is done to obtain the authentication information, filter out the unauthenticated navigation message and the corresponding observables RINEX files to obtain the PVT solution.



Unauthenticated positioning



Authenticated positioning

Hammarberg, Toni, García, José M. Vallet, Alanko, Jarno N., Bhuiyan, M. Zahidul H., "An experimental performance assessment of Galileo OSNMA," *Sensors*, 2024

# OSNMA Authentication Tags

## ADKD0

Ephemeris, clock, and status of the satellite are authenticated in each subframe (or 30 seconds (s)) delay.

- **SelfADKD0:** ADKD0 authentication of the satellite is done by itself.
- **CrossADKD0:** ADKD0 authentication of the satellite is done by some other satellite.

## ADKD12

Same information as in ADKD0 is authenticated, but there will be an additional 10 subframe (or 300 s) delay in transmitting the TESLA key needed to authenticate the tag.

- **SlowSelfAuthADKD12:** ADKD12 authentication of the satellite is done by itself.
- **SlowCrossAuthADKD12:** ADKD12 authentication of the satellite is done by some other satellite.

## ADKD4

Galileo constellation related timing information is authenticated.

# Case Studies

## Case Study 1: Authenticated Position under clean open sky scenario

- Reference:
  - 60.182°N, 24.828°E , 47.248 m
- Location: Finnish Geospatial Research Institute (FGI) office rooftop antenna in Espoo, Finland
- Galileo satellites: PRN 4, 9, 21, 31, 34, 36
- Signal duration: 460 seconds (~8 mins)

## Case Study 2: Authenticated Position in real world spoofing scenario

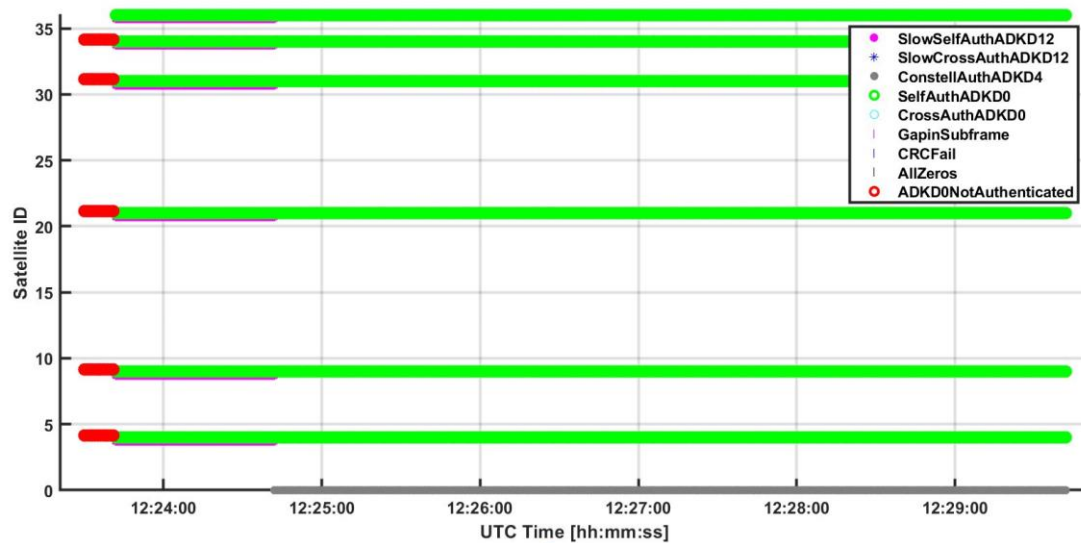
- Reference: 69.283°N, 15.998 °E
- Location: (Bleik community house parking lot), Andøya, Norway
- Galileo satellites: PRN 3, 5, 13, 15, ,24, 31
- Signal duration: 740 seconds (~12 mins)



# OSNMA based position authentication with FGI-GSRx

OSNMA Hot Start: Public Key and Root Key available at startup

## Scenario 1: Nominal open sky clean signal



Reference: 60.182°N, 24.828°E , 47.248 m

Location: FGI rooftop antenna in Espoo, Finland

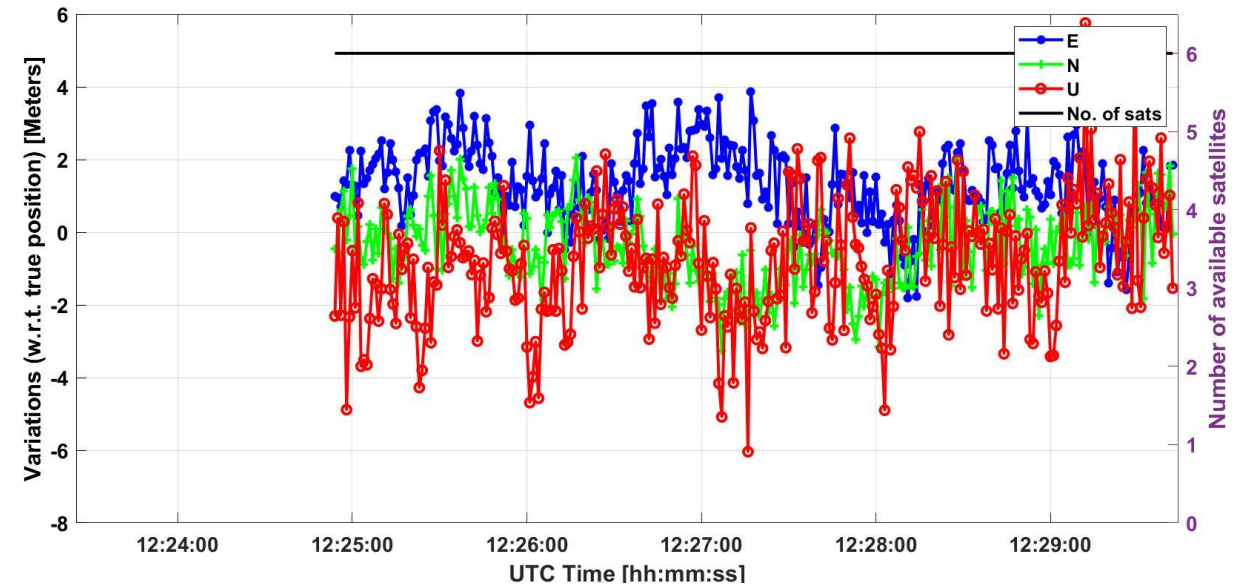
Galileo satellites: PRN 4, 9, 21, 31, 34, 36

Signal duration: 460 seconds (~8 mins)

## Live signal



	Availability (%)	$\epsilon_{3D}$	$\epsilon_V$	$\sigma_V$	$\epsilon_H$	$\sigma_H$	TTF
Auth. position	80.86	2.69	1.03	1.49	0.75	1.83	88 s
No Auth. position	100	2.68	1.45	1.14	1.84	1.73	NA



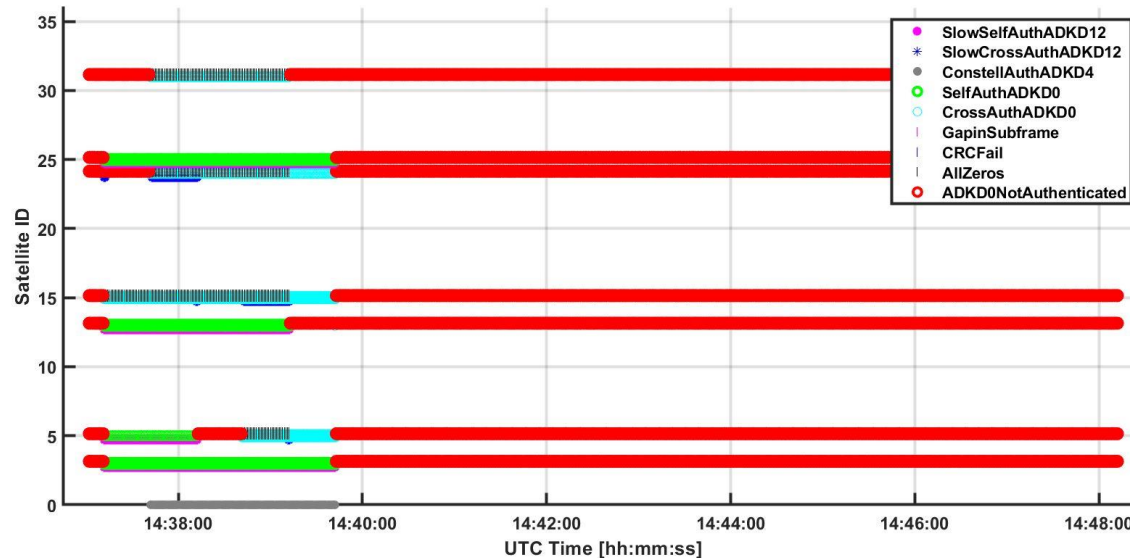
# OSNMA based position authentication with FGI-GSRx:

OSNMA Hot Start: Public Key and Root Key available at startup

## Scenario 2: JammerTest 2023 (Norway)

Dataset: 17.1.6 Simulated driving (route 1).

Spoofed Signals: GPS L1 C/A, L2C, L5 Galileo E1, E5



Reference: 69.283°N, 15.998 °E

Location: (Bleik community house parking lot), Andøya, Norway

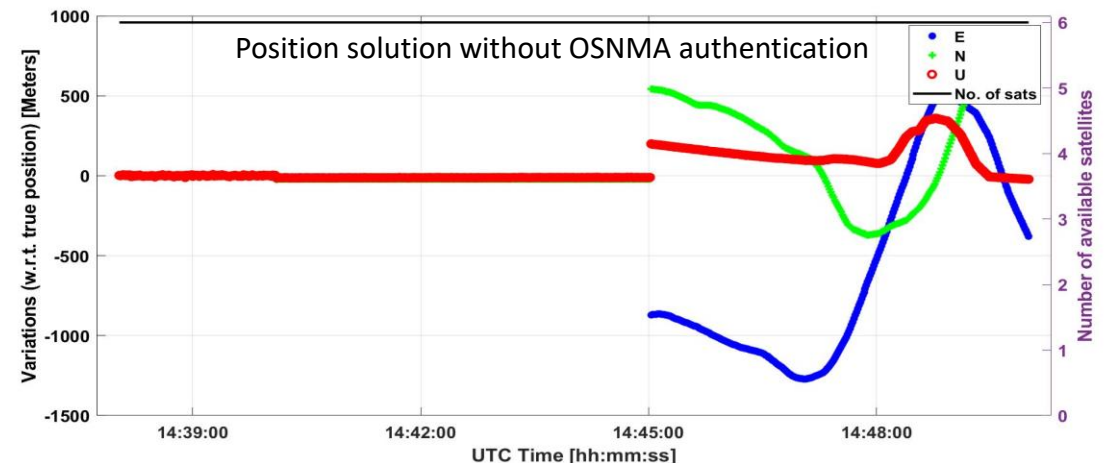
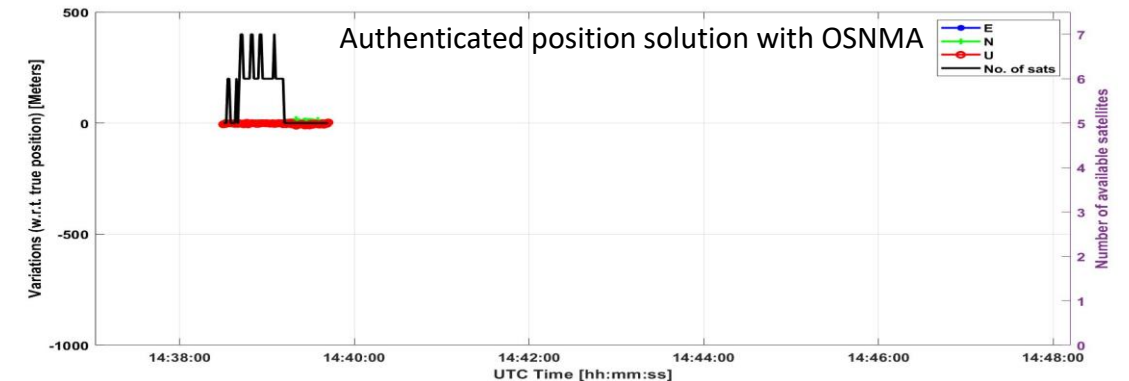
Galileo satellites: PRN 3, 5, 13, 15, ,24, 31

Signal duration: 740 seconds (~12 mins)

## Record and Relay



	Availability (%)	$\epsilon_{3D}$	$\epsilon_V$	$\sigma_V$	$\epsilon_H$	$\sigma_H$
Auth. position	16.21	4.06	2.35	2.06	0.78	0.56
No Auth. position	100	603.55	62.62	86.08	370.21	464.96



# Case Studies: FGI SpoofRepo

Reference: 60.182°N, 24.828°E , 47.248 m

Location: FGI rooftop antenna in Espoo, Finland; Signal duration: 370 seconds (~6 mins)



Scenario 1: Targeted SFMC: Galileo satellites: PRN 2,3,7,8,24,25,26,33



Scenario 2: Targeted DFMC: Galileo satellites: PRN 3,5,8,13,14,24,25,26,31



Scenario 3: Untargeted DFMC: Galileo satellites: PRN 4,9,13,24,31

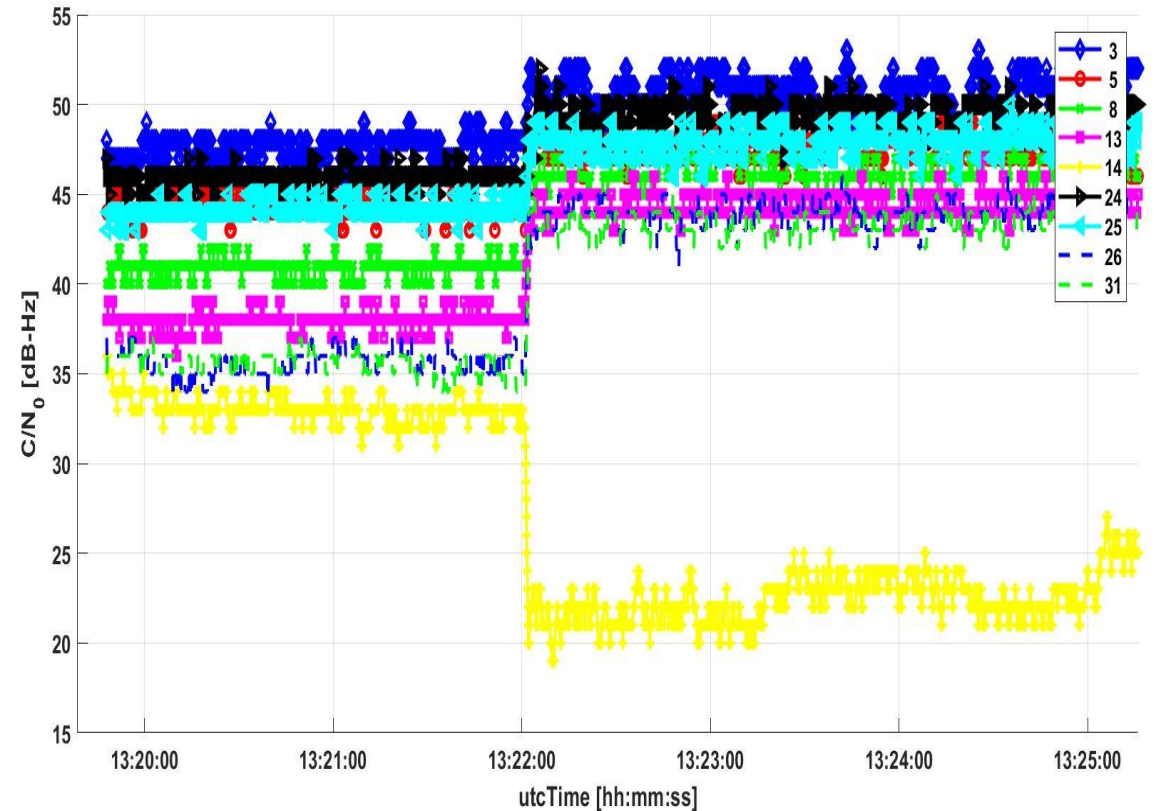
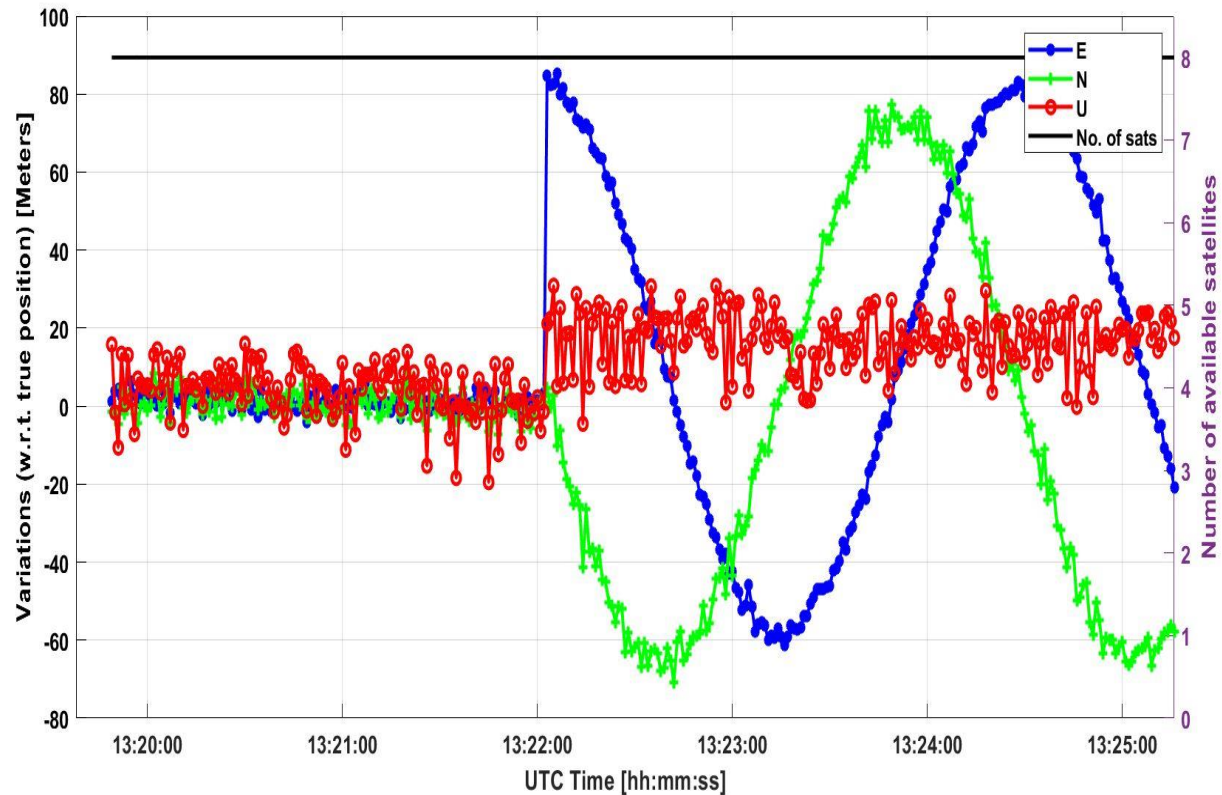


Scenario 4: Meaconing: Galileo satellites: PRN 2,3,7,8,10,12,24,25,33

# FGI-SpoofRepo: Scenario 2: Targeted DFMC

## Spoofed Signals: GPS L1 C/A, L5 Galileo E1, E5

OSNMA Hot Start: Public Key and Root Key available at startup



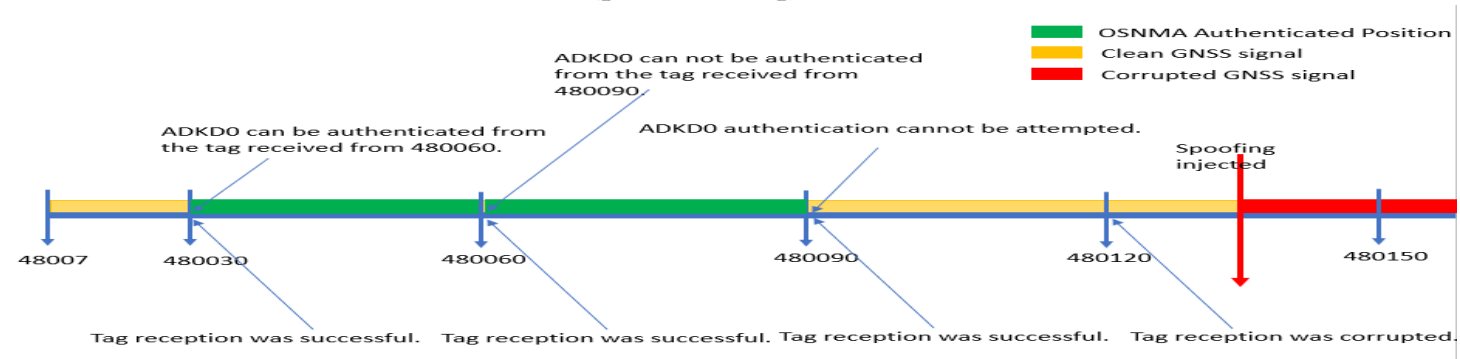
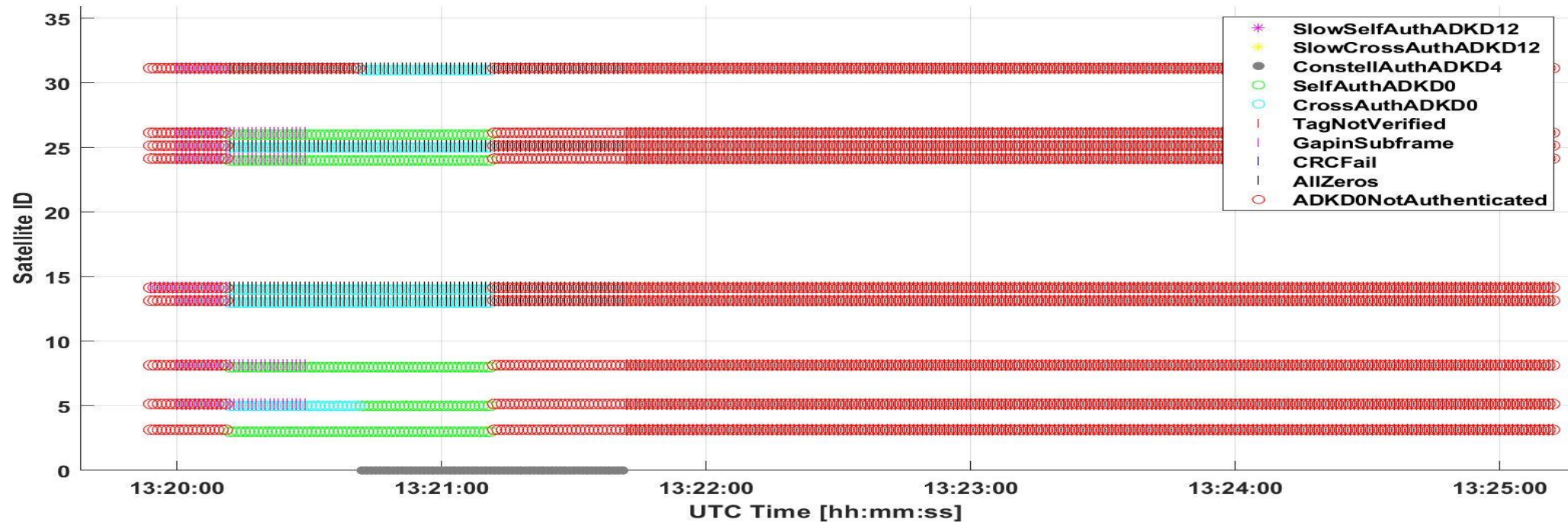
Liaquat, M., Bhuiyan, M. Z. H., Hammarberg, T., Islam, S., Saajasto, M., & Kaasalainen, S. (2025). An End-To-End Solution Towards Authenticated Positioning Utilizing Open-Source FGI-GSRx and FGI-OSNMA. *Engineering Proceedings*, 88(1), 58. <https://doi.org/10.3390/engproc2025088058>.



# FGI-SpoofRepo: Scenario 2: Targeted DFMC

## Spoofed Signals: GPS L1 C/A, L2C, L5 Galileo E1, E5

OSNMA Hot Start: Public Key and Root Key available at startup

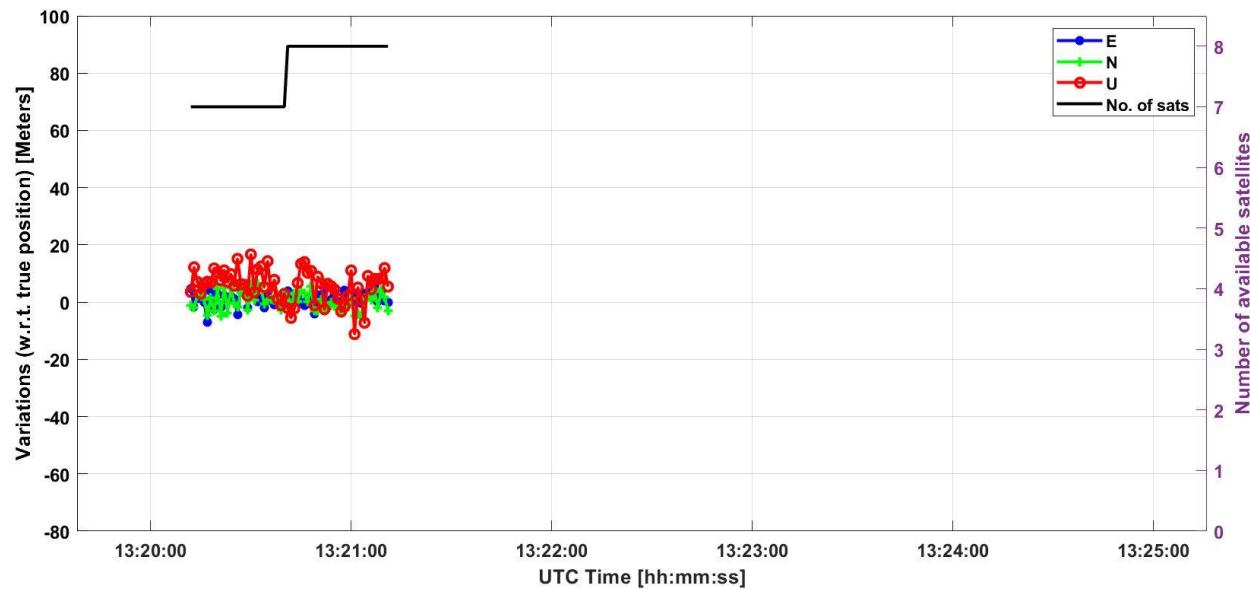


# FGI-SpoofRepo: Scenario 2: Targeted DFMC

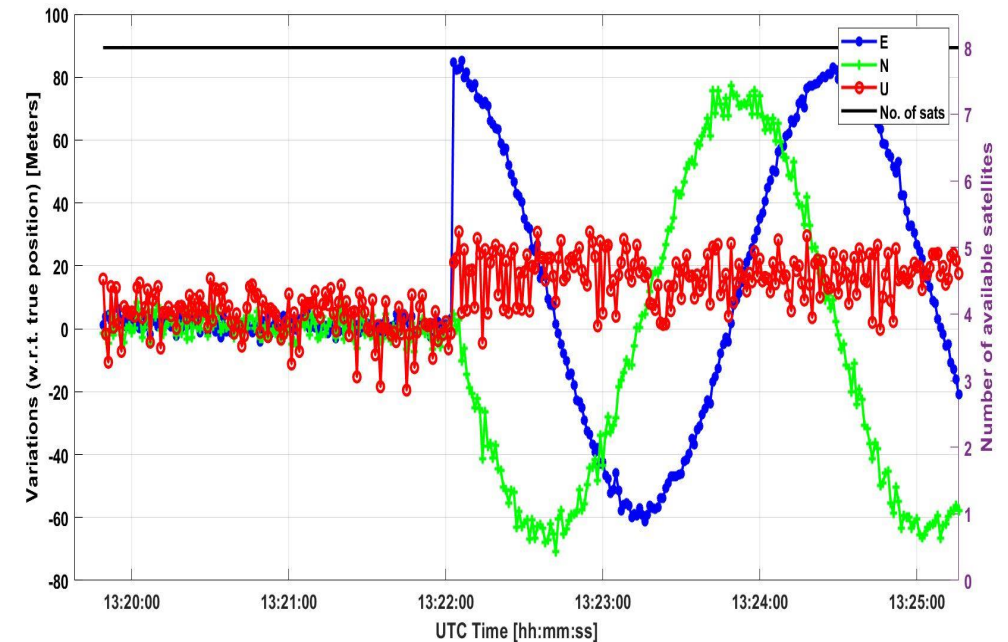
## Spoofed Signals: GPS L1 C/A, L2C, L5 Galileo E1, E5

OSNMA Hot Start: Public Key and Root Key available at startup

	Availability (%)	$\epsilon_{3D}$	$\epsilon_V$	$\sigma_V$	$\epsilon_H$	$\sigma_H$
Auth. position	16.21	7.06	5.85	2.20	3.17	0.83
No Auth. position	100	57.52	45.01	32.29	13.38	7.99



Authenticated position solution with OSNMA

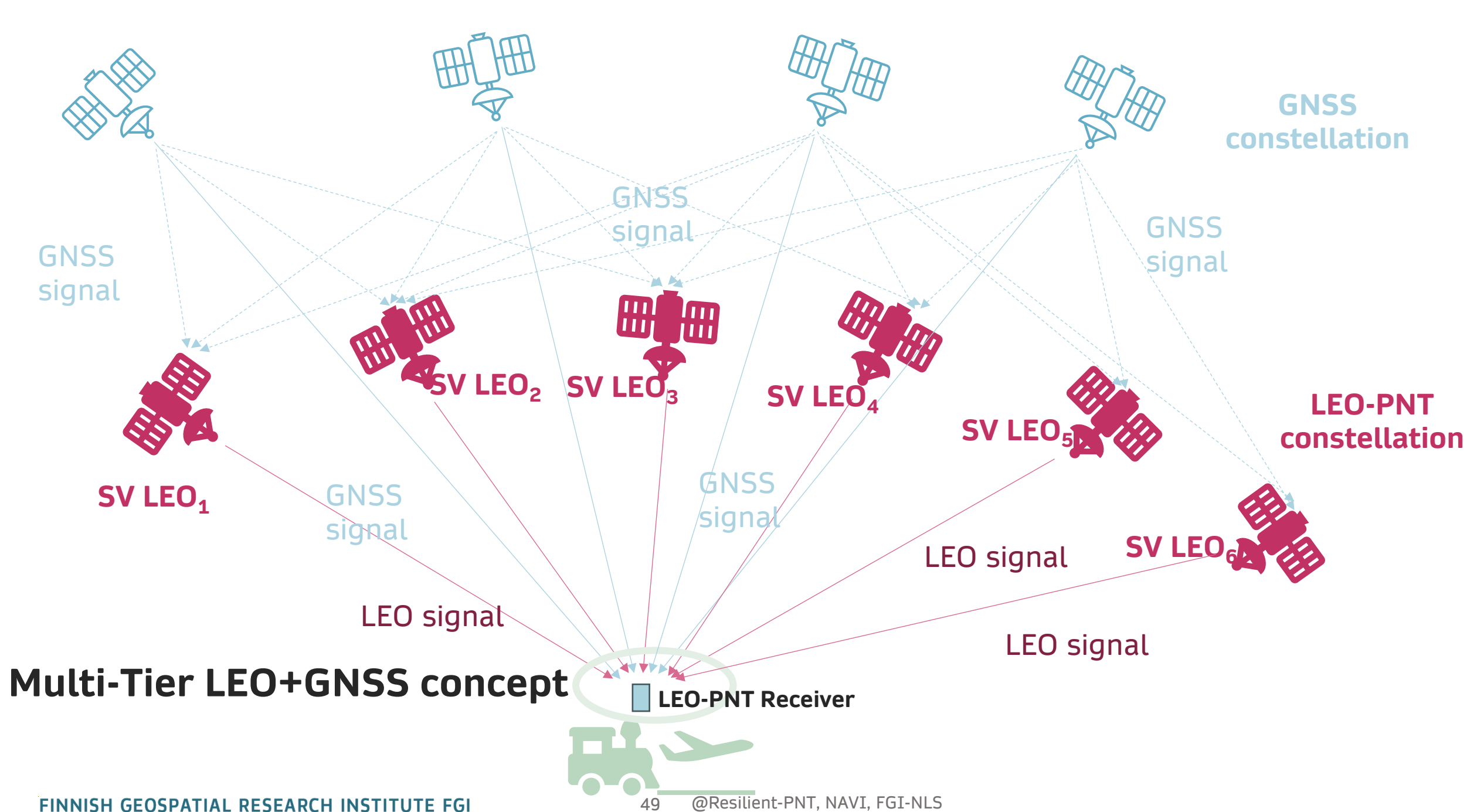


Position solution without OSNMA authentication



**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

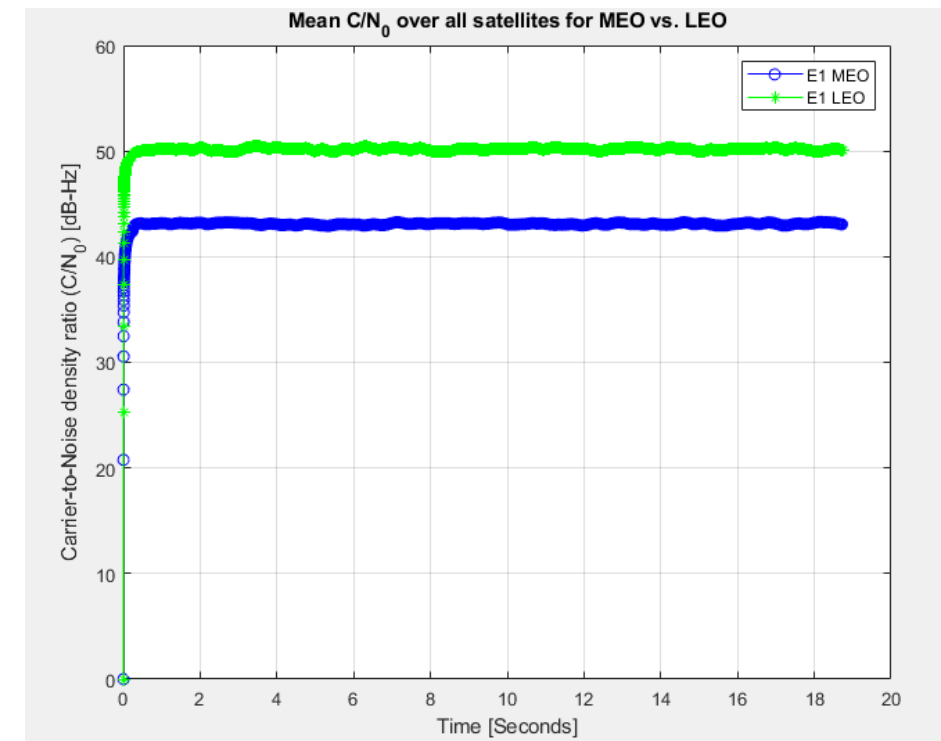
# The new Frontier for PNT: Low Earth Orbit (LEO)





# Signal Strength, MEO vs. LEO

- Depending on the allowed received signal power on a specific frequency band, LEO-PNT receivers are expected to offer **>10 dB or more improvement** over MEO GNSS receivers.
- **Stronger signals:** The proximity of LEO allows for much stronger signals compared to classical GNSS.
- **Enhanced tracking accuracy:** New spectral allocations for broadband communication or dedicated hosted PNT payload may enable wider bandwidth and higher chip-rate signals, potentially improving tracking accuracy.



C/N<sub>0</sub>s are averaged across all MEO satellites vs. all LEO satellites

# Introducing LEO-based PNT Solutions (1)

- Why Low Earth Orbit (LEO) ?  
=> Advantages over MEO (e.g., faster Doppler shifts, stronger signals, global reach)



Methods: e.g. Multi-Tier LEO-GNSS, Doppler-based positioning, TDOA  
Challenges: clock synchronization, signal access, regulation

# Introducing LEO-based PNT Solutions (2)

Dedicated	Network-aided	Fused	Opportunistic
<p>LEO constellation or hosted payloads solely dedicated to PNT (e.g., Xona, TrustPoint).</p> <p><b>High deployment cost (constellation of SVs or hosted payloads)</b></p> <p>Mid-term</p> <p>~Decimeter accuracy</p> <p>&lt;10 second fix</p> <p><b>Expensive to make independent of traditional GNSS</b></p>	<p>Network of 3<sup>rd</sup>-party reference receivers provides corrections that unlock PNT from broadband LEO.</p> <p><b>High deployment cost (network of reference receivers)</b></p> <p>Near-term</p> <p>&lt;1 meter accuracy</p> <p>&lt;10 second fix</p> <p>Some dependency on traditional GNSS (at reference stations)</p>	<p>Fuse a secondary PNT mission with the primary communications one.</p> <p><b>Low deployment cost</b></p> <p>Near-to-mid term</p> <p><b>accuracy not known yet</b></p> <p>&lt;10 second fix</p> <p>Eventually independent of traditional GNSS</p>	<p>Exploit unmodified signals from unmodified LEOs across multiple constellations for PNT.</p> <p><b>No deployment cost</b></p> <p>Immediate-term</p> <p><b>&lt;100 meter accuracy</b></p> <p><b>&lt;15 minute fix</b></p> <p><b>Doppler-based schemes</b></p> <p><b>Do not provide accurate timing</b></p>

Source: Z.M. Komodromos, S.C. Morgan, Z.L. Clements, W. Qin, W.J. Morrison, T.E. Humphreys (2025), Network-Aided Pseudorange-Based LEO PNT from OneWeb, Proc. of IEEE/ION PLANS, Salt Lake City, US, 2025.

# Introducing LEO-based PNT Solutions (3)

Company	Country	First Launch	Launched	Frequency Band	Total Planned
Iridium	USA	2017 <sup>14</sup>	66	L	66
Xona Space	USA	2022, 2025*	1 tech demo	L	258
TrustPoint	USA	2023	2 tech demos	C	300
JAXA	Japan	-	0	C	480
ArkEdge Space	Japan	-	0	VHF	50-100
Centispace	China	2018	5 tech demos	L	190
Geely	China	2022	0	L	240
SatNet LEO	China	2024	0	L	506
ESA's FutureNAV LEO-PNT IoD	Europe	-	0	L, S, C, UHF	10 demos (up to 263)

\*) Xona Space Systems successfully launched its Pulsar-0 satellite, the first production-class satellite for its new navigation constellation, in late June 2025.

Source: FrontierSI (2024), State of the Market Report, Low Earth Orbit Positioning Navigation and Timing – 2024 Edition, available at <https://frontiersi.com.au/wp-content/uploads/2025/01/FrontierSI-State-of-Market-Report-LEO-PNT-2024-Edition-v1.1.pdf>



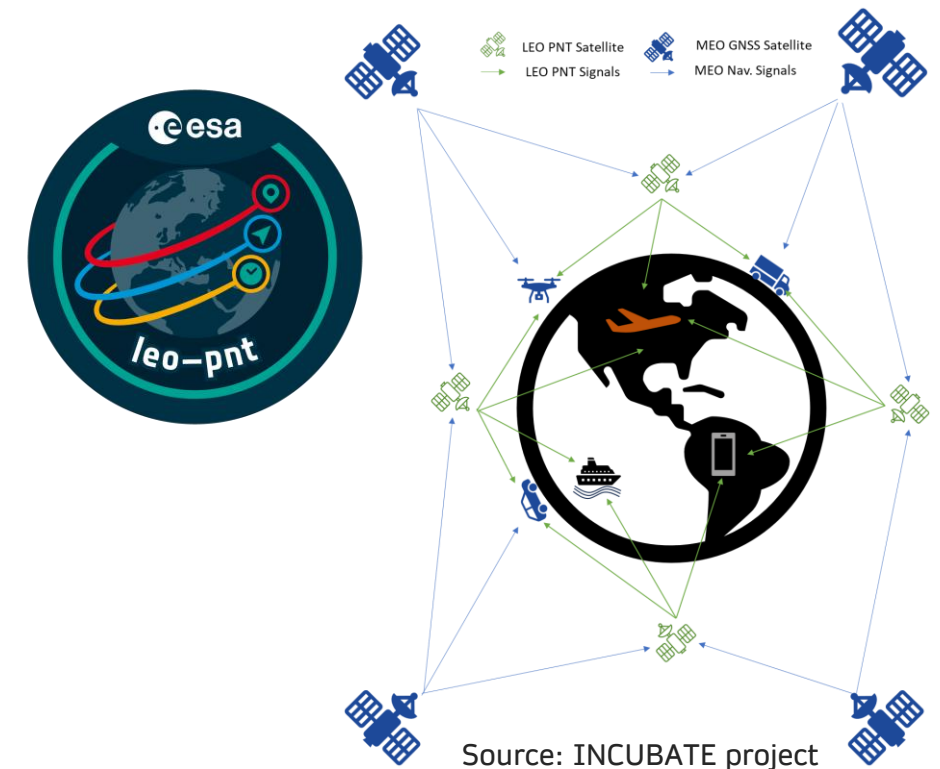
# Dedicated LEO-PNT Solution

- Characteristics of LEO satellite constellations

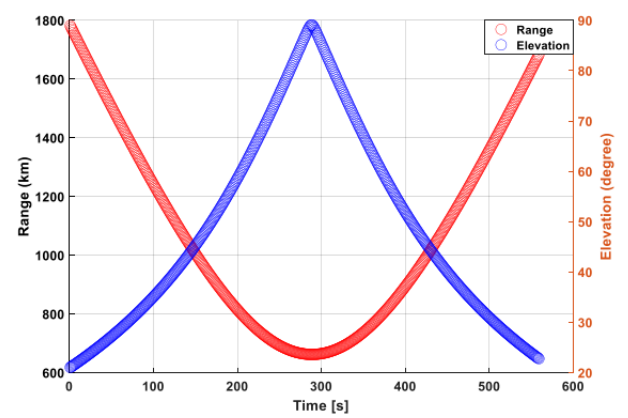
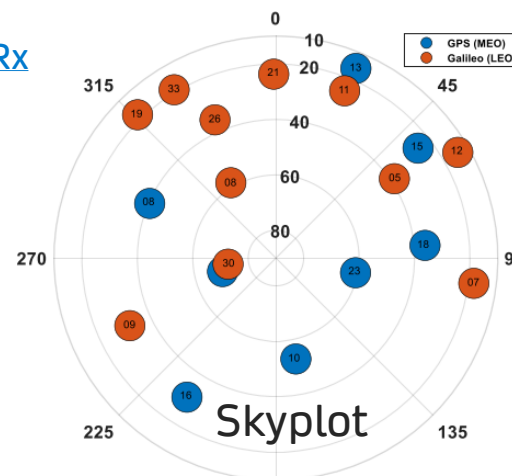
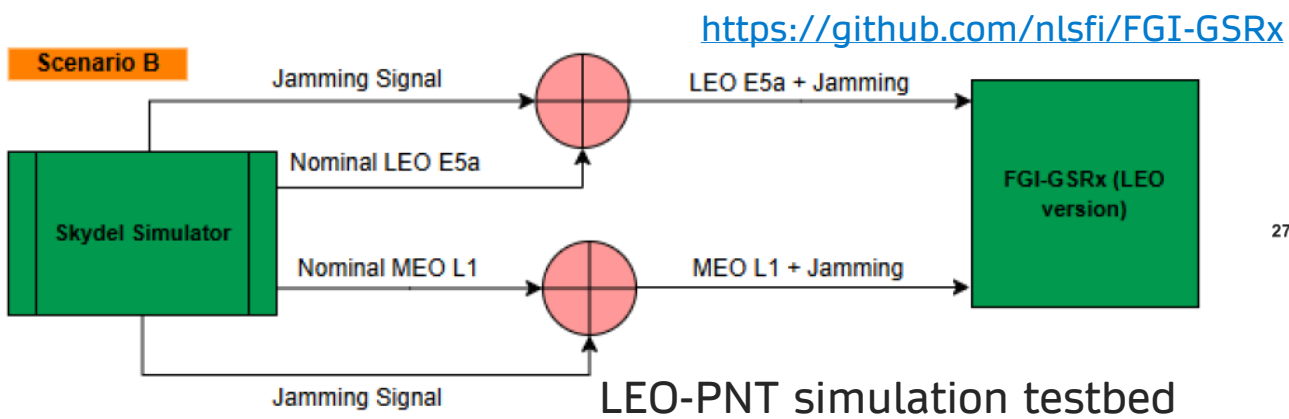
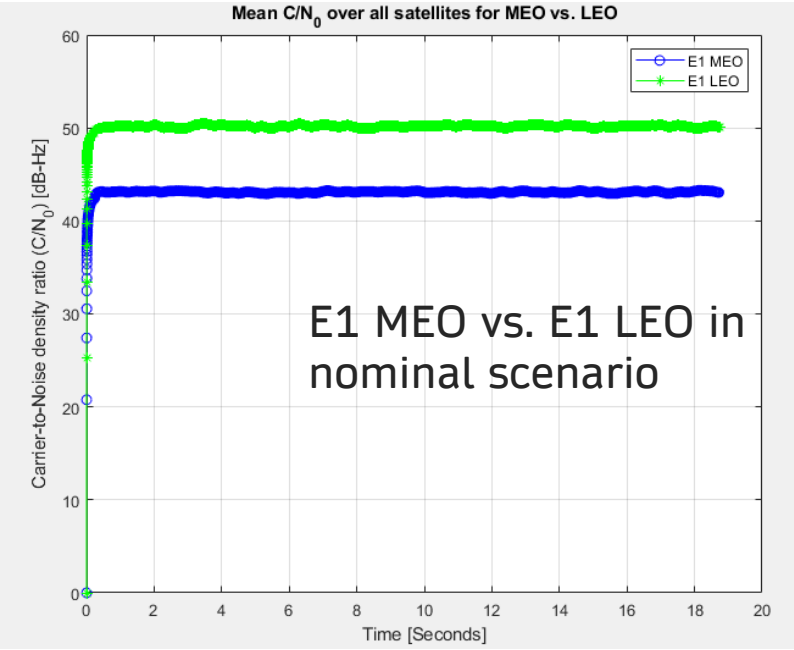
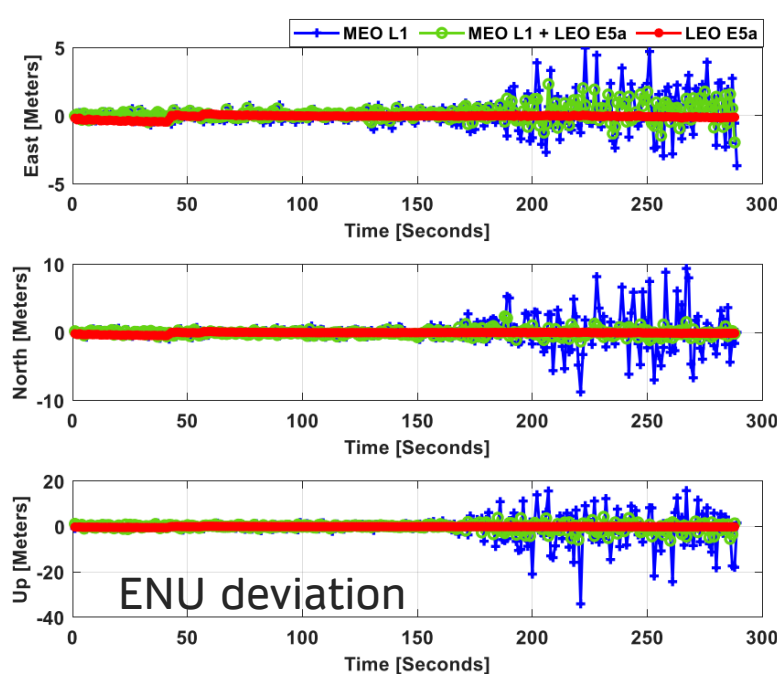
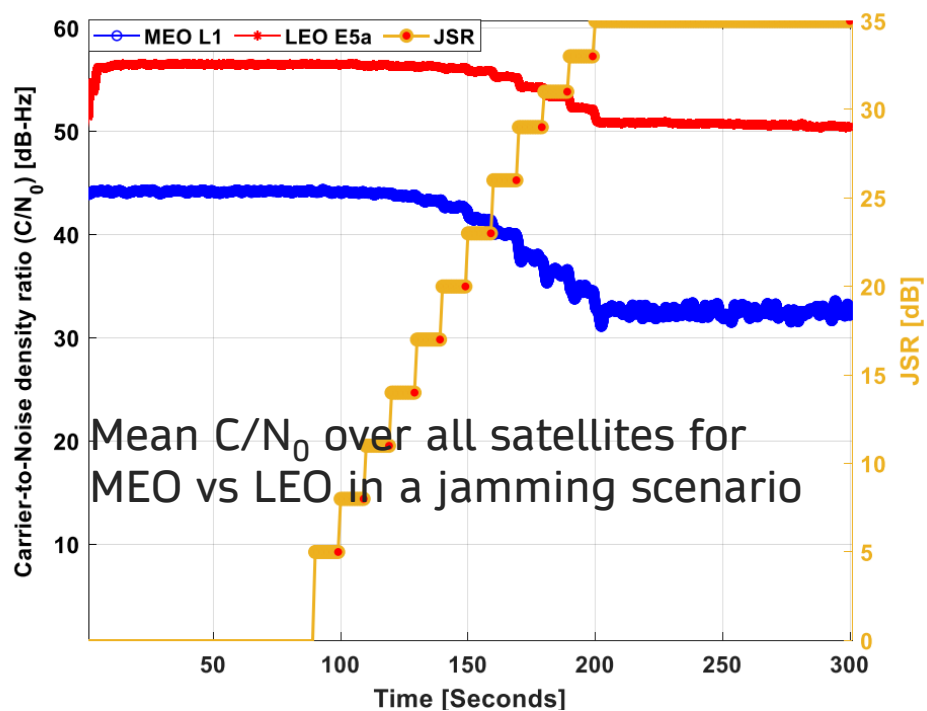
- ⇒ Larger constellations with rapid revisit times
- ⇒ Faster speed and lower latency
- ⇒ Inter Satellite Links (ISL)
- ⇒ Multi-beam transmission possibility
- ⇒ **Resilience and robustness in PNT service**
  - ⇒ Higher signal strength and lower proximity
  - ⇒ Handful options from a variety of players:
    - ⇒ **Frequency diversity: UHF, L, S, C bands**
      - ⇒ GNSS-like signal characteristics are expected from L & S bands
    - ⇒ **Both private and public service providers**
    - ⇒ **Added layer of encryption already at the signal level**
    - ⇒ Faster response to interference

- ⇒ **A hacker would need to wipe out a wide range of frequencies with higher transmission power for a complete GNSS-like disruption**

- **Key systems and initiatives:** Xona, Centispace, TrustPoint, FutureNAV, and other regional initiatives



# Resilience Expectation from LEO-PNT Receiver



# Challenges with Dedicated LEO-PNT Solution

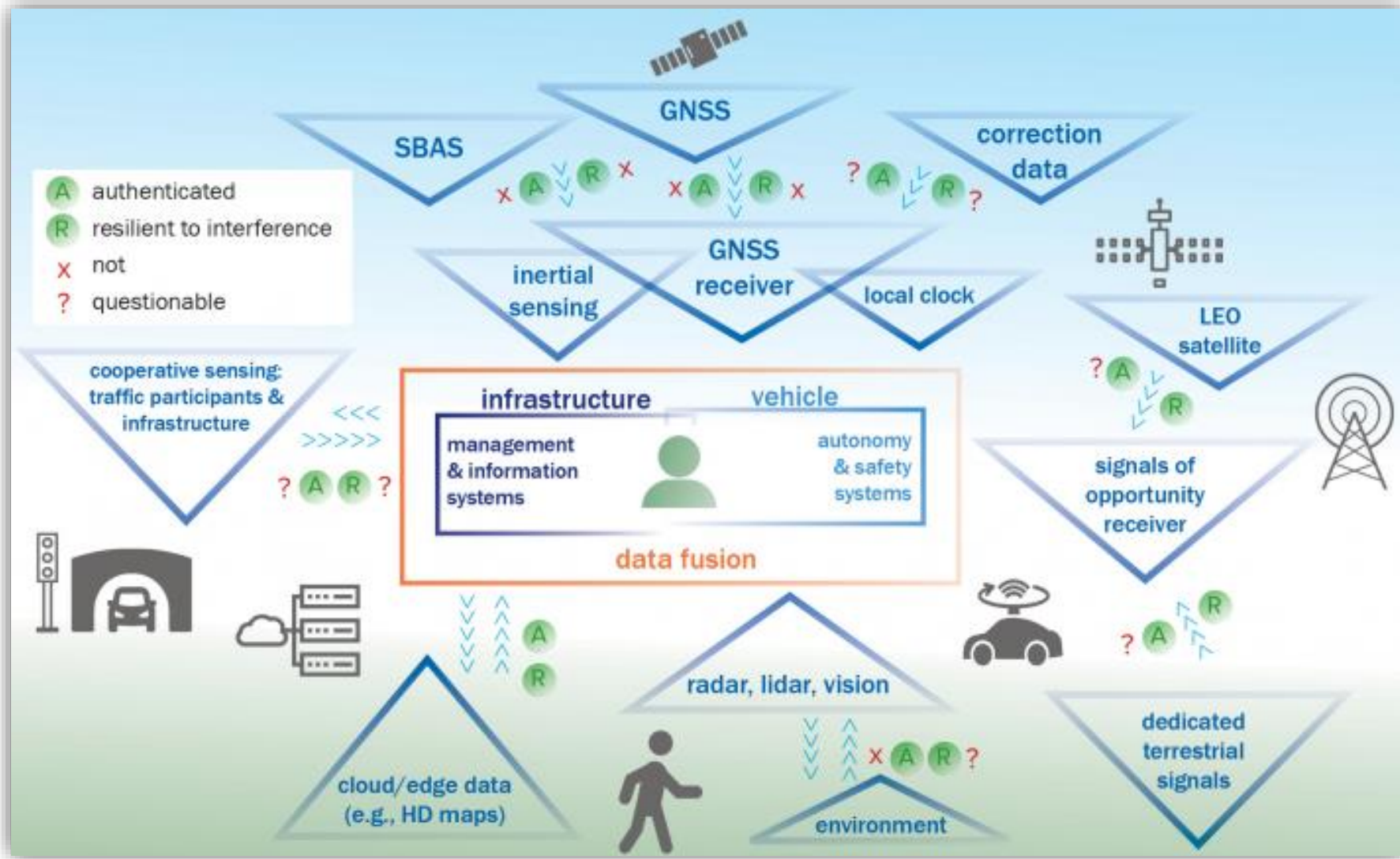
- **Actual LEO signal reception gain** will depend on **the defined reference received signal power level on that frequency band**, respecting guidelines from **ITU to also protect signals in adjacent frequency bands**.
- **Signal-level encryption** will make it impossible/**harder to spoof LEO signals**.
- Signal reception gain will improve precision; but **to achieve higher accuracy**, a variety of other challenges should be addressed:
  - **Highly accurate reference system needs to be maintained at a global scale to achieve accuracy at cm-level**
  - Impact on ionosphere: **the ionosphere correction model needs to accommodate wide variations in terms of orbit, frequency, signal propagation**, etc.
  - GNSS-derived Precise Orbit Determination (POD) for LEO:
    - ⇒ Faster speed and **higher atmospheric drag** at lower altitudes
    - ⇒ **Fast pass-over time** (e.g. 5-10 minutes) can make it challenging to broadcast navigation and correction data in time: needs to deal with **fast convergence time for Precise Point Positioning**
    - ⇒ Correction/navigation data validation duration and update rate

# Technology Trends in PNT

	CURRENT STATE	DESIRED STATE
<b>Multiplicity of PNT sources</b>	LEO-based PNT Examples: Satelles/Iridium, Xona	Next generation PNT with combined all-in effort from space and ground: LEO, MEO, GEO + SOOP (5G and beyond)
	Alternate PNT with 5G or beyond	Hybrid GNSS with 5G or beyond
	Sensor fusion with GNSS+IMU	GNSS + IoT data fusion based on ML/AI
<b>Receiver / Antenna Technologies</b>	Signal processing algorithms	Implementation of advanced interference detection and mitigation techniques
	<b>Antenna-based technologies</b>	<b>Antenna-array based processing for interference detection, localization and mitigation</b>
	Diversity	Intelligent multi-GNSS multi-frequency diversity for interference detection and mitigation



# Multi-Layer System of Systems Approach



Source: the Ohio State University's CARMEN, [Center](#) for Automated Vehicles Research with [Multimodal AssurEd Navigation](#)



**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# Recommendations on Resilient PNT

# Recommendations on Resilient PNT: 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](https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf)

# Recommendations on Resilient PNT: 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 on Resilient PNT: 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



**NLS**  
FINNISH GEOSPATIAL  
RESEARCH INSTITUTE  
FGI

# EUSIPCO Student Challenge 2025

## Detection, Localization and Mitigation of Noise-like Jamming via Phased Array Signal Processing

Matias Mikkonen<sup>1,2,\*</sup>, M. Zahidul H. Bhuiyan<sup>1,3</sup>, Daniele Borio<sup>4</sup>, and Veli Hytönen<sup>1,2</sup>

<sup>1</sup>Finnish Geospatial Research Institute (FGI)


<sup>2</sup>Aalto University

<sup>3</sup>Tampere University

<sup>4</sup>European Commission, Joint Research Centre (JRC)

\*matias.mikkonen@aalto.fi

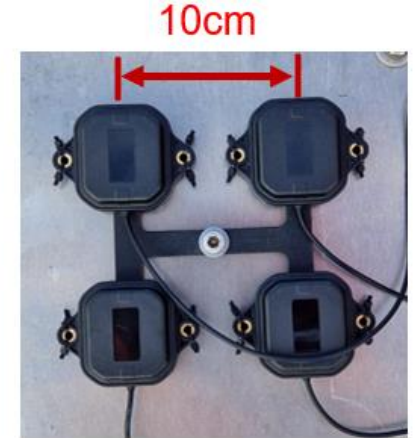
# Presentation outline

- 
- ① Background
  - ② Jamming Characterization and Detection
  - ③ Direction finding for the Jamming source
  - ④ Jamming mitigation

# Background: JammerTest 2024



- Organized by Norwegian authorities in Andøya
- Various GNSS resilience test scenarios
  - Jamming from low-power CW to high-power wideband
  - Spoofing attacks
  - Meaconing
- ESA participated in capturing data with antenna arrays



**$F_c = 1575.42\text{MHz}$**



Images courtesy of EUSIPCO 2025, ESA and David Jensen

# The Challenge

## Scenario:

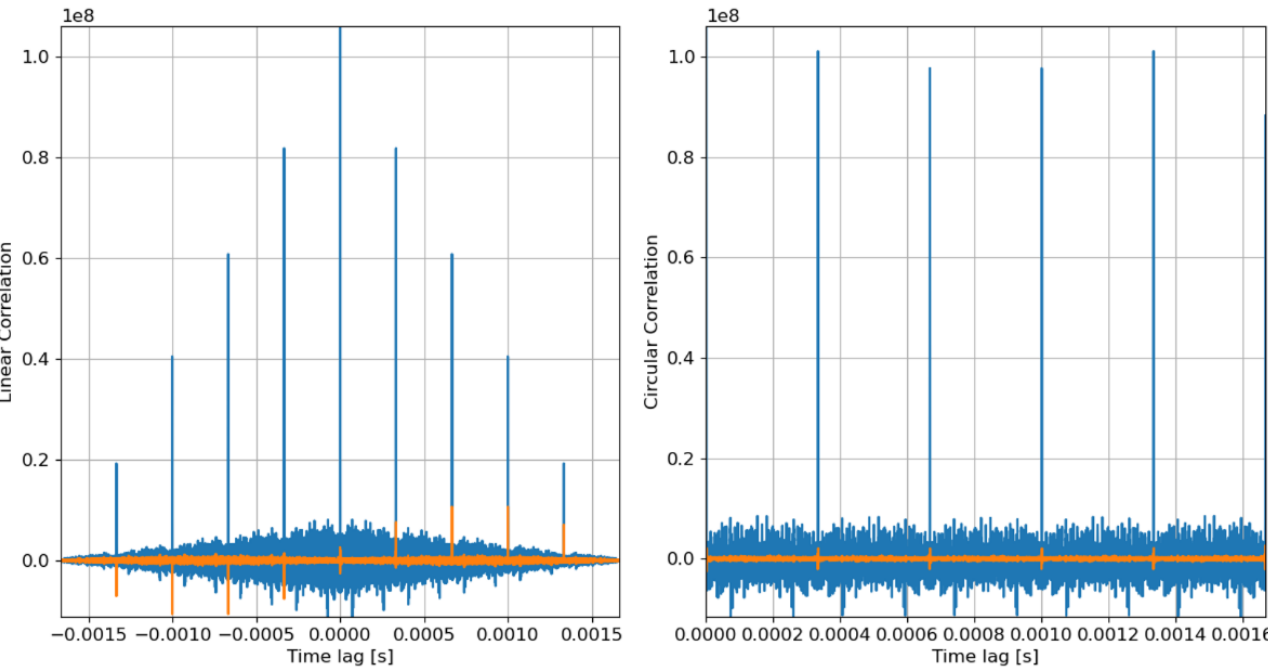
- Coherently sampled IQ data from antennas of a four-element rectangular array
- Beginning of the dataset is nominal with only GNSS signals present
- A noise-like jamming signal increases in power over time

## Objectives:

- Detection of the start time of the jamming event
- Estimation of the direction-of-arrival of the jamming signal
- Mitigation of the effects of the jamming

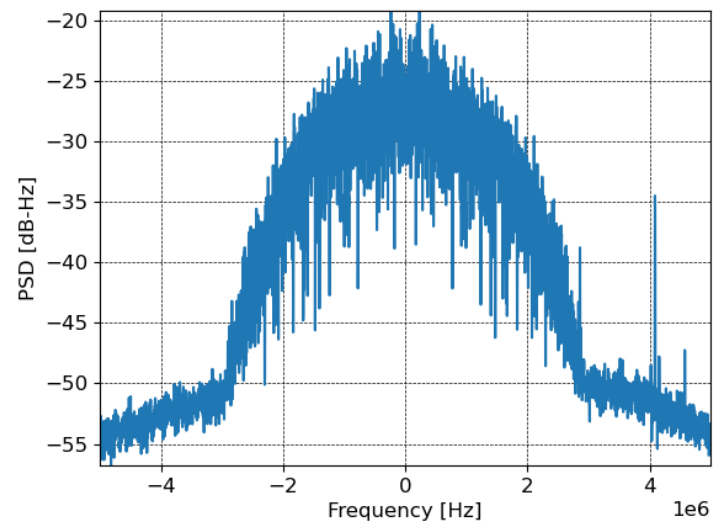


# Jamming Signal Characterization



Autocorrelation analyses show the jamming signal to be a repeating sequence with a period of 1/3 ms

Images courtesy of Dr. Daniele Borio



- PSD analysis indicates a one-sided bandwidth of approx. 3 MHz
- Jamming power approximately 35 dB above the noise floor at the end of the test

TABLE I: Characteristics of the jamming signal.

Parameter	Value
Code rate	3.072 Mchips/s
Code length	1024
Code duration	1/3 ms
Bandwidth	~ 3 MHz
Modulation	BPSK
Data	Un-modulated

# Objective 1 – Jamming Detection

- Two primary techniques were implemented:
  - Chi-square test
    - Observe sample amplitude variation from normal distribution in real-time
    - Signal-agnostic
  - Model-based detection
    - GNSS-like acquisition possible for PRN jamming
    - Feasible in post-processing

## Implementation and Performance Analysis of a Chi-square Test based GNSS Signal Anomaly Detection

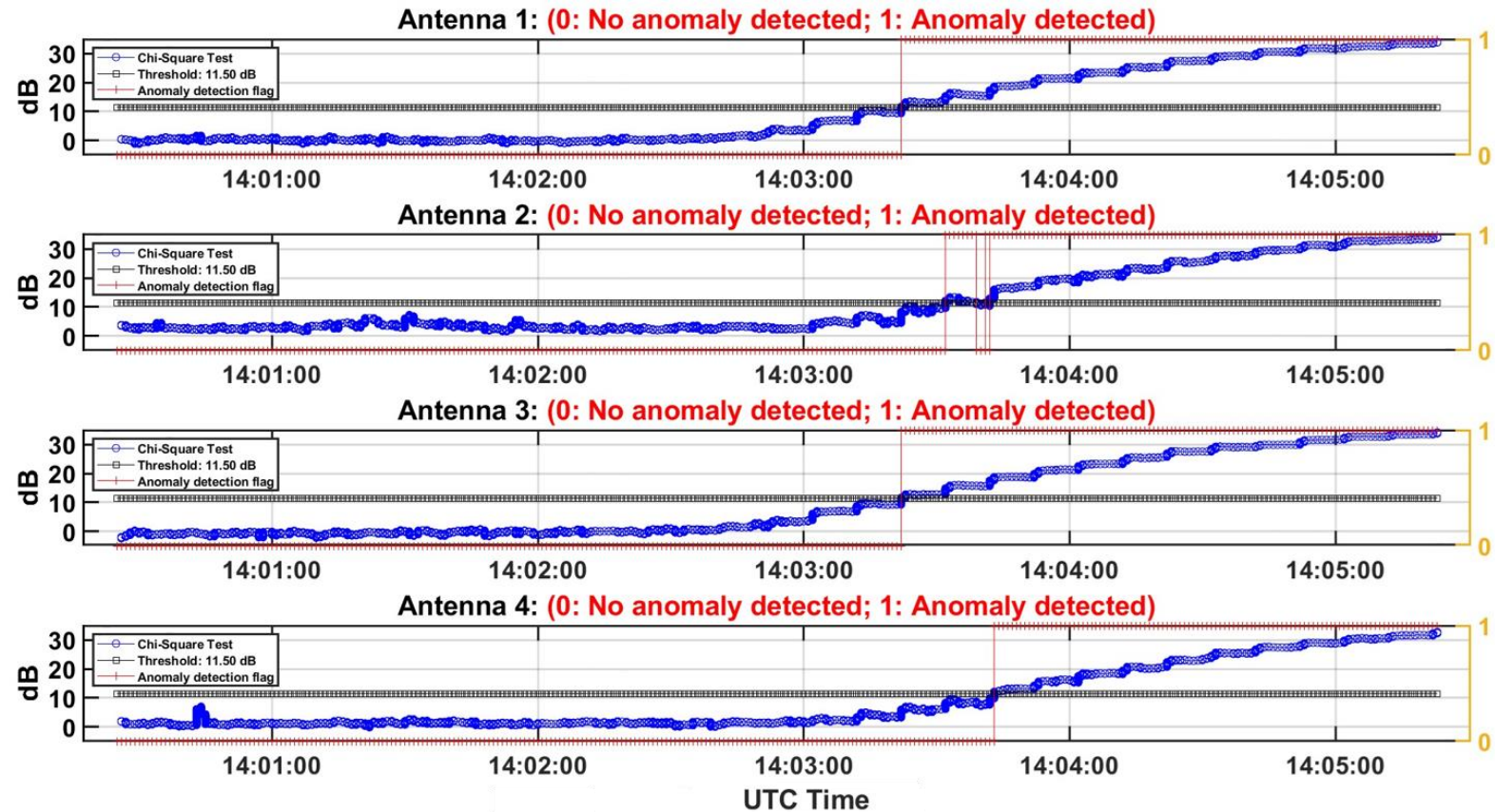
Mohammad Zahidul H. Bhuiyan<sup>\*1,2</sup>, Muwahida Liaquat<sup>1</sup>, Saiful Islam<sup>1</sup>, Into Pääkkönen<sup>1</sup>, Mika Saajasto<sup>1</sup>, and Sanna Kaasalainen<sup>1</sup>

<sup>1</sup>Department of Navigation and Positioning, Finnish Geospatial Research Institute, FGI-NLS, Espoo, Finland

<sup>2</sup>Department of Radio and Satellite Navigation, Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland

# Objective 1 – Detection of Jamming Signal: Chi-square test results (1/2)

- The Chi-square test metric indicates the presence of an anomalous signal only when it is above the noise floor



# Model-based Jamming Detection (1/2)

- Conventional GNSS acquisition and tracking loops were modified to operate with the jammer PRN
- Acquisition results at the very beginning of the dataset show that the jamming signal is always present throughout the test

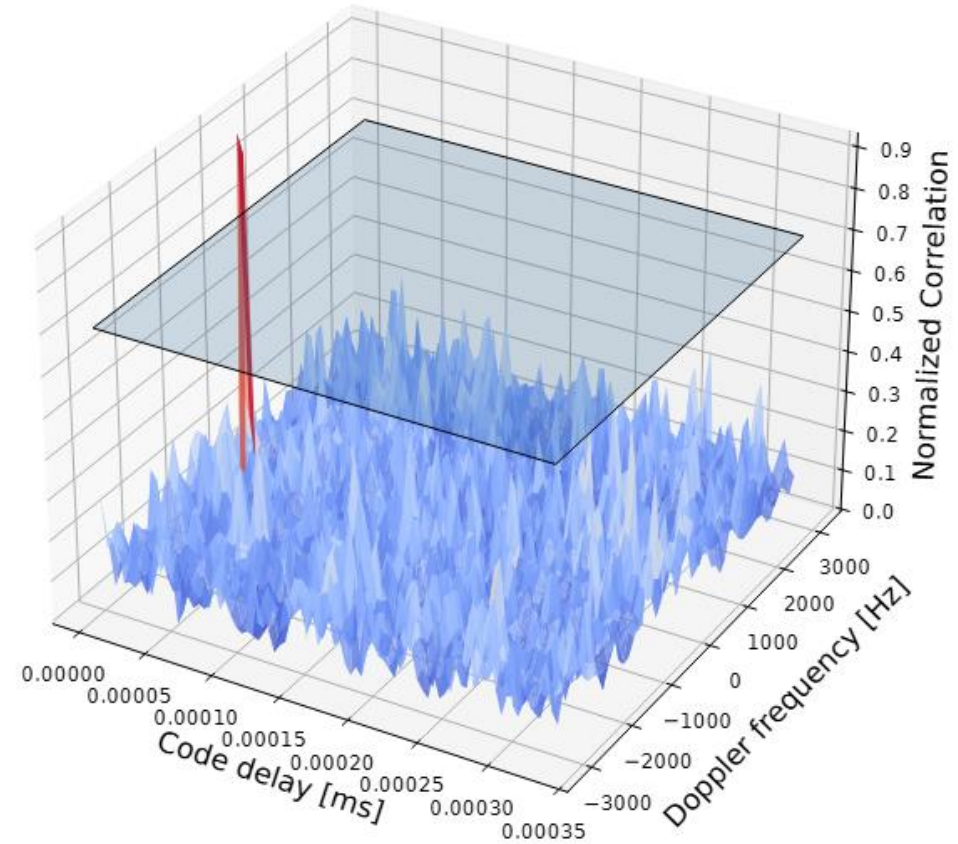
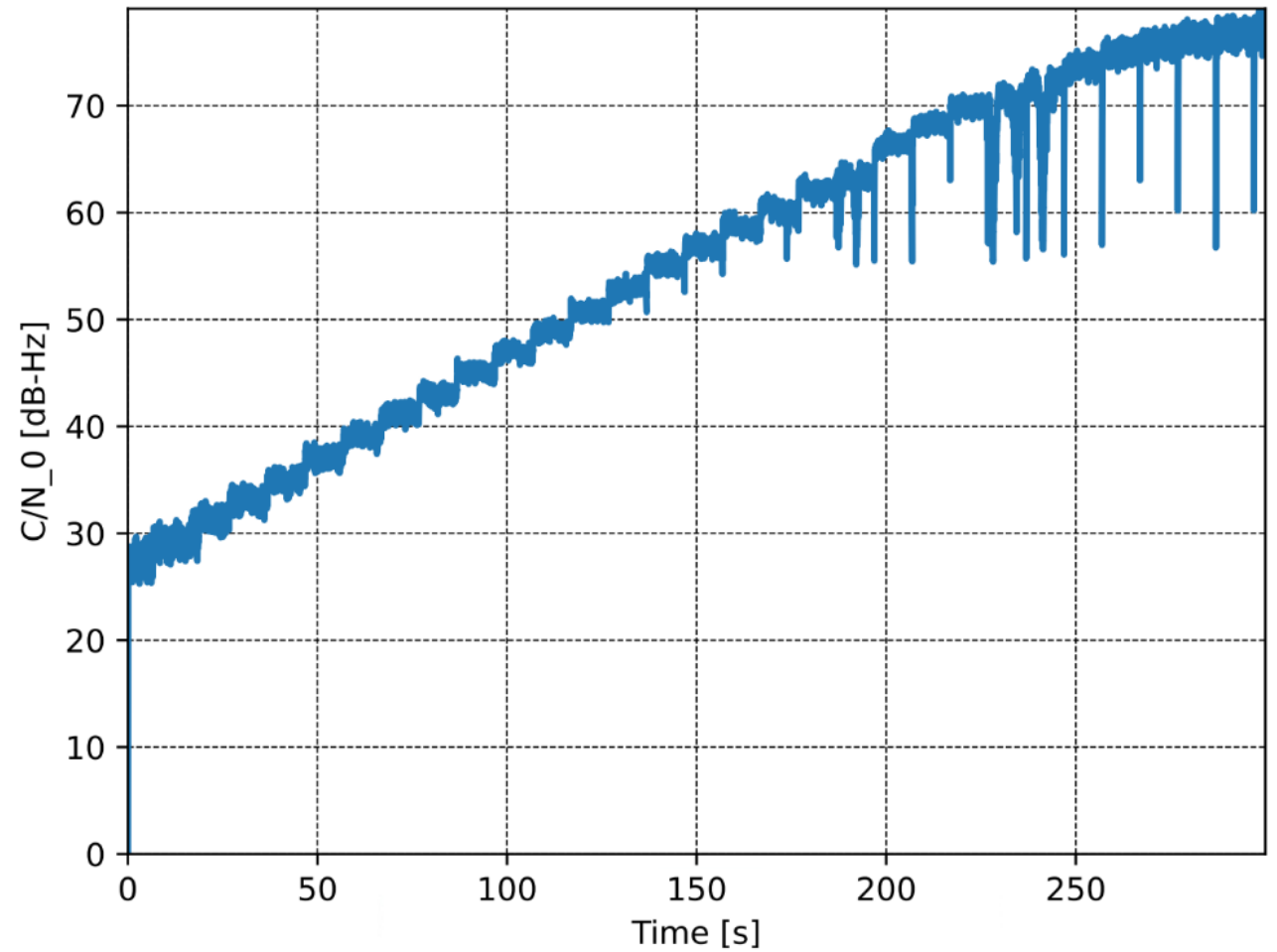


Fig. 2: CAF of the jamming signal obtained at the start of the test from a single antenna. 10 coherent and 5 non-coherent integrations.

# Model-based Jamming Detection (2/2)

- Jamming power is very low at the beginning of the dataset
- Power is increased by 2 dB every 10 seconds
- Noise floor is exceeded approximately half-way into the test

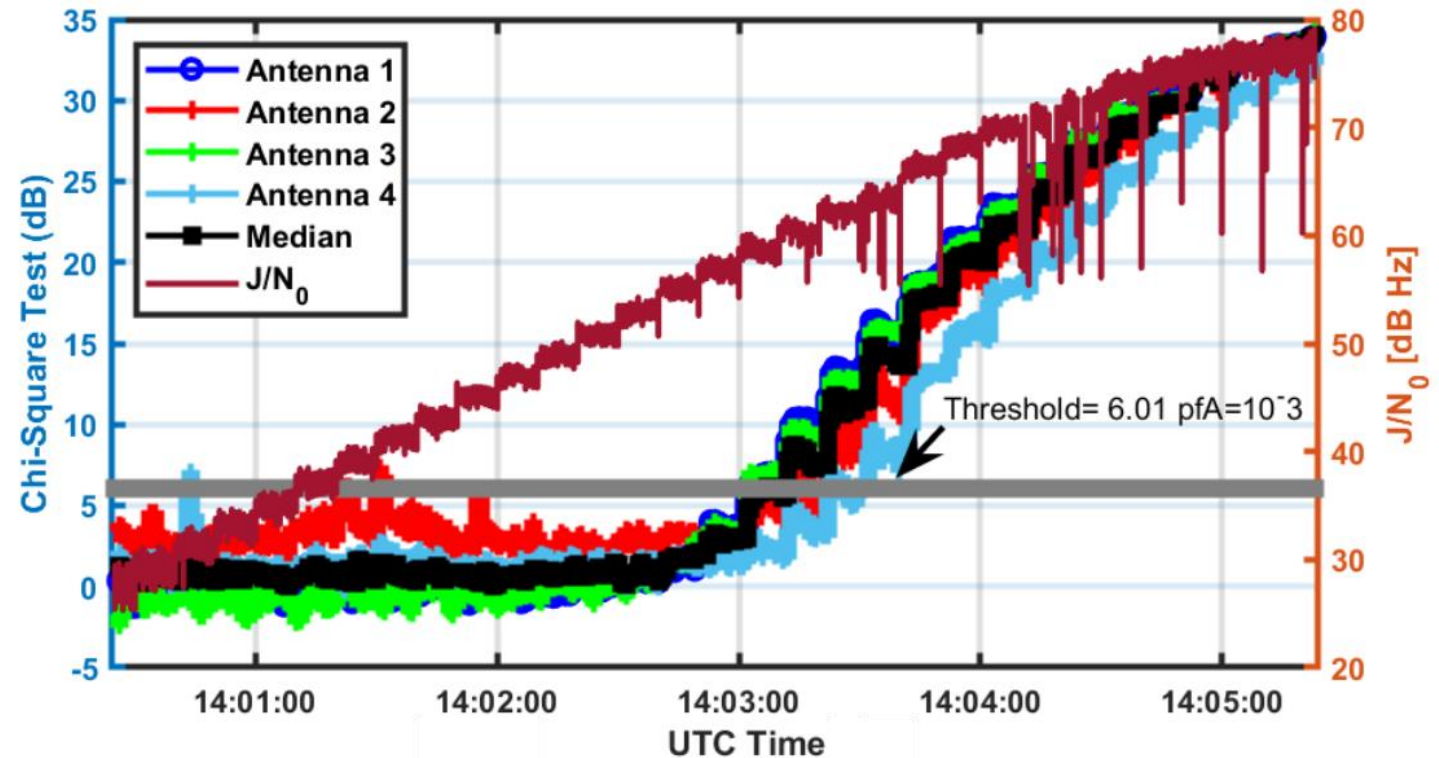


Jammer's  $C/N_0$  in dB-Hz



# Objective 1 - Conclusions

- The Chi-square test successfully detects the jamming signal after its power exceeds the noise floor – real-time detection
- Post-processing with the model-based approach reveals the presence of the jamming signal since almost the beginning of the dataset

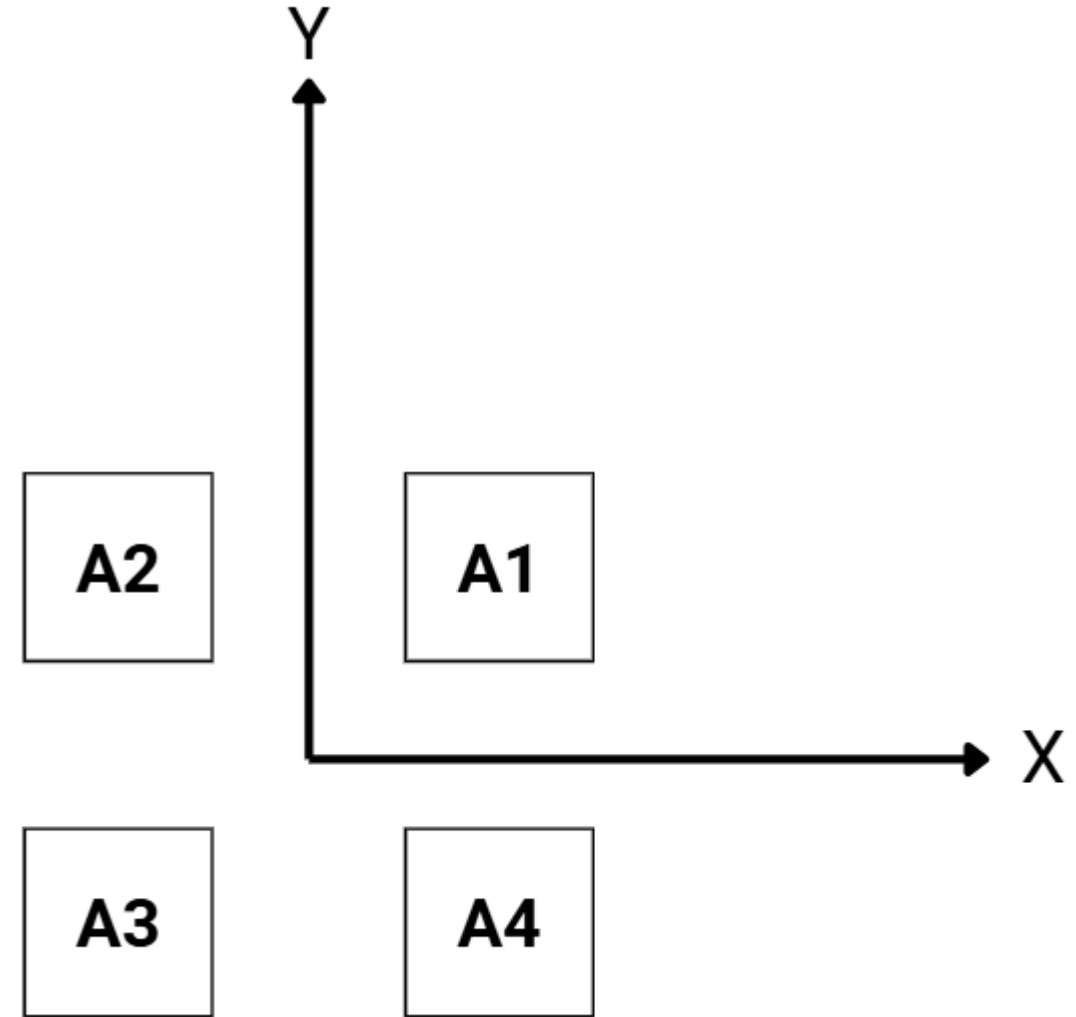


# Objective 2 – Direction Finding

- Phased array signal processing facilitates DOA analysis
  - Additional dimension to signal processing w.r.t a conventional receiver
- Three techniques were implemented:
  - Conventional beamforming
  - Multiple Signal Classification
  - Differential phase analysis of post-correlation signals
- To present results with respect to true north, a physical reference frame is required
  - Recall that the challenge dataset is provided as four IQ files without specifying location of each element within the array

# Reference Frame

- Chosen reference frame places each antenna element in the quadrant indicated by its number
- Phased array signal processing allows platform attitude estimation when known reference signals are available
  - I.e., we can infer what azimuth direction is true north in our arbitrary reference frame

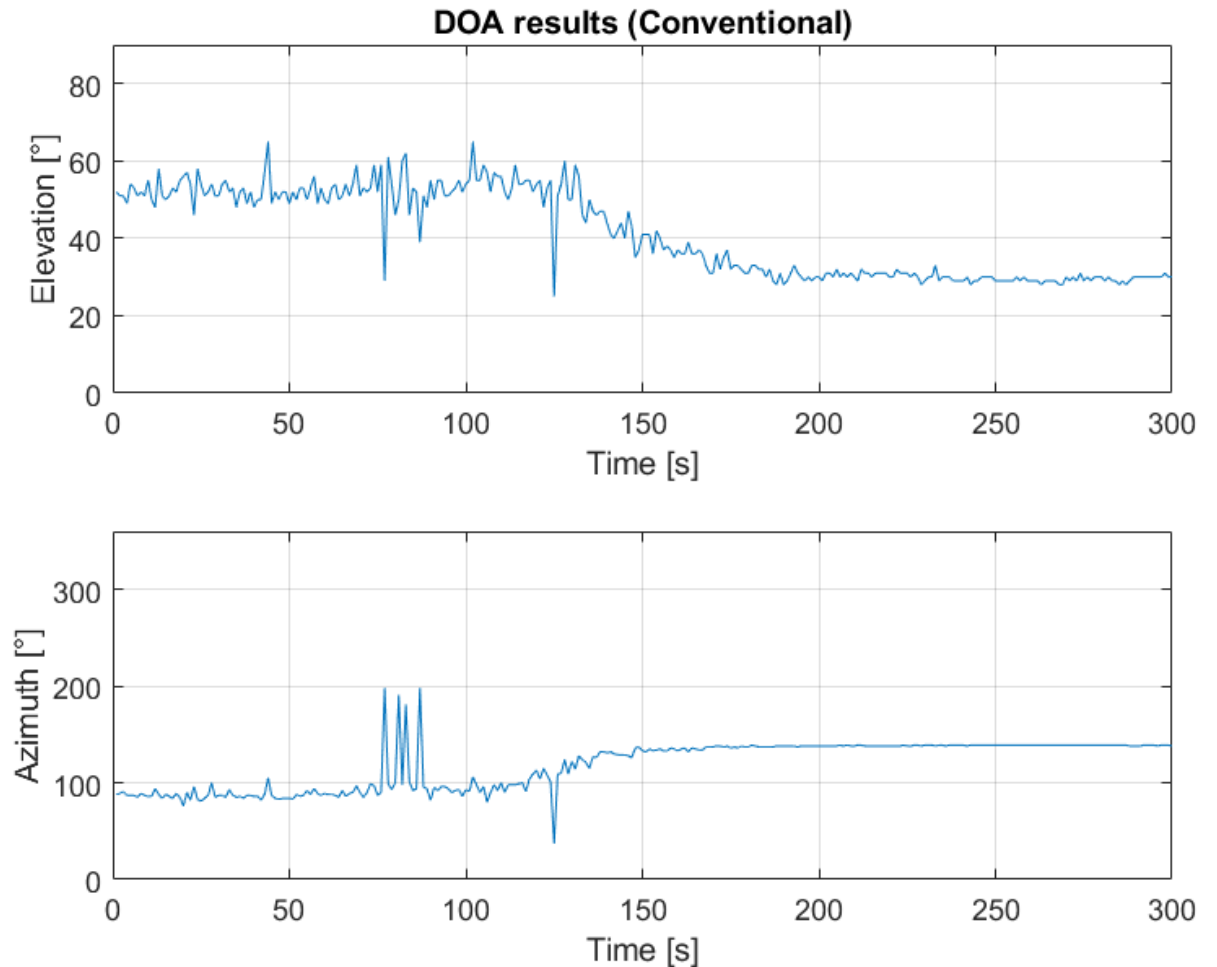


# Direction Finding – Conventional Beamforming

- The system used for data capture is an active electronically scanned array (AESA)
  - The array output is a linear combination of signals from each array element
- By adjusting the summation coefficients for each element, the array output can be biased such that signals from a particular spatial direction sum coherently
  - For a rectangular array with four elements, the direction of coherent summation is unambiguous (in the upper hemisphere)
- A direction-of-arrival estimate is obtained by steering the array main beam in each direction of a search grid and observing received power
  - The conventional beamformer DOA estimate is the direction from which highest power is received
  - Resolution is limited by the size of the array

# Results of DOA by Beamforming

- The power-measurement-based technique only produces reliable results for signals with power exceeding the noise floor
- Estimates for jammer azimuth and elevation converge near half-way into the test
- The planar array of patch antennas on a ground plane is likely insensitive to signals from low elevations
  - True elevation can be lower than estimated
  - No array characterization available





# Direction Finding – MUSIC

IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, VOL. AP-34, NO. 3, MARCH 1986

## Multiple Emitter Location and Signal Parameter Estimation

RALPH O. SCHMIDT, MEMBER, IEEE

- 1. Compute the covariance matrix of received signals

$$\vec{R}_s = \frac{1}{N_s} \vec{S} \vec{S}^H$$

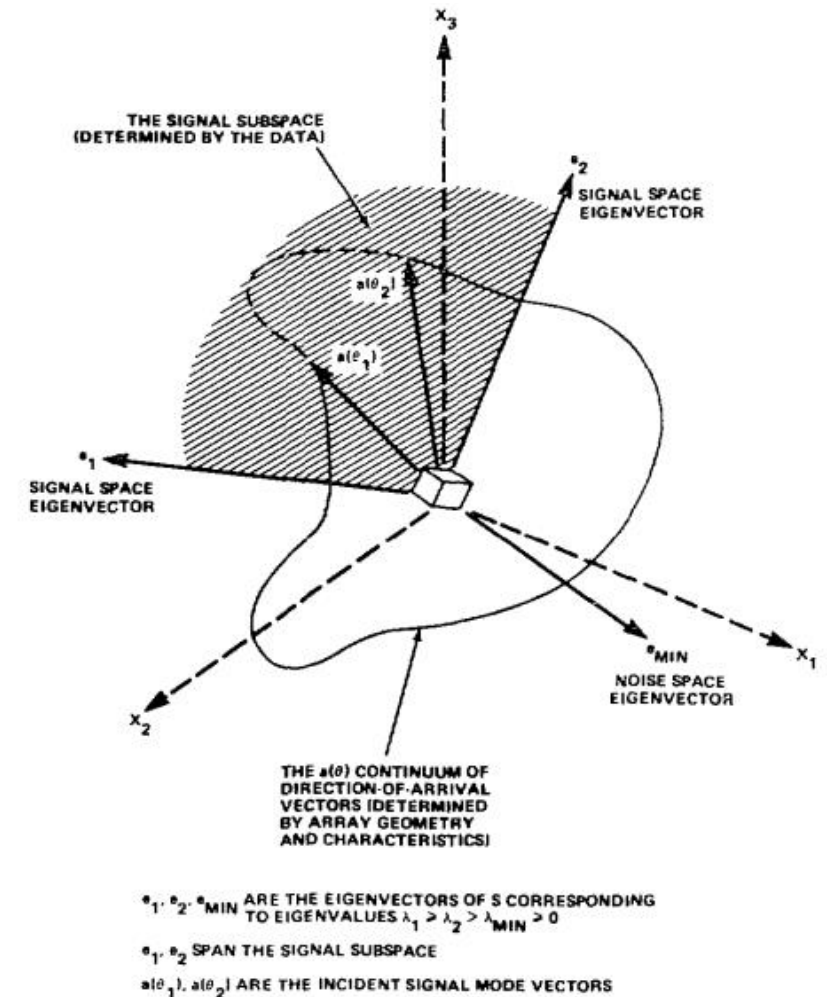
- 2. Perform eigenvector decomposition

- Eigenvectors corresponding to the largest eigenvalues span the signal subspace
- Those corresponding to the remaining eigenvalues span the orthogonal noise subspace

- 3. Compute MUSIC pseudospectrum

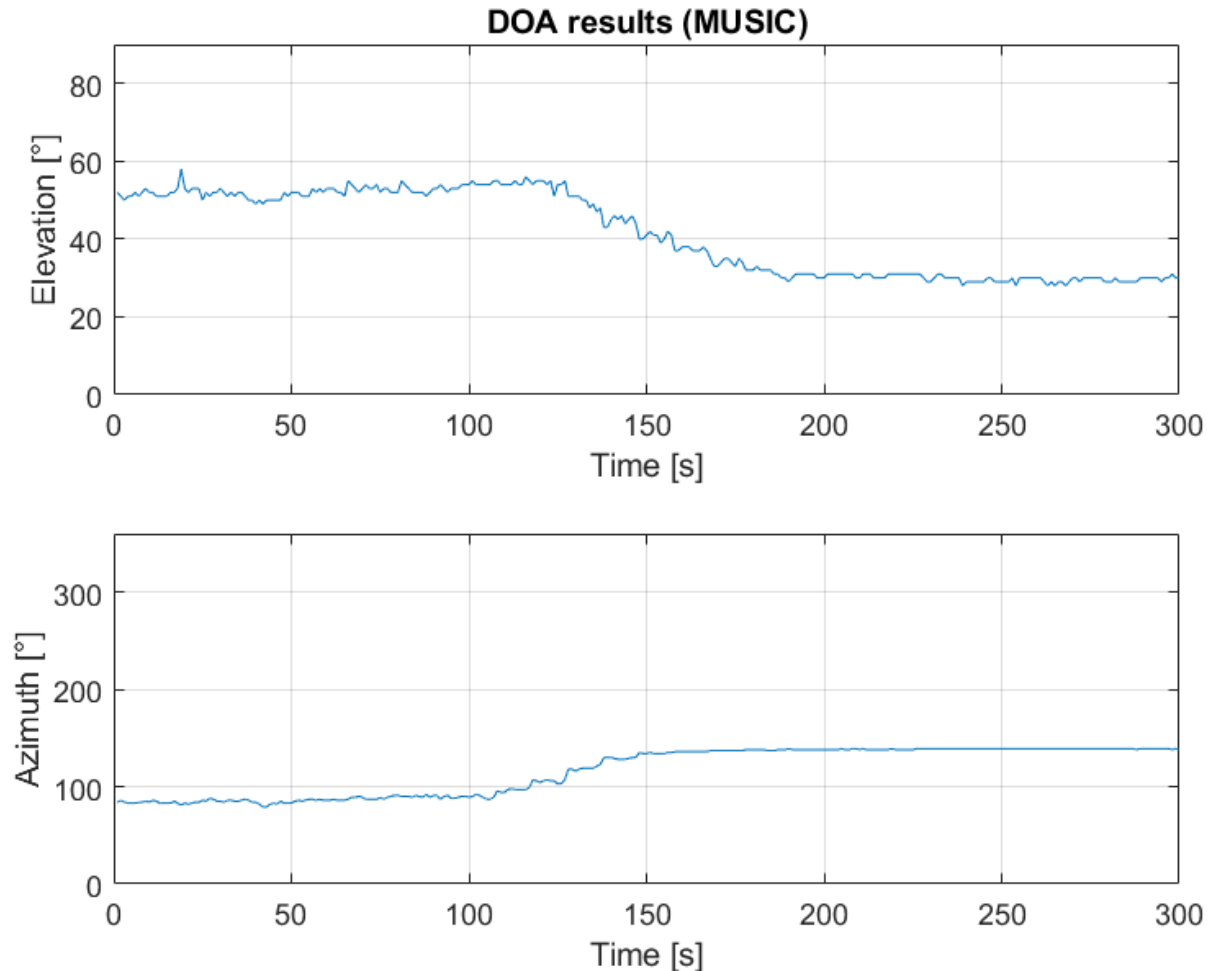
$$\frac{1}{\vec{w}^H \vec{V}_n \vec{V}_n^H \vec{w}}$$

- Denominator of the pseudospectrum is the magnitude of the projection of a spatial signature vector in the noise-only subspace
- The noise subspace is probed with different signature vectors => the magnitude of the projection of the jamming signature vector in the noise subspace is ideally zero



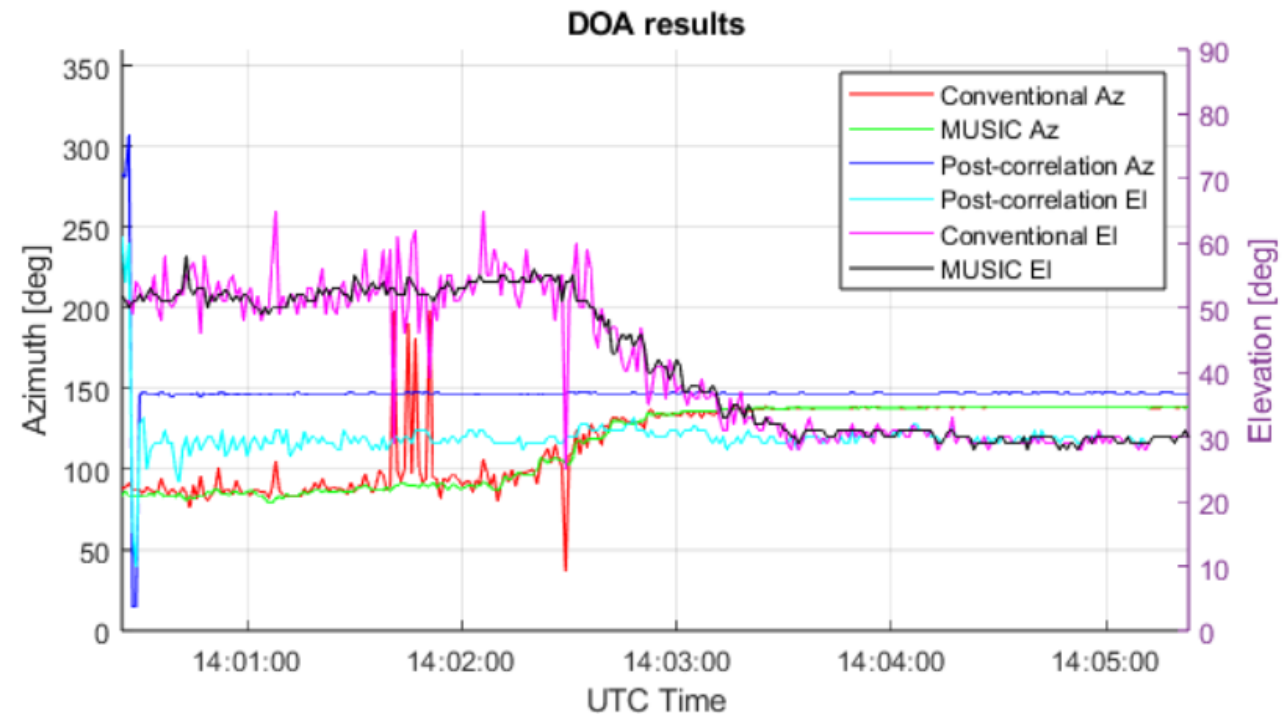
# Results of MUSIC DOA

- Results very close to those of the conventional beamformer
- Fewer spurious events due to averaging of the covariance matrix



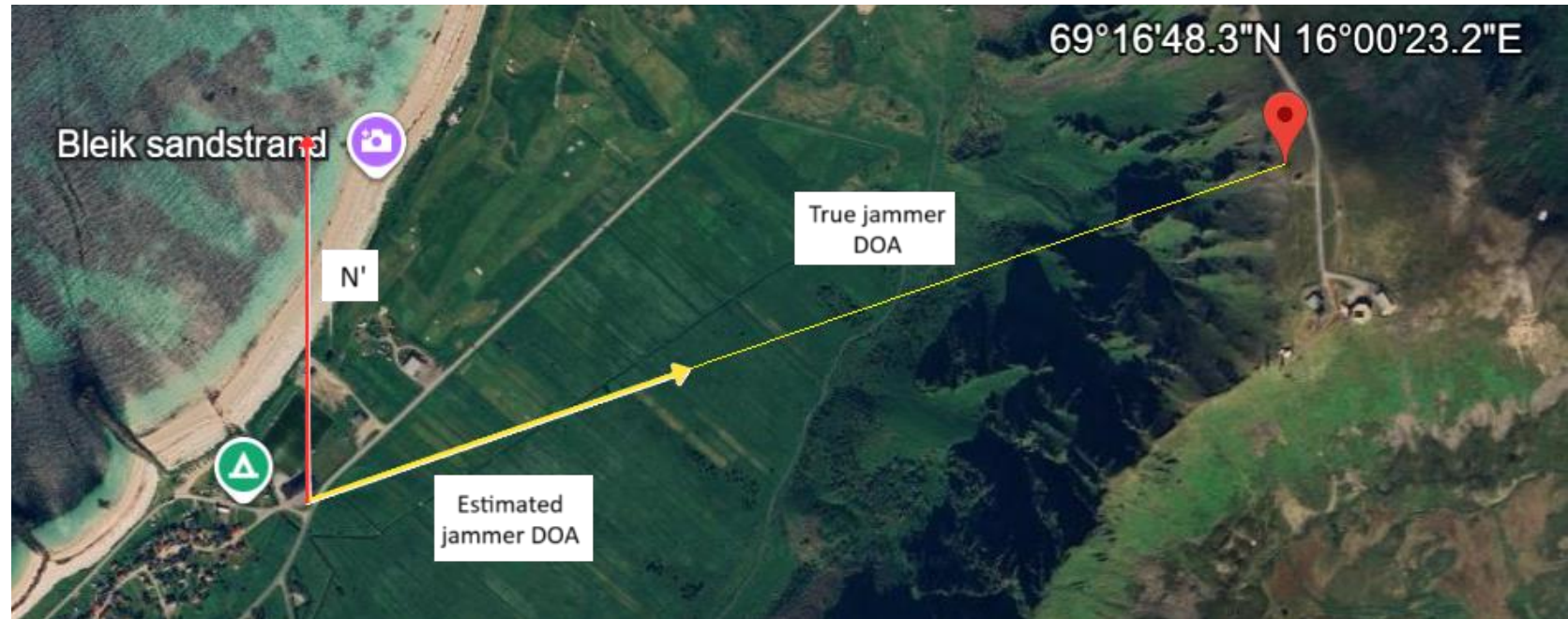
# Objective 2 – Conclusions (1/2)

- The conventional beamformer and MUSIC algorithm produce near-identical real-time DOA estimates
- Bonus: a post-correlation estimate confirms the jammer DOA since before it is detectable over the noise floor
  - Slight azimuth mismatch



# Objective 2 – Conclusions (2/2)

- North estimate aligned with north in Google Earth
- Jammer DOA w.r.t to north same as in the reference frame
- Jammer location obtained from JammerTest test catalog: Location of 'SENDER':
  - lat: 69.28007238;
  - long: 16.00643461;
  - Ellipsoidal height: 381.98 m



# Objective 3 – Jamming Mitigation

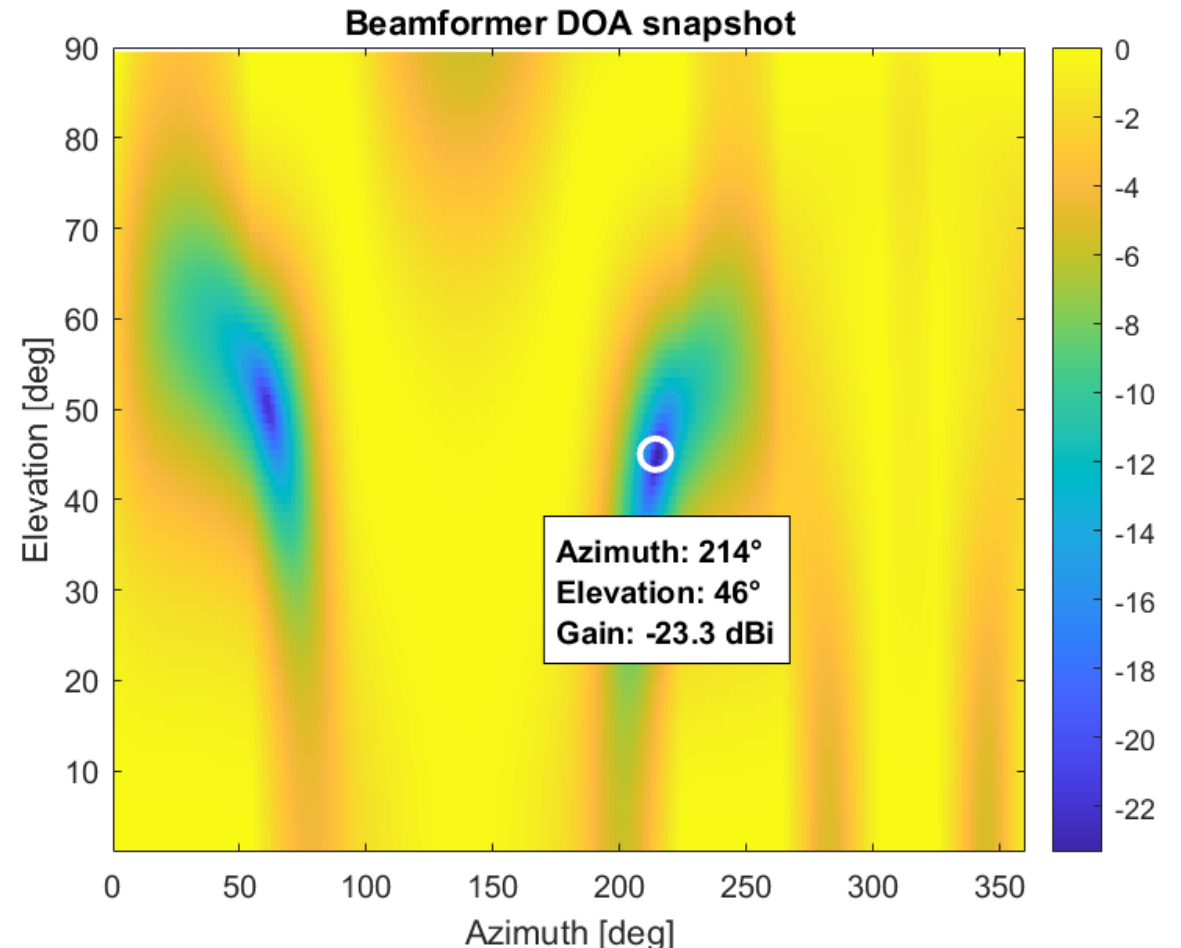
- Recall that appropriate selection of array summation coefficients allows coherent summation of signals from a desired direction
  - The coefficients may also be computed for destructive summation
- GNSS signals are received with power below the noise floor
  - Minimizing total array output power can be expected to suppress interfering signals
  - Care must be taken not to affect reception of GNSS signals significantly
- Note that it is possible to both amplify desired signals while suppressing interfering signals



# Jamming Mitigation via Power Minimization

- A possible power minimization approach is to find the optimal steering angle for the conventional beamformer
  - Obtainable from the DOA estimate
- A single interference source is likely to fall into a null region for some steering angle
  - Useful approach if this steering angle permits acceptable GNSS reception
  - The wide main beam of the small array allows reception of a large part of the sky at once

=> Blind steering

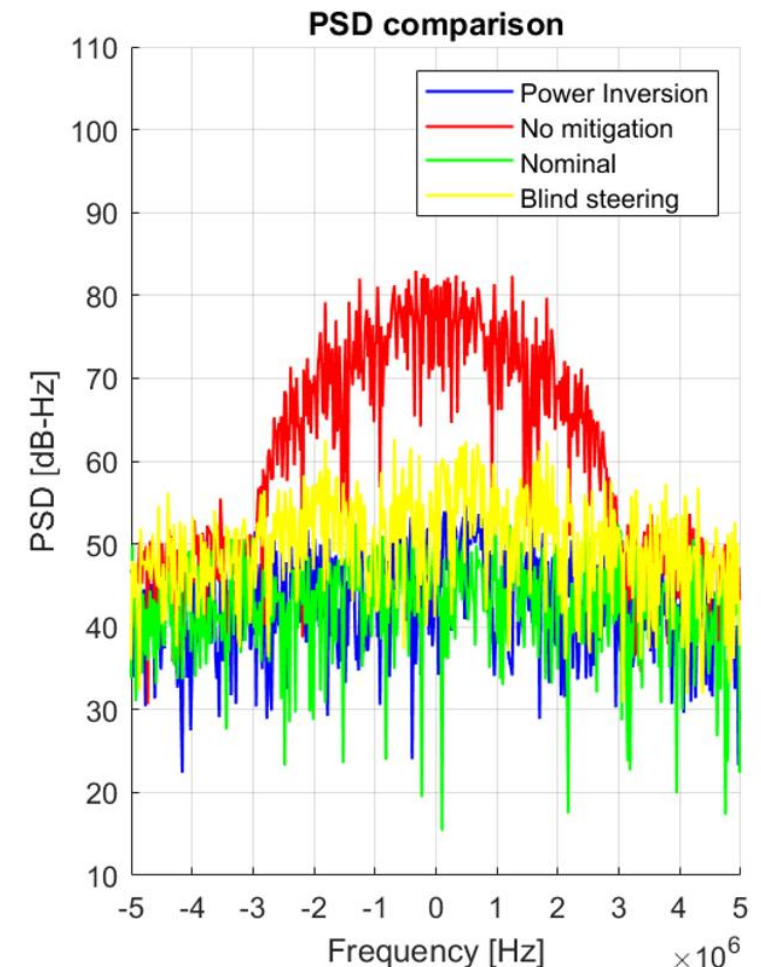


# Jamming Mitigation – Results (1/5)

- Results are evaluated with respect to
  - In-band power spectral density
  - Array factor under interference
  - Sample amplitude distribution
  - PNT solution
    - Availability
    - Accuracy
  - Receiver observables
- For PSD and sample distribution analysis, all data were taken from the last second of the dataset
  - Nominal reference from first second of the dataset

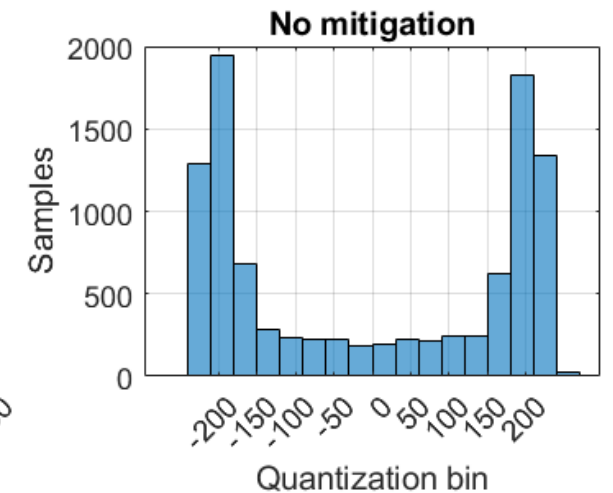
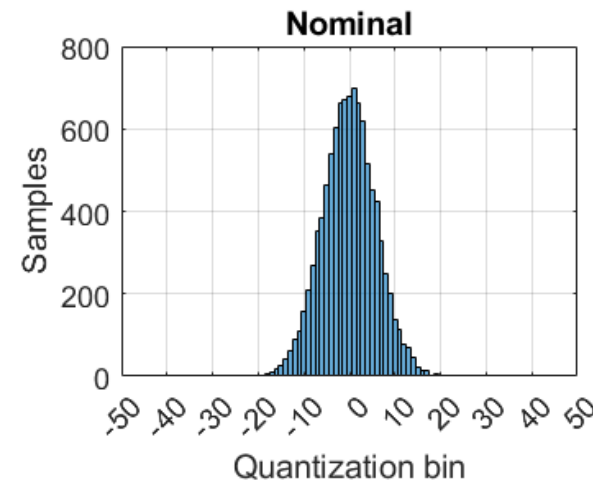
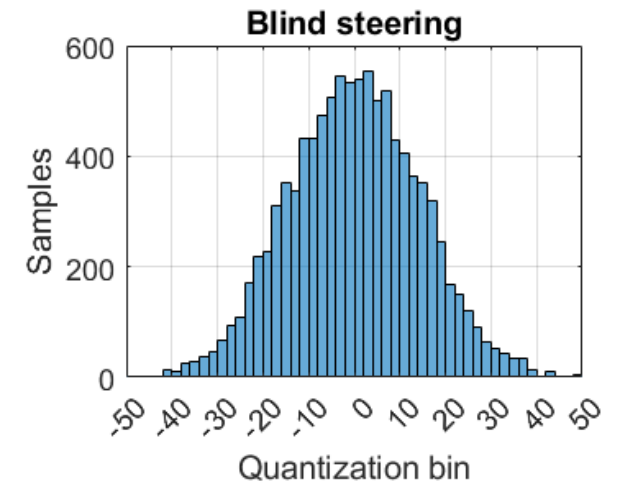
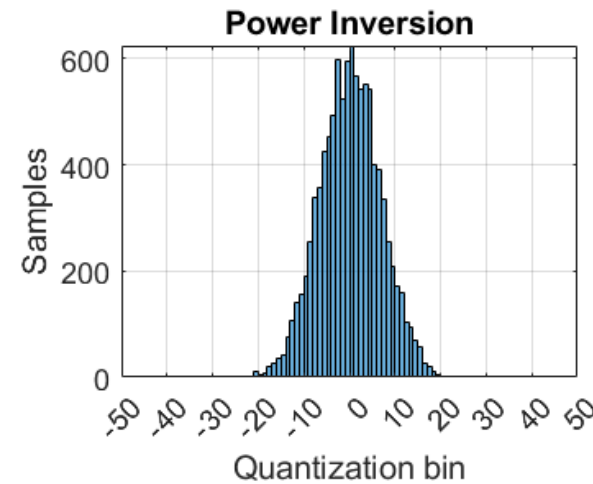
# Jamming Mitigation – Results (2/5)

- In-band power spectral density is reduced significantly upon application of the mitigation techniques
- Only a measure of received power: separate analysis required to ascertain impact on GNSS reception
  - Most effective way to reduce perceived in-band PSD would be to remove the antenna :)



# Jamming Mitigation – Results (3/5)

- Sample distribution analysis confirms the RF environment is closer to nominal with mitigation applied
- Impact of BPSK signal on sample distribution clearly observable



# Jamming mitigation – results (4/5)

TABLE II: PVT solution error statistics.

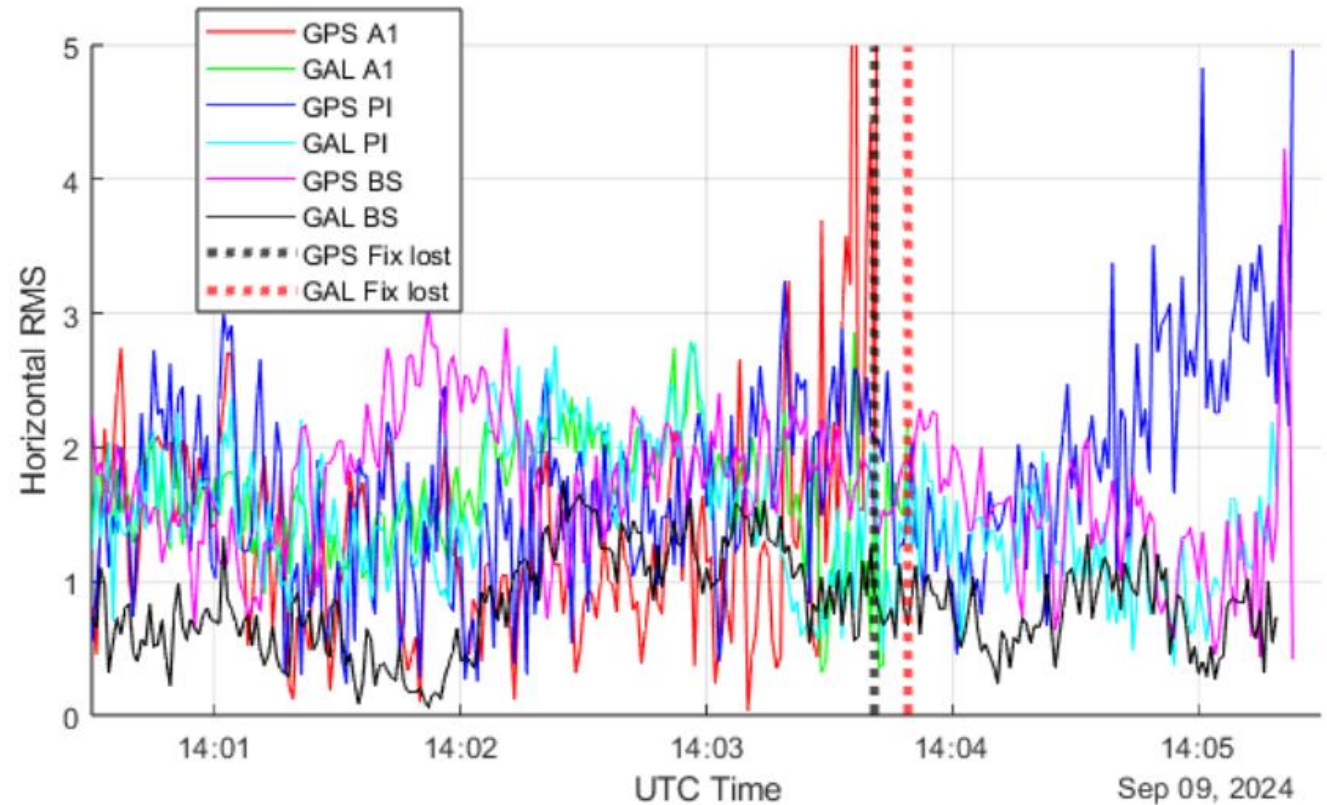
Constellation	GPS						GALILEO					
Input	ANT 1	ANT 2	ANT 3	ANT 4	PI	BS	ANT 1	ANT 2	ANT 3	ANT 4	PI	BS
Horizontal RMS (m)	2.22	7.3	18.06	5.43	1.52	2.07	1.5	1.71	6.53	12.02	1.36	0.98
Horizontal Mean (m)	1.56	7.23	28.79	3.7	1.75	1.7	1.65	1.49	1.78	1.92	1.47	0.83
Mean HDOP	1.59	1.94	8.36	1.64	1.52	1.63	1.52	1.42	2.16	3.71	1.36	1.36
Availability	67%	77%	67%	77%	100%	100%	69%	65%	69%	78%	100%	100%

- Key notes about error statistics:
  - Availability of PNT solution with both phased array mitigation techniques is 100%
  - No performance lost against a single-antenna solution in the nominal section
- PNT processing in FGI-GSRx!



# Jamming Mitigation – Results (5/5)

- Phased array mitigation techniques allow performance comparable to a nominal scenario even under strong jamming
  - ⇒ **Phased array signal processing has significant potential for resilient PNT**
  - ⇒ Resilient-PNT-specific CRPAs will be removed from ITAR list



Horizontal RMS position error for different processing configurations

# Advancing together

