Jammertest 2024
ESA Testing Activities

04/04/2025

N. Bni Lam
X. Otero Villamide
L. Musumeci
S. Binda

Presentation Outline

- Jammertest 2024 → Program & Locations

What is Jammertest?

- Organized by four branches of government, all backed by the Norwegian Space Agency
- The regulatory aspect is handled by the Organizers
- 5 days of various tests
- The Location (at a high latitude 69.27N, 15.96E) of the test is unique with open sky, rural, and limited canyon (near the mountain)
- Jammertest 2024 - more than 250 participants

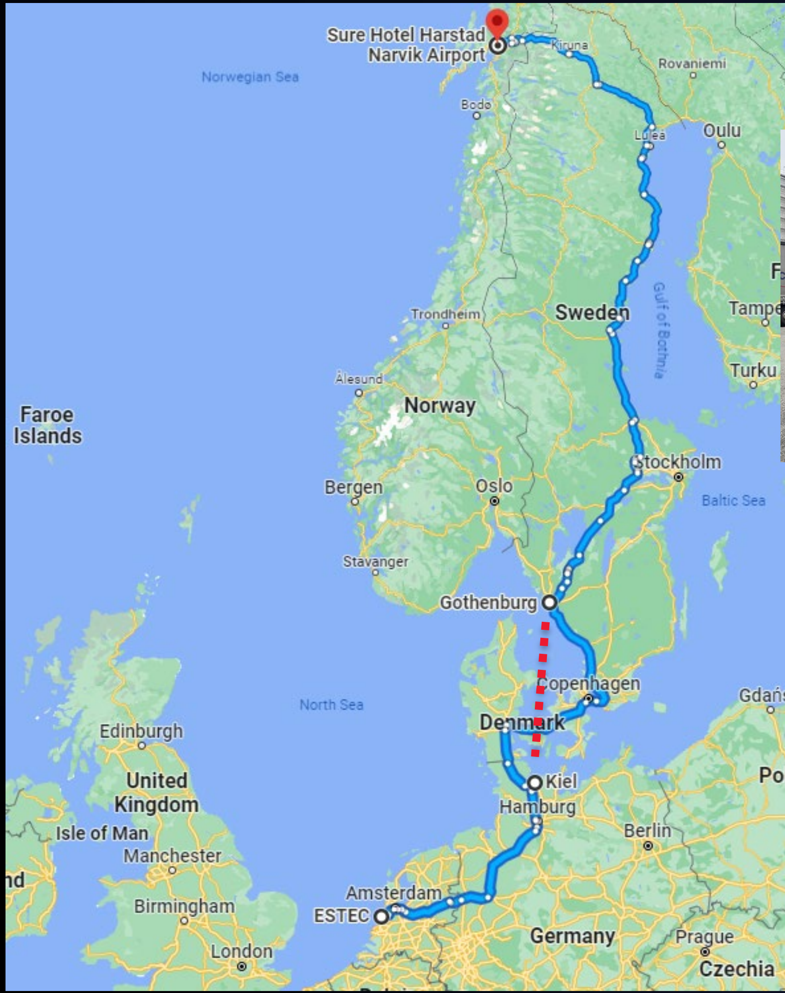
Photo: David Jensen

Presentation Outline

- Jammertest 2024 → Program & Locations
- ESA Jammertest → Logistics and setups

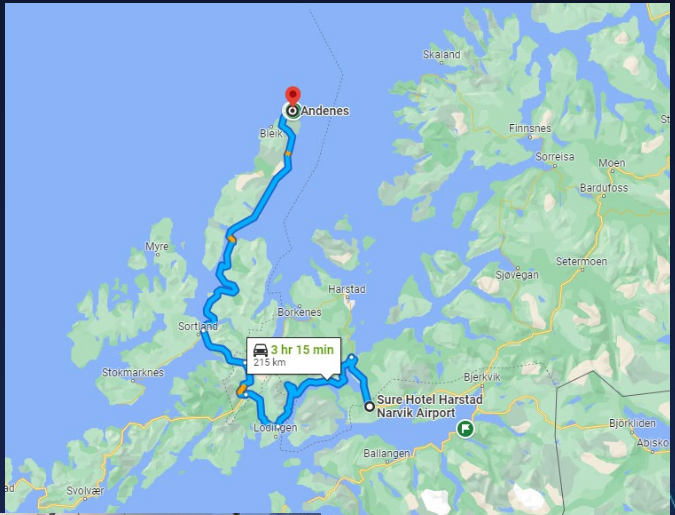
ESA Jammertest logistics

Vehicle main transportation



*Ferry was taken from Kiel to Gothenburg

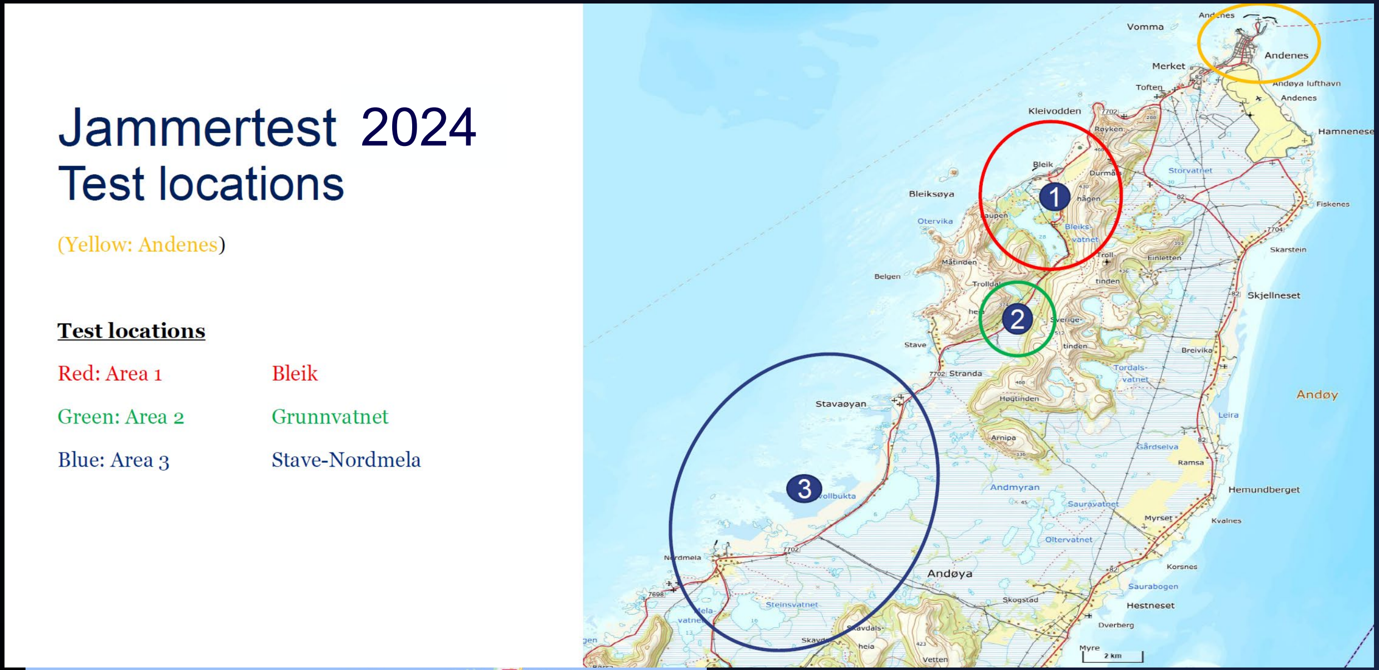
ESA team trip



Round trip : **5500 km** approx.

ESA Jammertest Base Camp

Base camp in Andenes, approximately 10 to 20km from testing locations

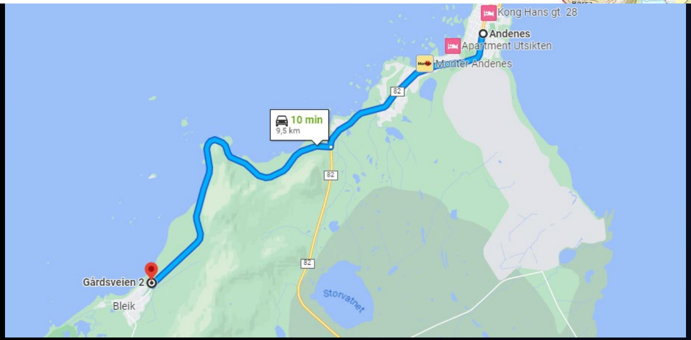


Jammertest 2024
Test locations

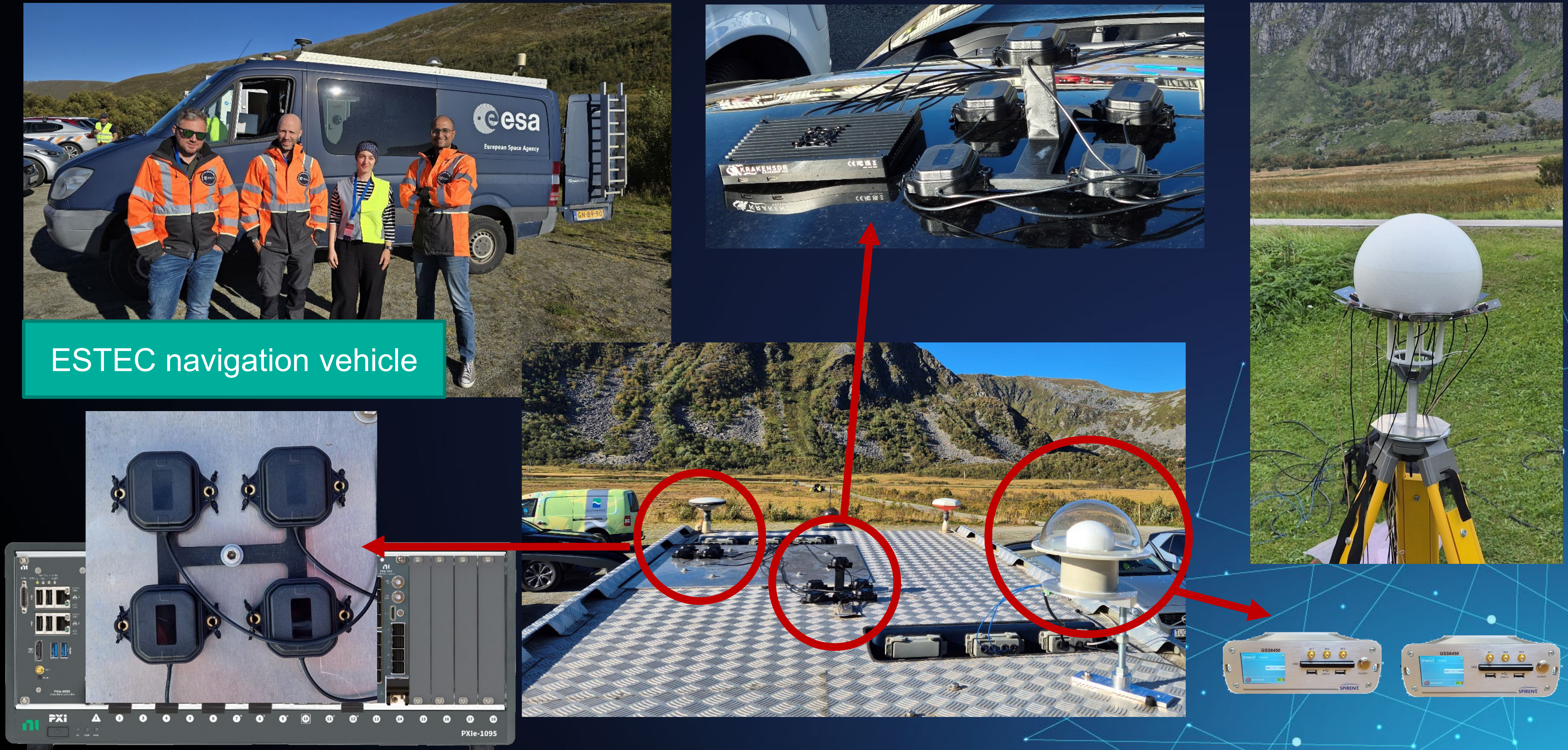
(Yellow: Andenes)

Test locations

Red: Area 1	Bleik
Green: Area 2	Grunnvatnet
Blue: Area 3	Stave-Nordmela



ESA Set-up



ESTEC navigation vehicle

Presentation Outline

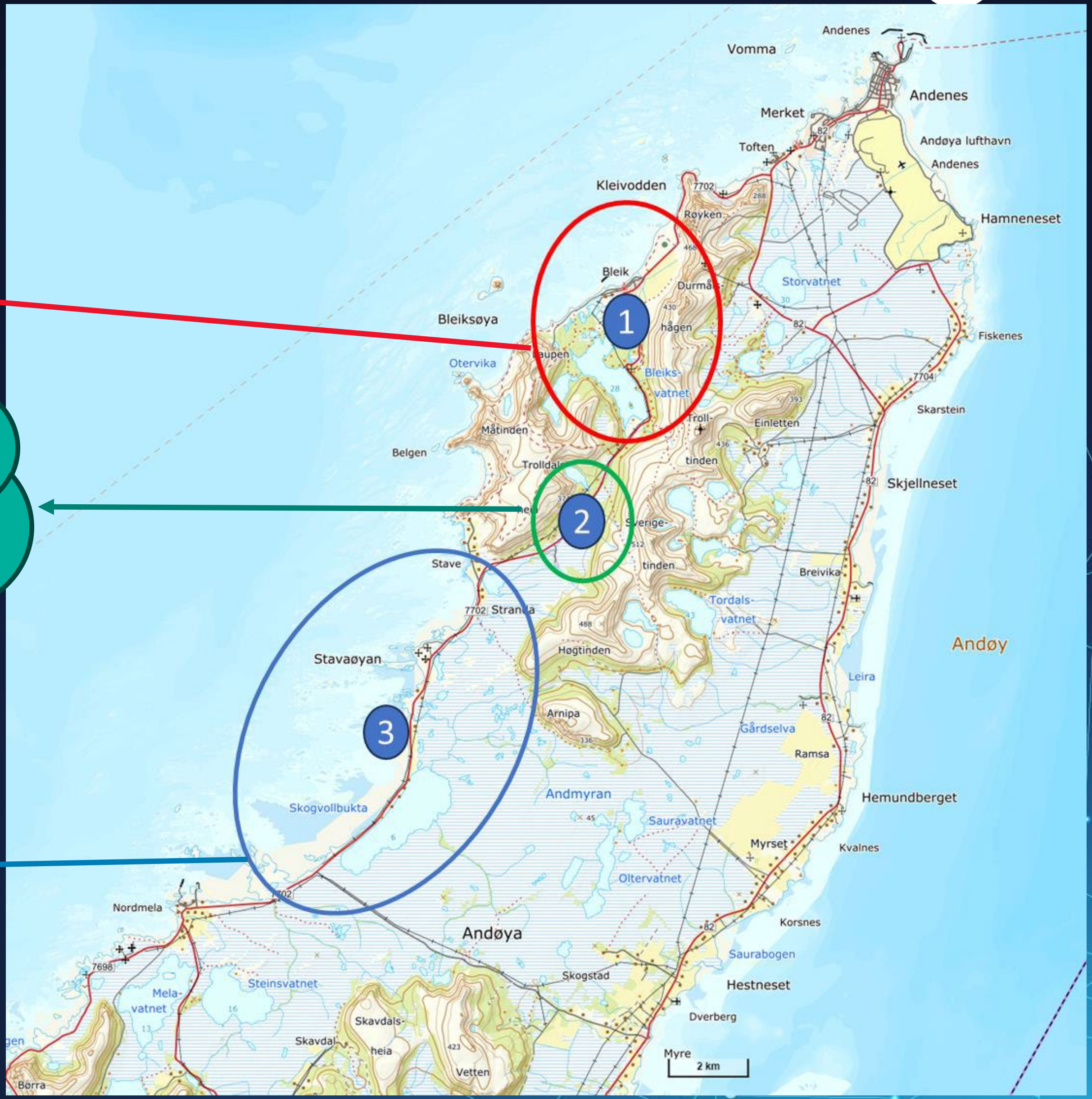
- Jammertest 2024 → Program & Locations
- ESA Jammertest → Logistics and setups
- Resilient Navigation → Scenarios, **Mobile** and Sensor station

Andoya Jammertest

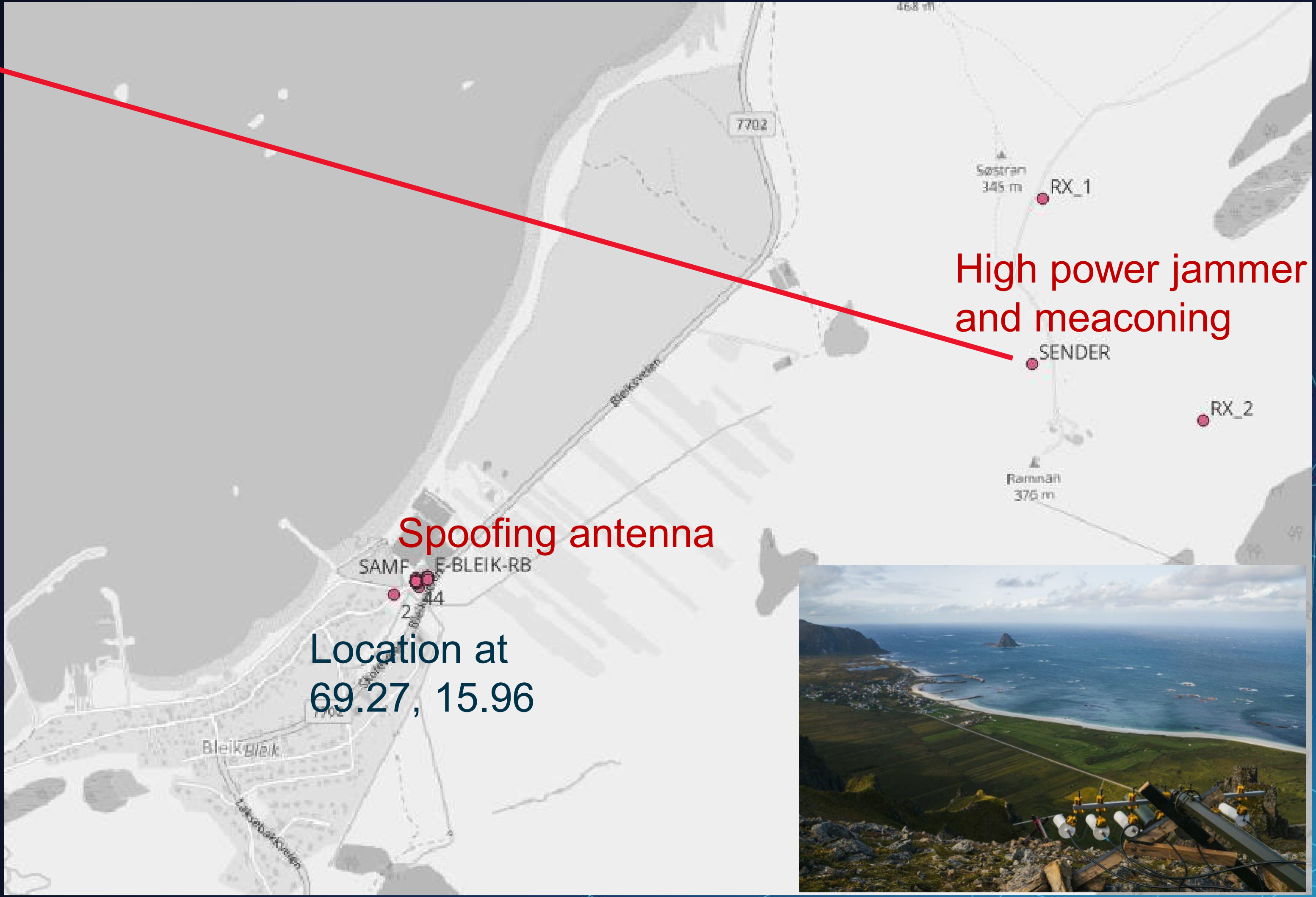
High power Jamming, Meaconing, and spoofing

COTS Jamming

Motorcade jamming and spoofing



Andoya Jammertest



High power jammer and meaconing

Spoofing antenna

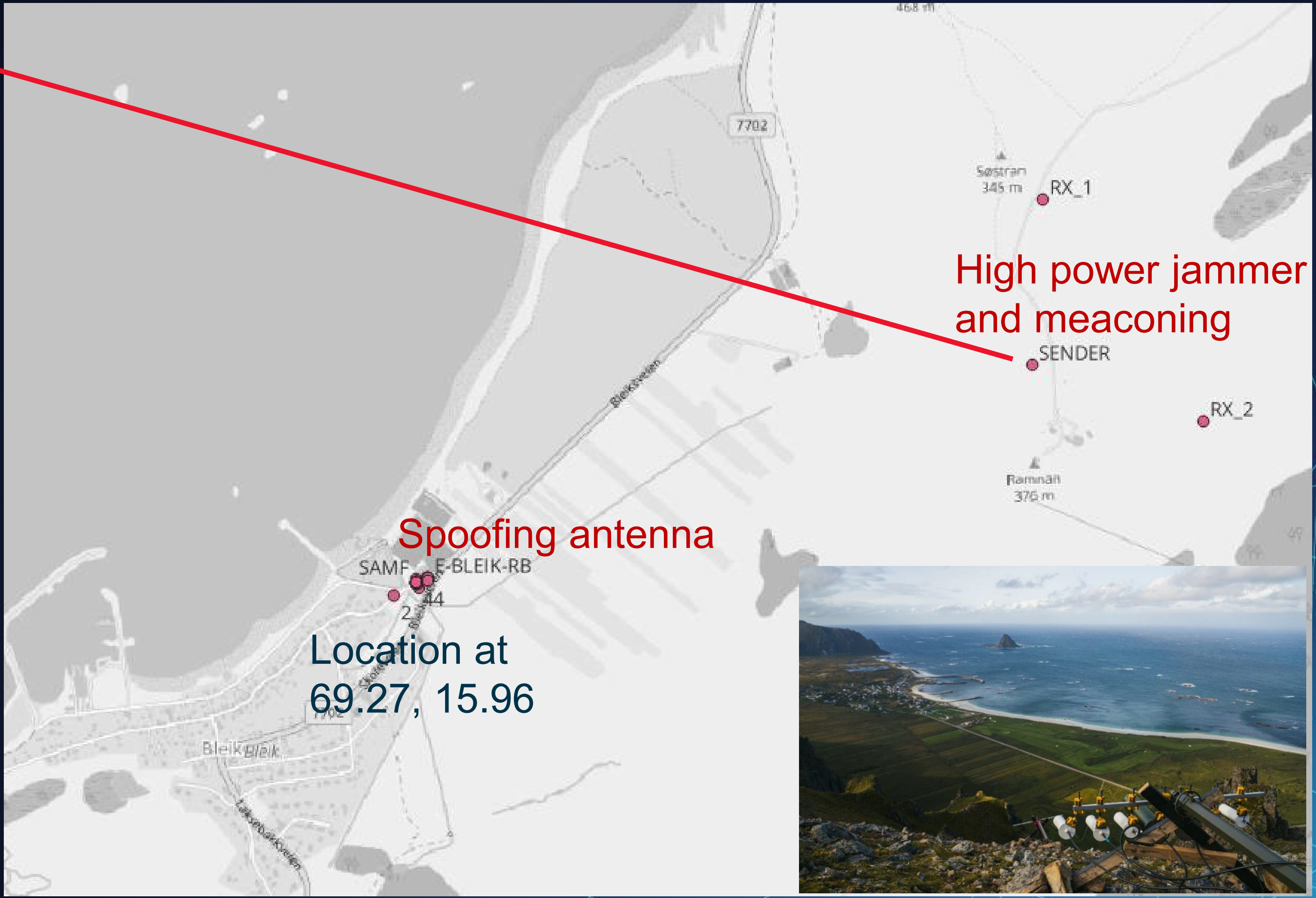
Location at 69.27, 15.96

High power Jamming, Meaconing, and spoofing

Andoya Jammertest - High Power Jamming

- High Power up to 100 W
- Various jamming signals: CW, Wideband signals, Chirp signals, modulated signals, frequency sweep.
- Jamming all or part of the L frequency sub-bands.

High power Jamming, Meaconing, and Spoofing



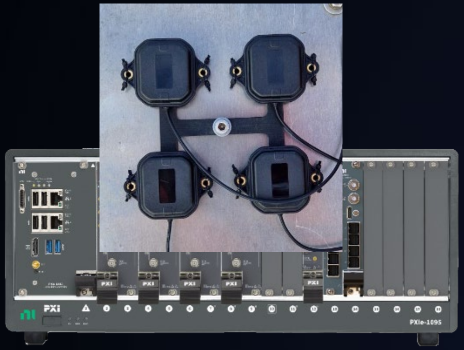
High power jammer and meaconing

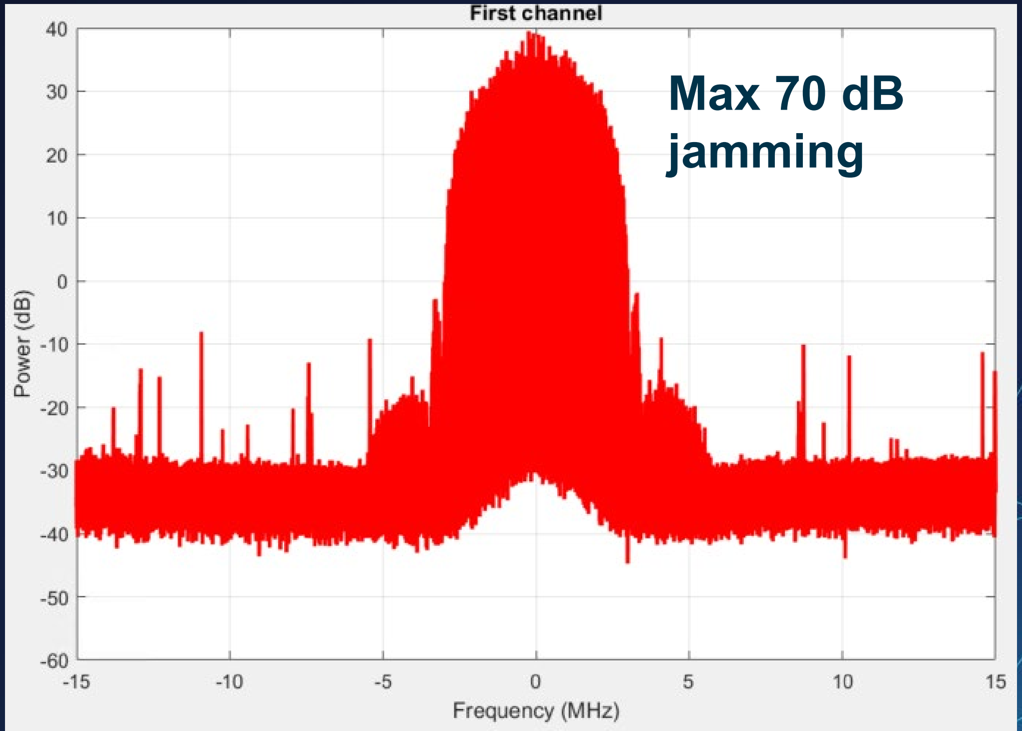
Spoofing antenna

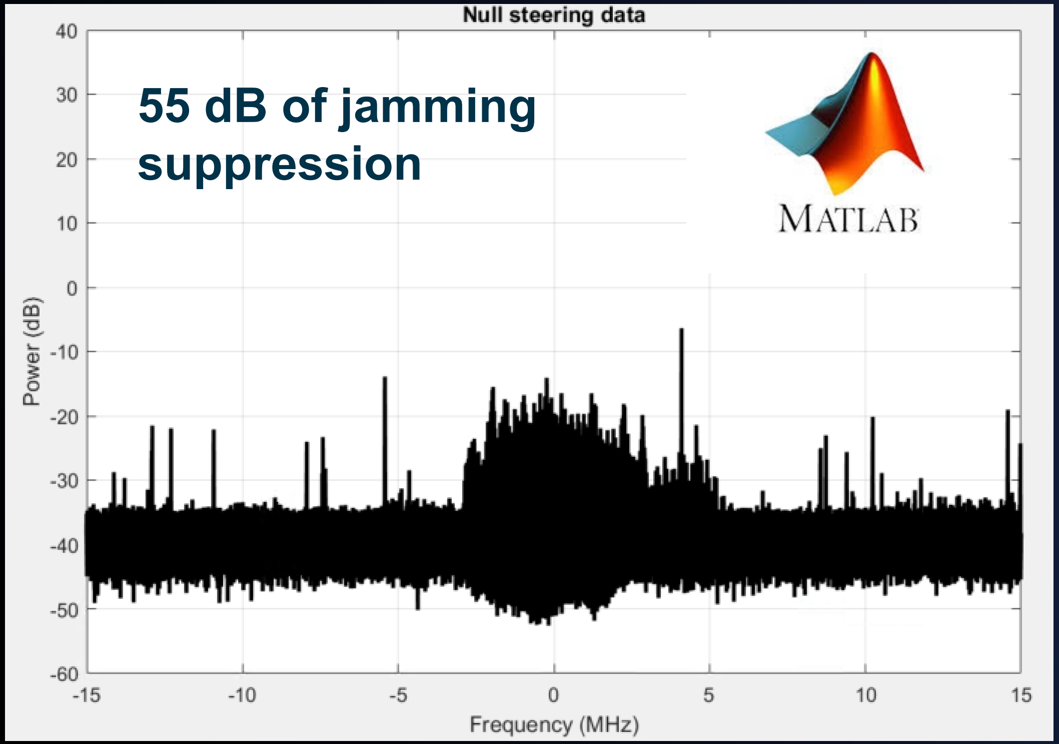
Location at 69.27, 15.96

E1 Power Ramp Scenario 1.6.1 – STAP TDL20

0.2 µW (-37dBm) to 50 W (47dBm) with 2 dB increments





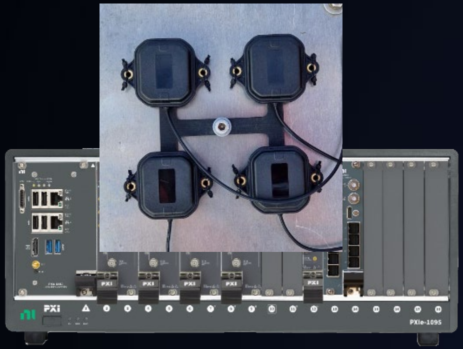


E1 only - 40 MHz BW - STAP TDL20

O. L. Frost, "An algorithm for linearly constrained adaptive array processing," Proceedings of the IEEE, vol. 60, no. 8, pp. 926–935, 1972.

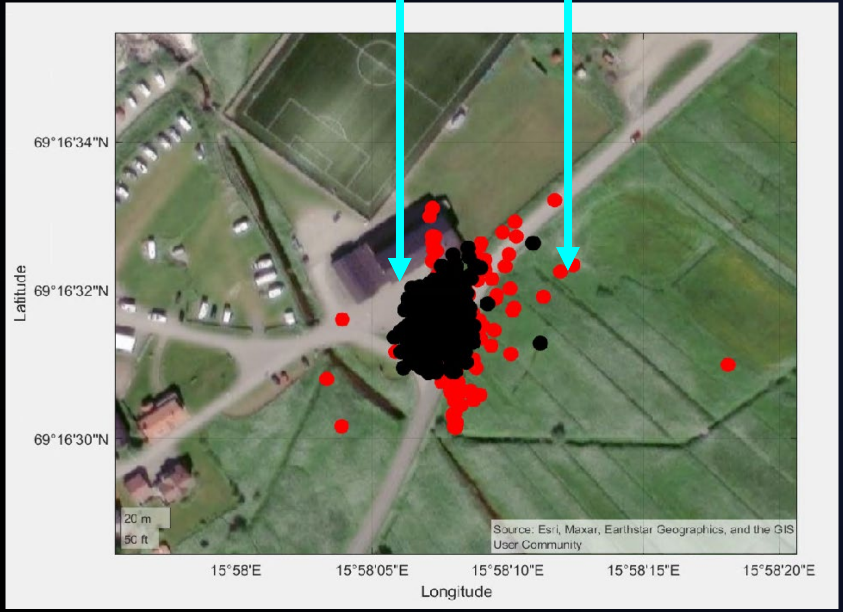
E1 Power Ramp Scenario 1.6.1 – STAP TDL20

0.2 µW (-37dBm) to 50 W (47dBm) with 2 dB increments

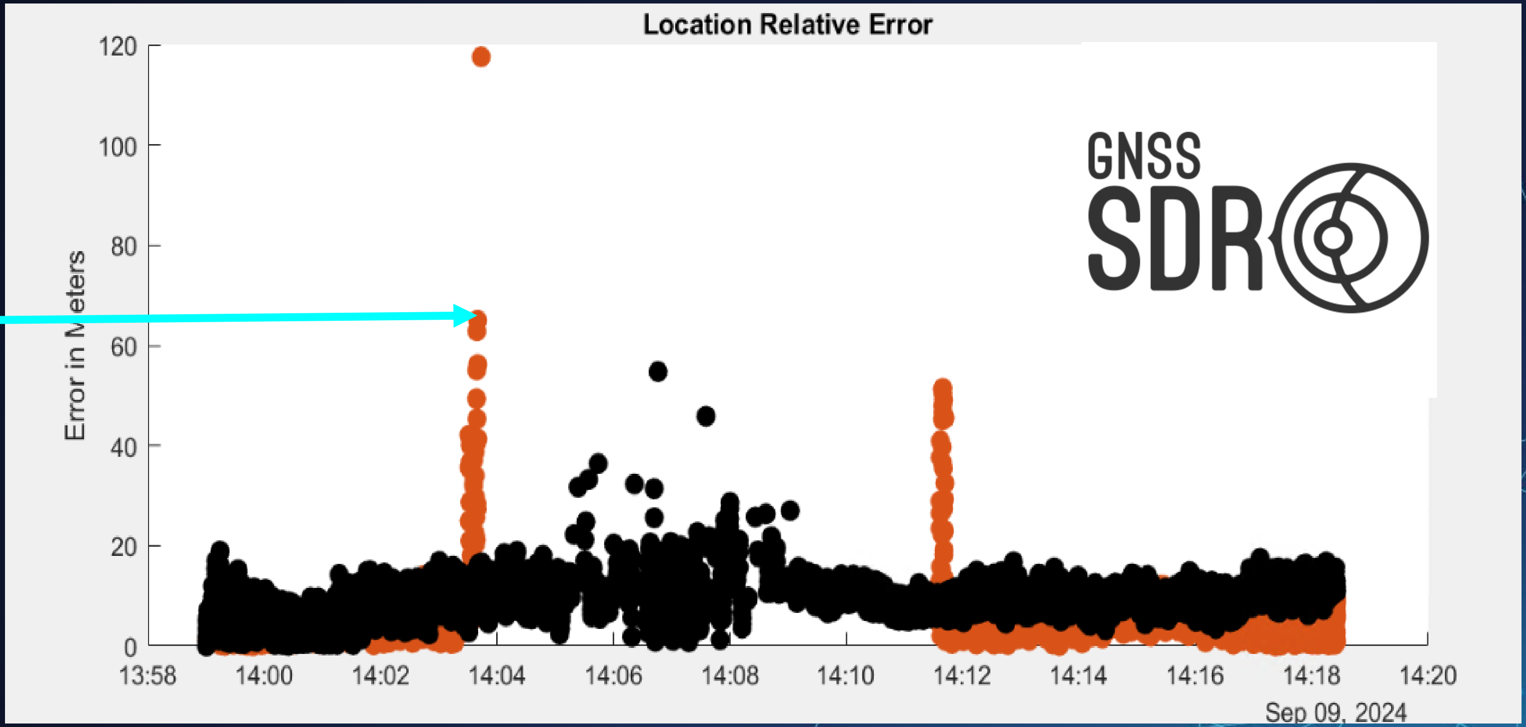


Single antenna

Null steering



Source: Esri, Maxar, Earthstar Geographics, and the GIS User Community



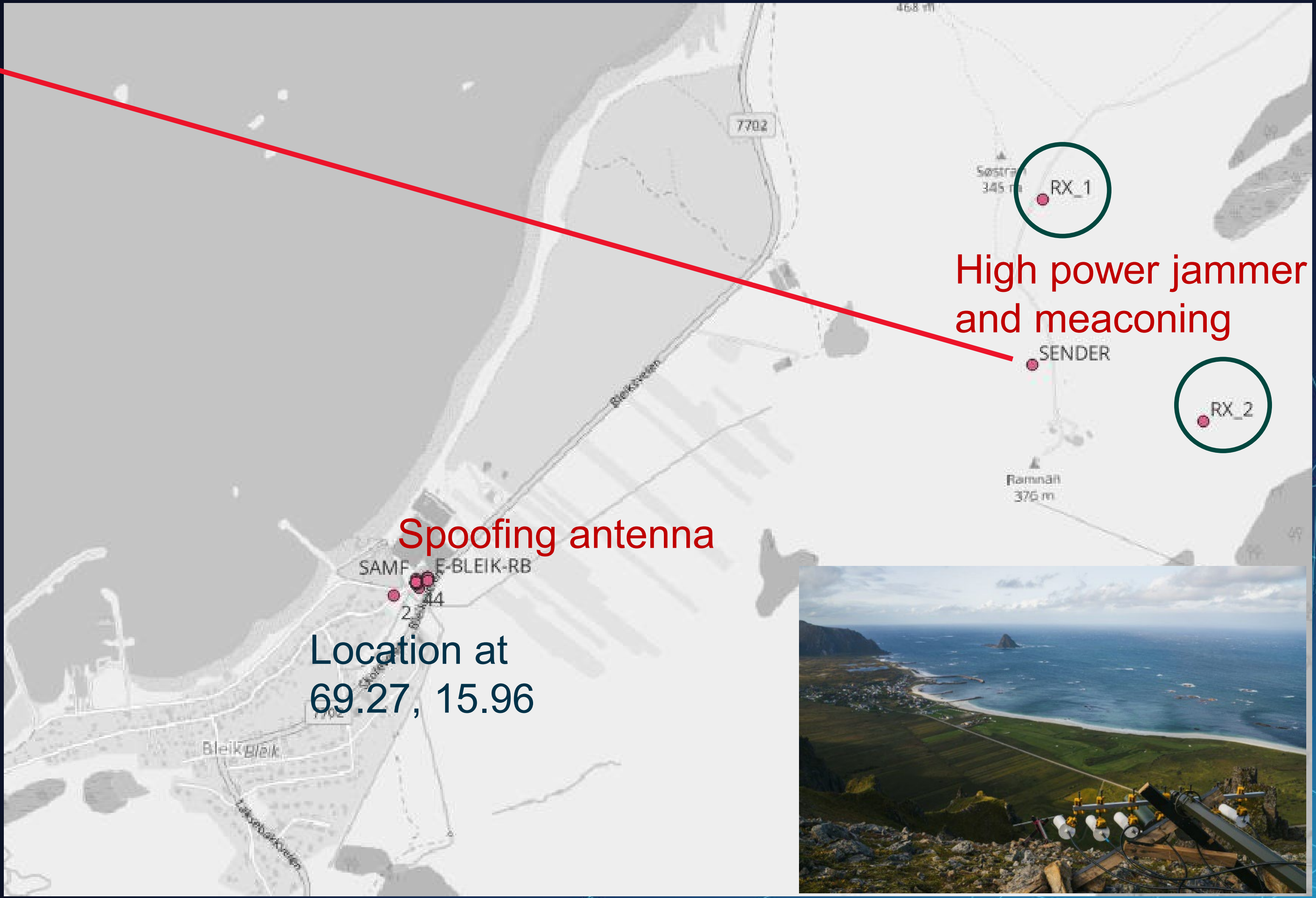
E1 only - 40 MHz BW - STAP TDL20

O. L. Frost, "An algorithm for linearly constrained adaptive array processing," Proceedings of the IEEE, vol. 60, no. 8, pp. 926–935, 1972.

Andoya Jammertest - Meaconing

- Alter the received GNSS signal to provide Meaconing
- Two meaconing locations, RX1 and RX 2
- Time manipulation

High power Jamming, Meaconing, and Spoofing



High power jammer and meaconing

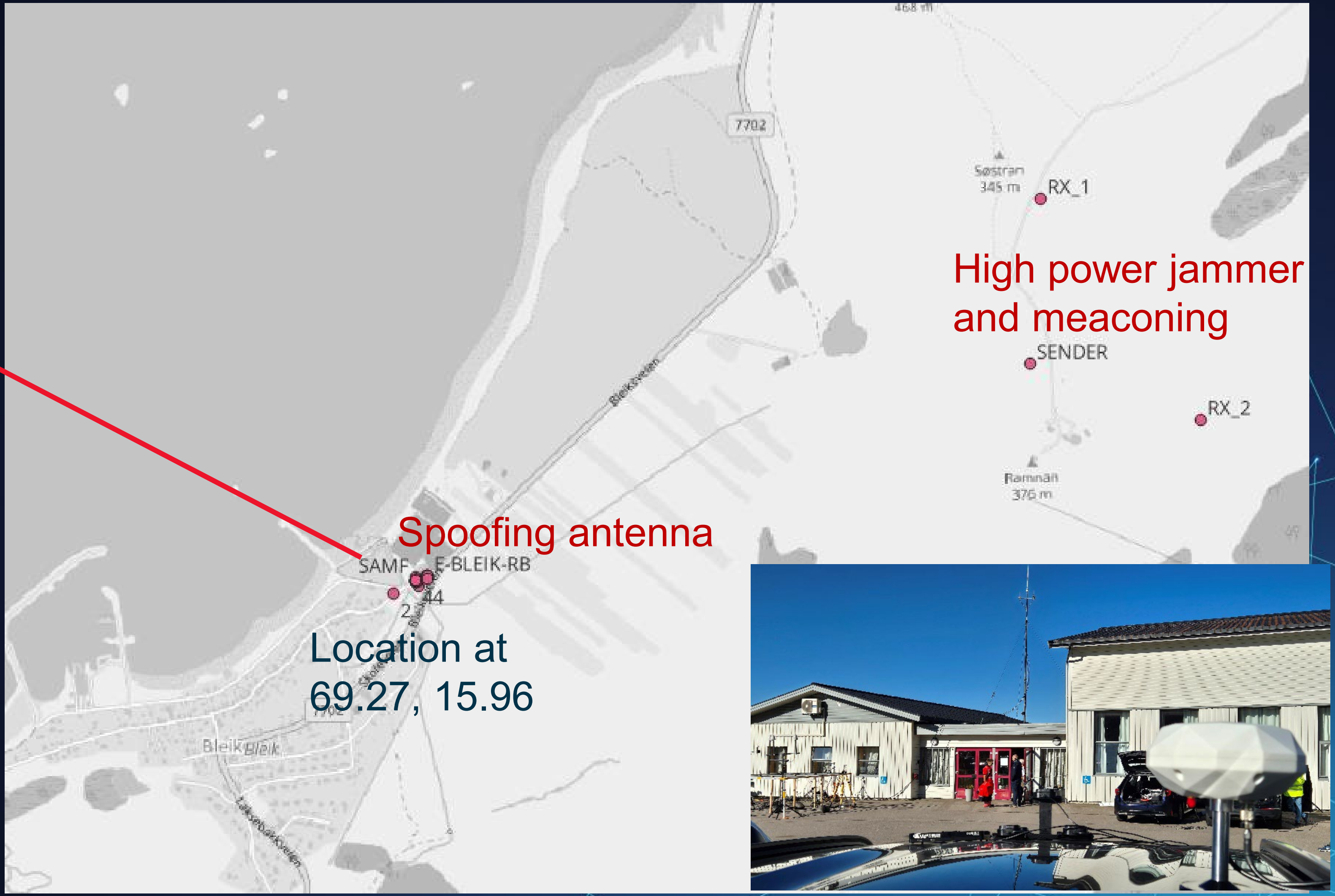
Spoofing antenna

Location at 69.27, 15.96

Andoya Jammertest - Spoofing

- Spoofing with a small jump
- Spoofing with a large jump (location coordinate 70N,10E)
- Jamming before the spoofing
- Simulating a driving car, drone and helicopter
- Spoofing all the bands and constellations
- Time manipulations
- …

High power Jamming, Meaconing, and Spoofing

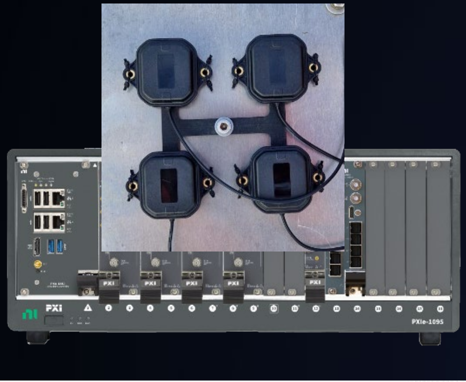


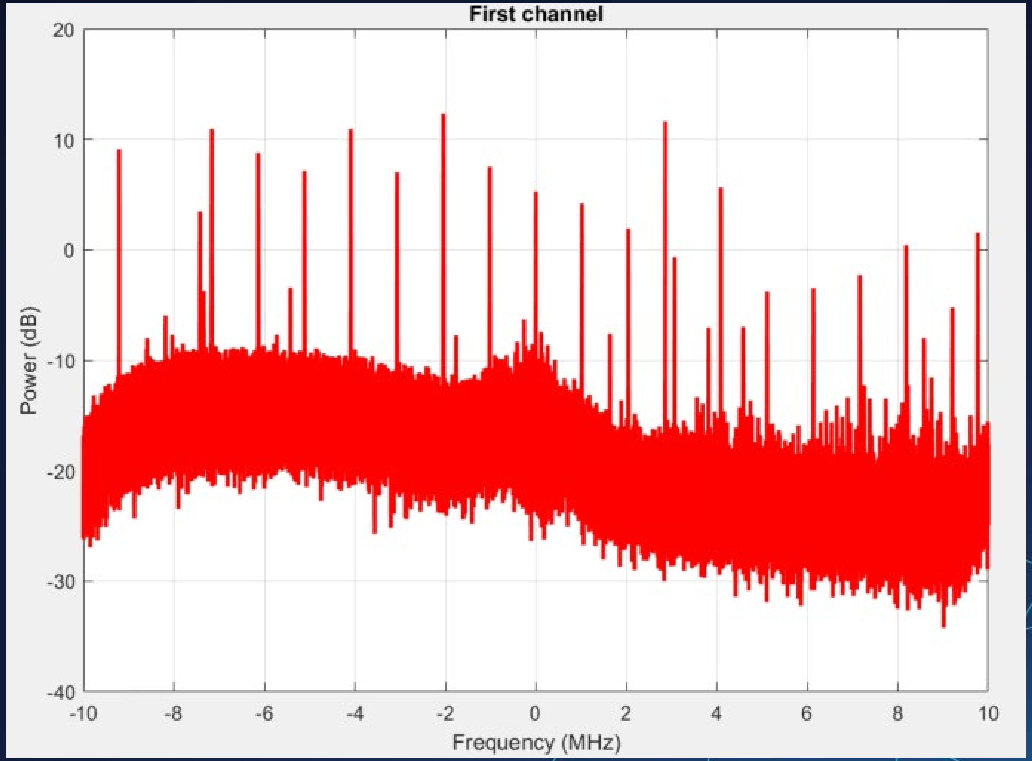
High power jammer and meaconing

Spoofing antenna

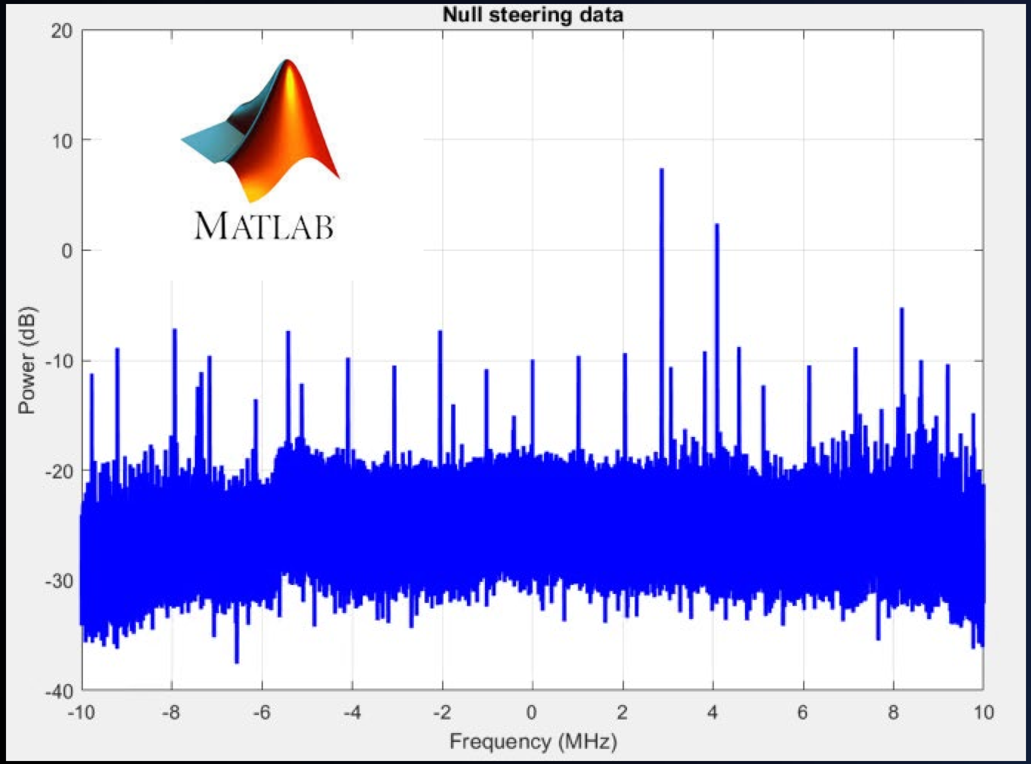
Location at 69.27, 15.96

E1 1W Meaconing 3.1.1 – MVDR





First channel

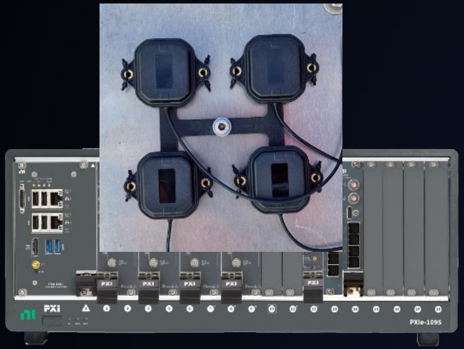


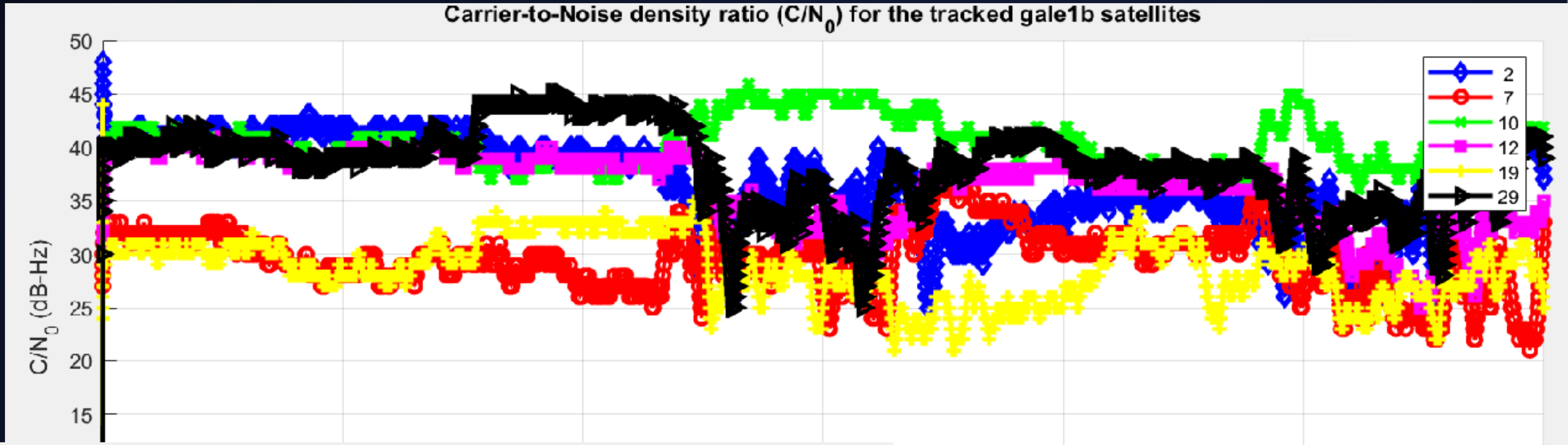
Null steering data

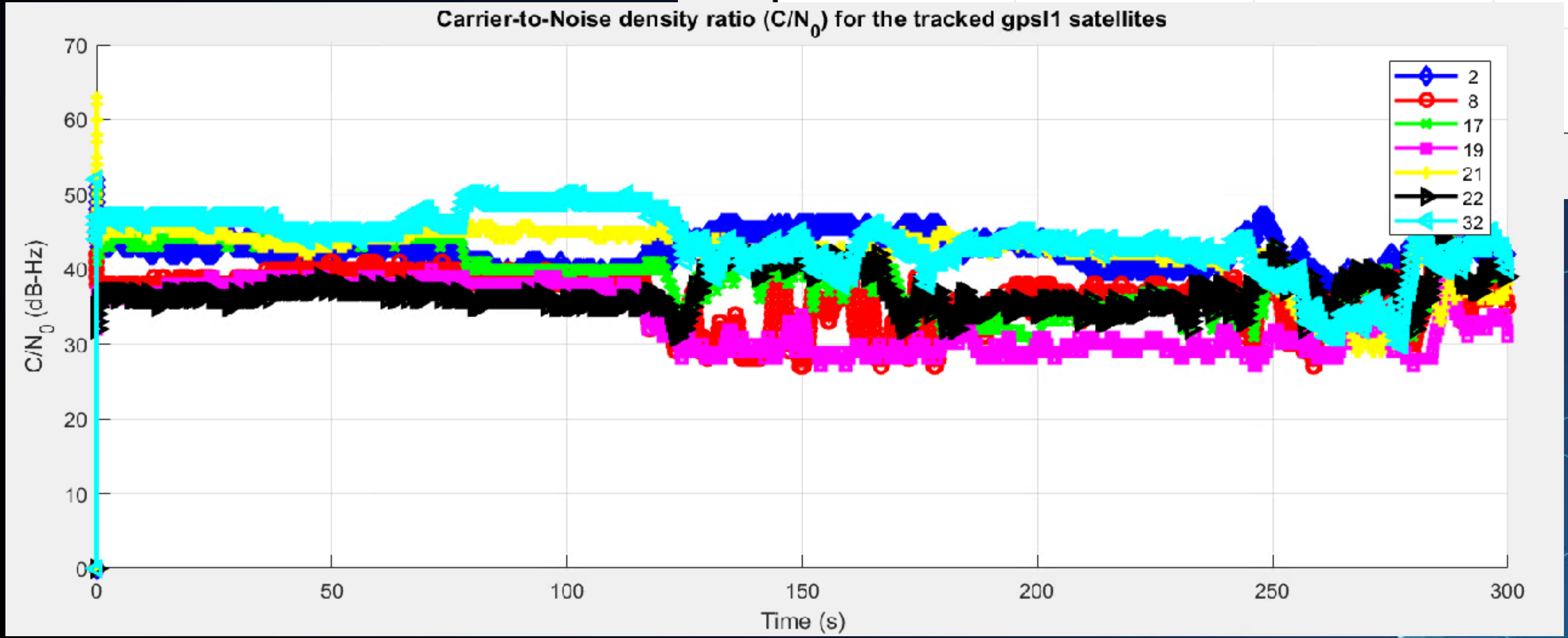
E1 only - 20 MHz BW - MVDR

BniLam, N., Ergeerts, G., Subotic, D., Steckel, J., & Weyn, M., "Adaptive probabilistic model using angle of arrival estimation for IoT indoor localization", *IEEE International conference on indoor positioning and indoor navigation (IPIN 2017)*

E1 1W Meaconing 3.1.1 – MVDR

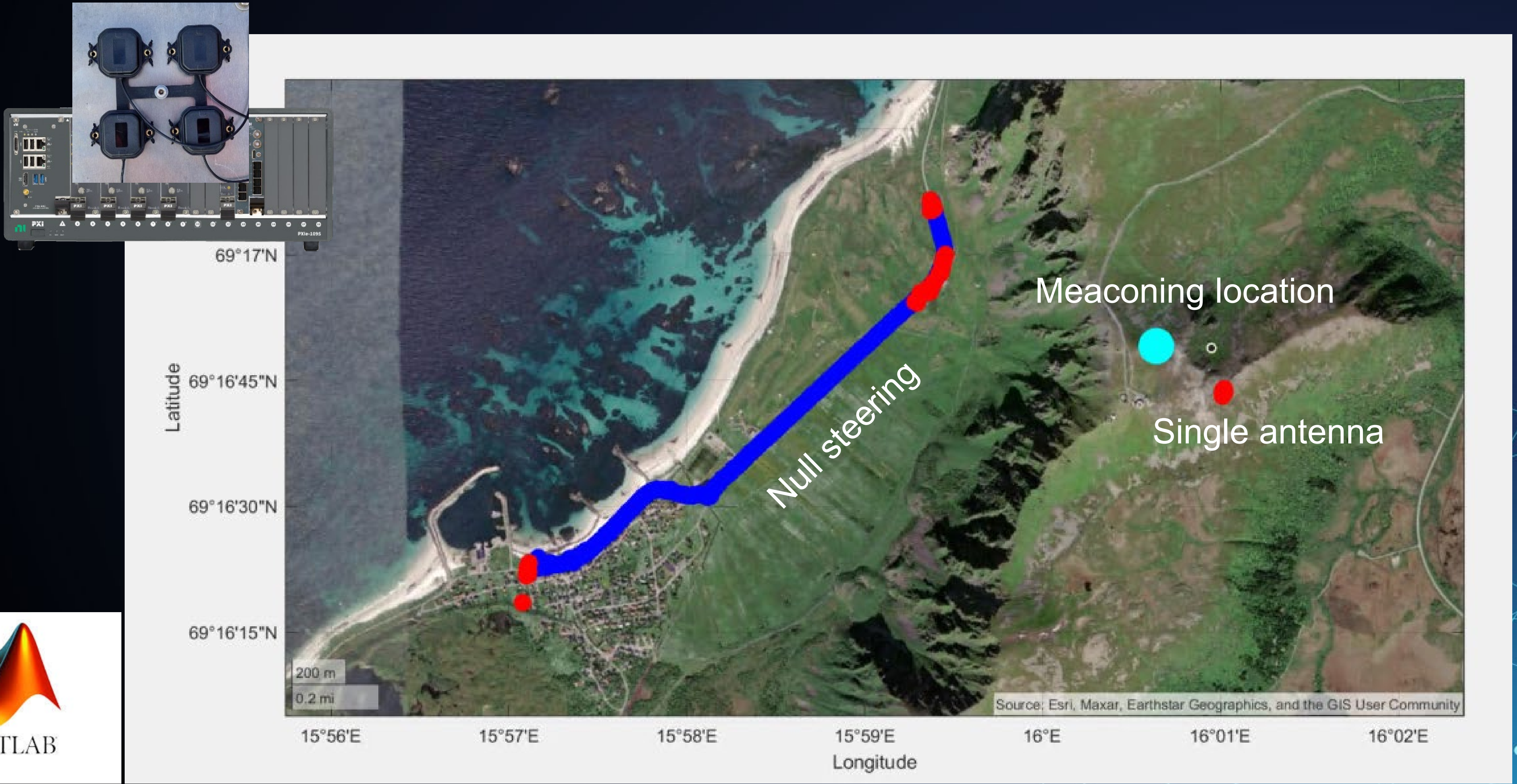



Carrier-to-Noise density ratio (C/N0) for the tracked gale1b satellites
C/N0 (dB-Hz)
50
45
40
35
30
25
20
15
200
250
300
2
7
10
12
19
29



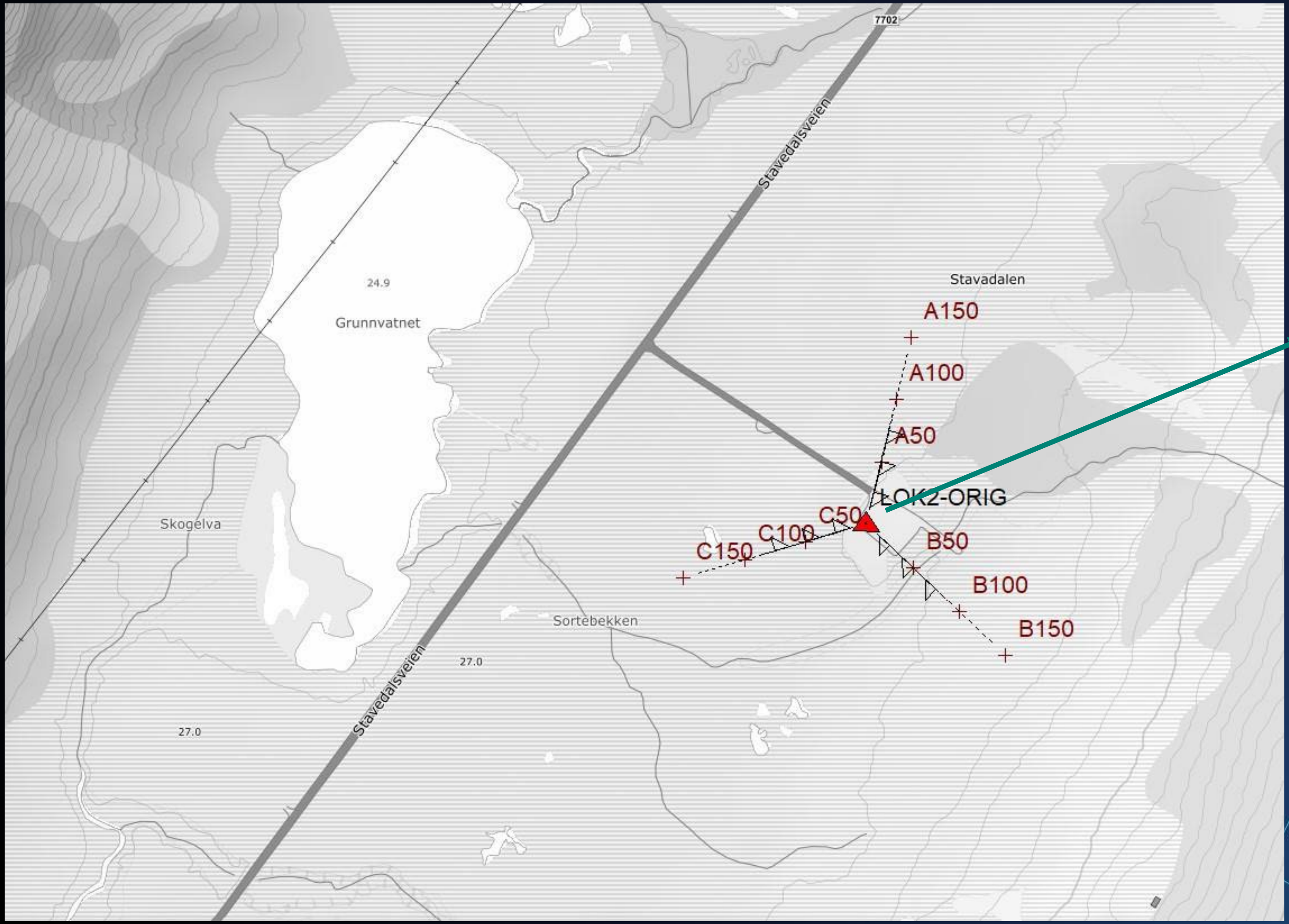
MATLAB

E1 1W Meaconing 3.1.1 – MVDR



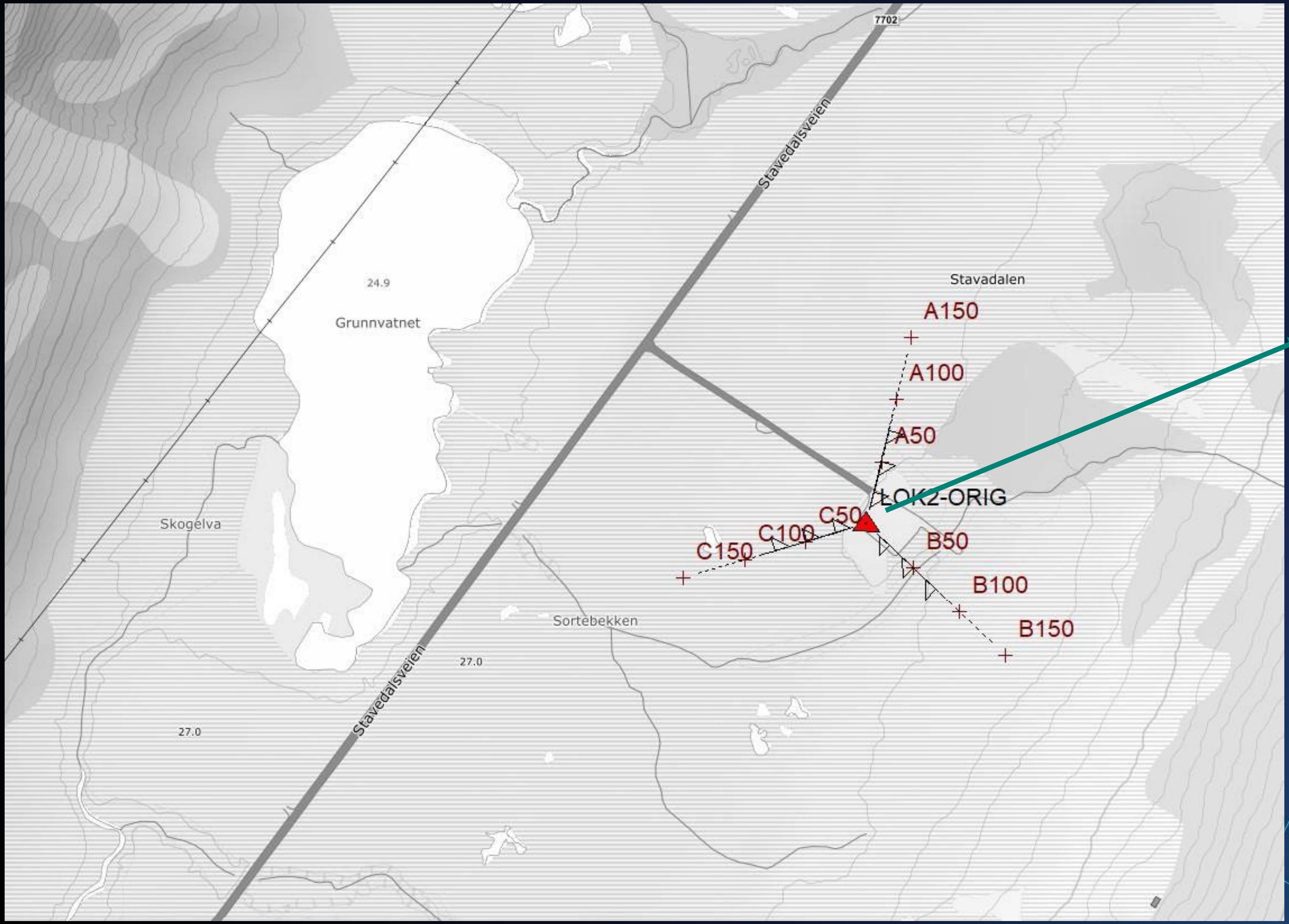
Source: Esri, Maxar, Earthstar Geographics, and the GIS User Community

Andoya Jammertest - COTS Jamming



COTS Jamming

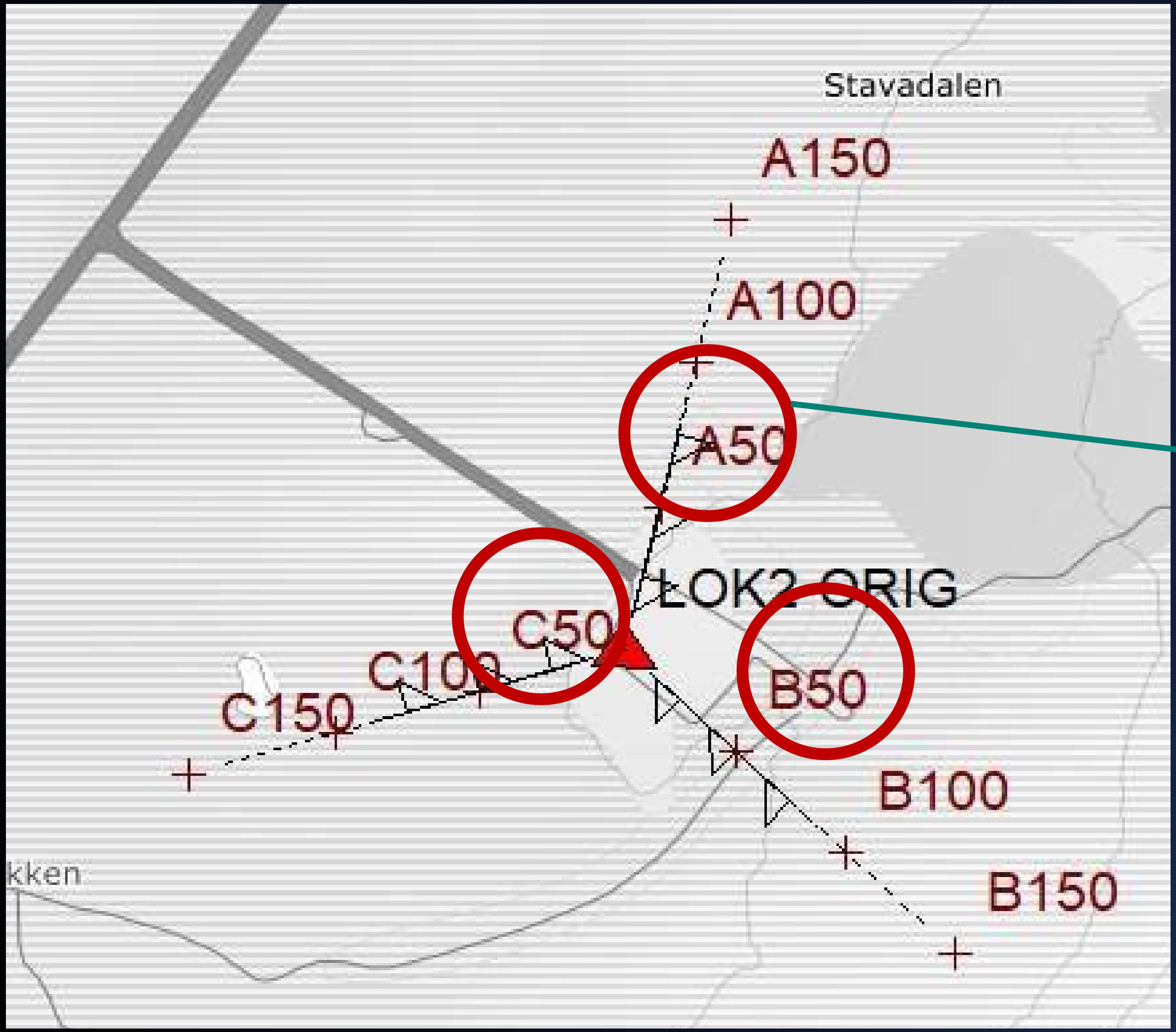
Andoya Jammertest - COTS Jamming



- Three jammers at the same time
- Various distance from the testing side
- Jamming bands and constellations ’G1’, ’L1’, ’E1’, ’B1C’, ’B1I’, ’E6’, ’B3I’, ’G2’, ’L2’, ’E5b’, ’B2b’, ’B2I’, ’L5’, ’E5a’, ’B2a’

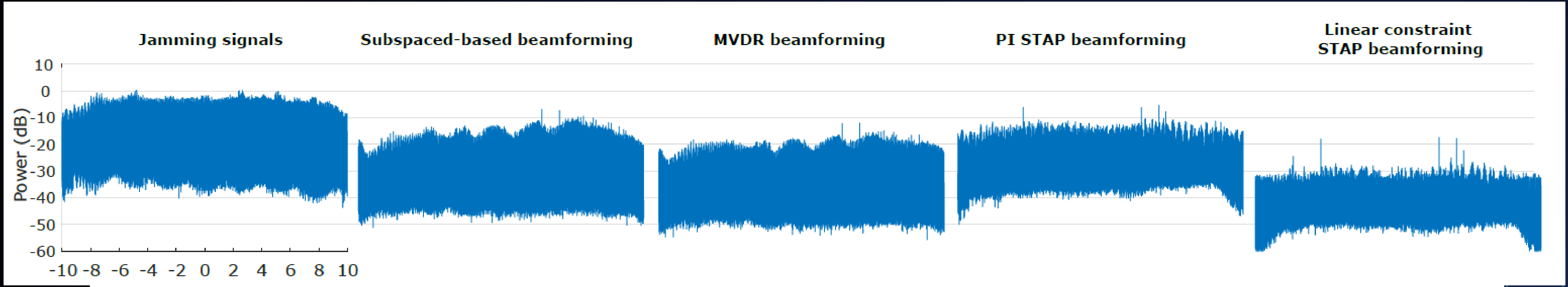
COTS Jamming

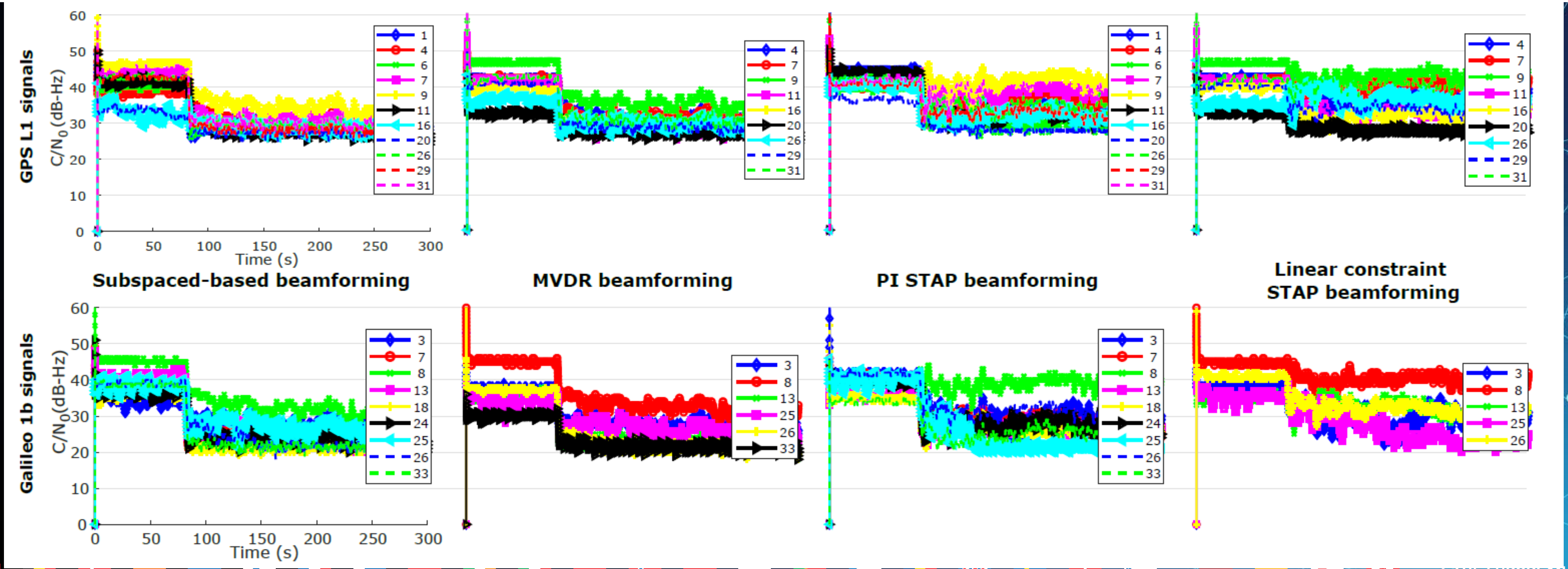
3 Jamming scenario- COTS Jamming



- Three jammers at the same time
- 50 m away from the receiver

3 jammers – multiple algorithms





3 jammers – multiple algorithms

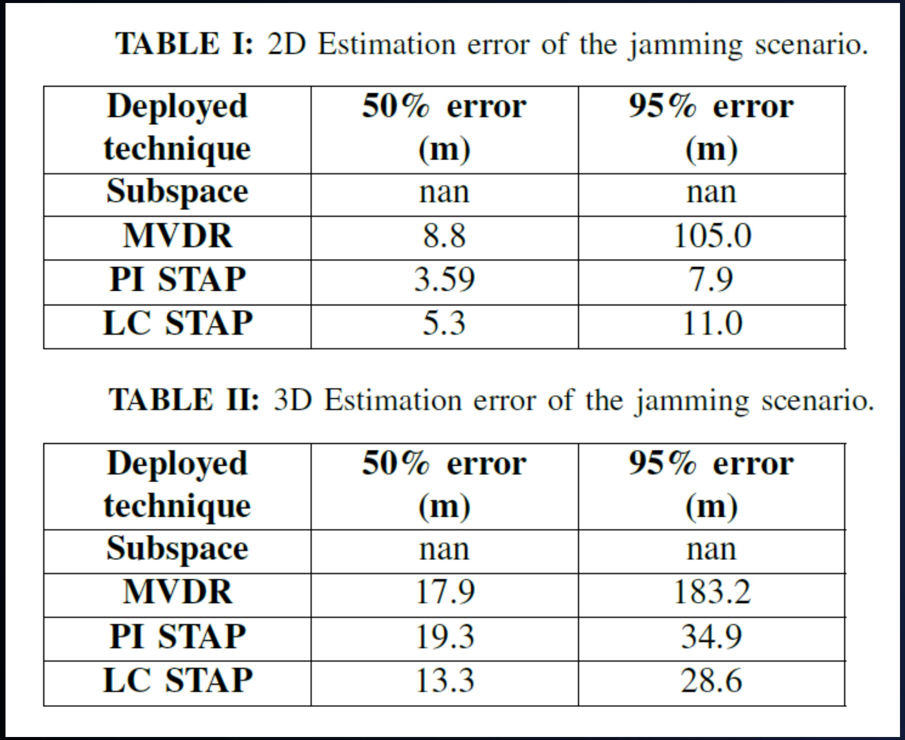
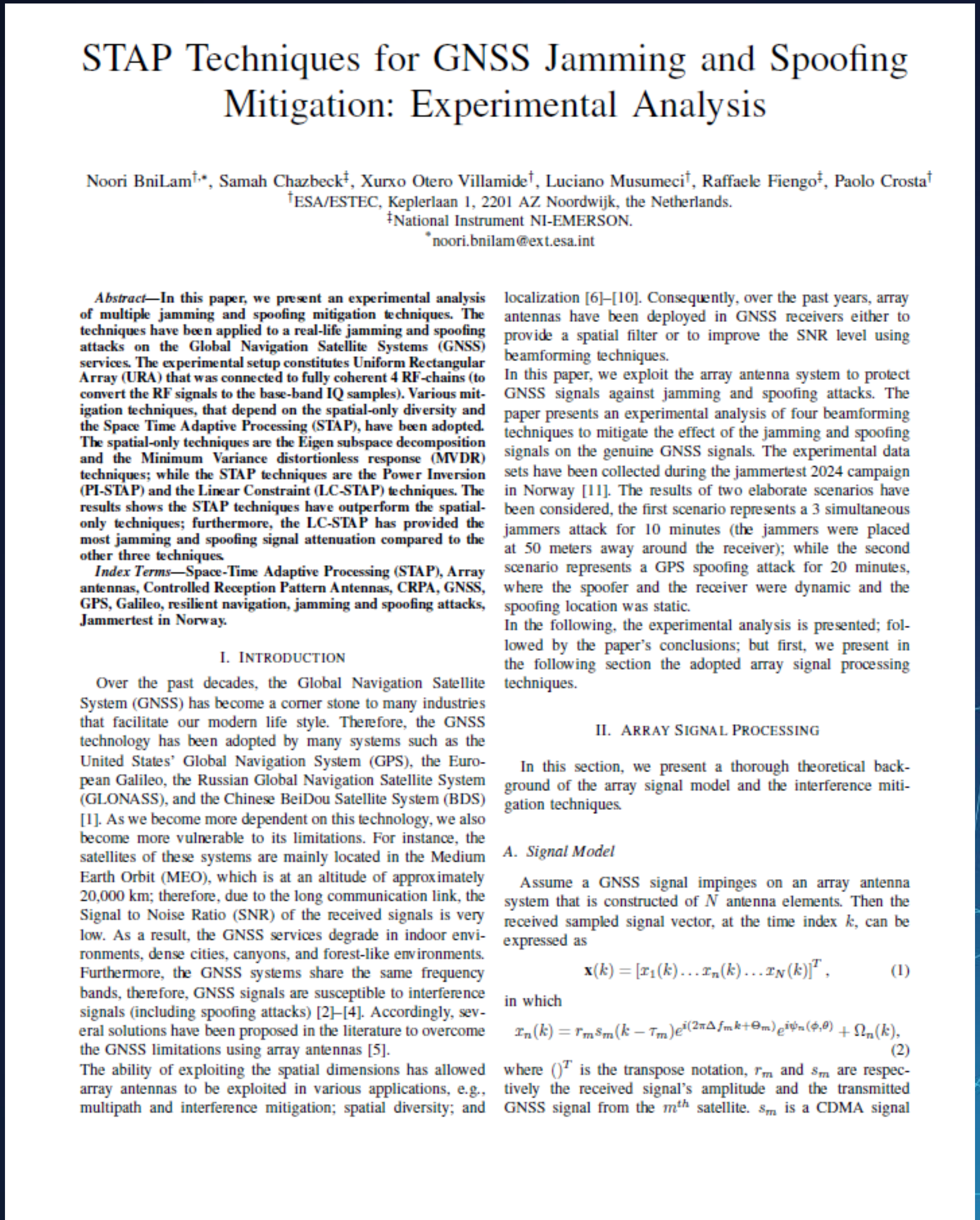


TABLE I: 2D Estimation error of the jamming scenario.

Deployed technique	50% error (m)	95% error (m)
Subspace	nan	nan
MVDR	8.8	105.0
PI STAP	3.59	7.9
LC STAP	5.3	11.0

TABLE II: 3D Estimation error of the jamming scenario.

Deployed technique	50% error (m)	95% error (m)
Subspace	nan	nan
MVDR	17.9	183.2
PI STAP	19.3	34.9
LC STAP	13.3	28.6



STAP Techniques for GNSS Jamming and Spoofing Mitigation: Experimental Analysis

Noori BniLam[†,*], Samah Chazbeck[‡], Xurxo Otero Villamide[†], Luciano Musumeci[†], Raffaele Fiengo[‡], Paolo Crosta[†]
[†]ESA/ESTEC, Keplerlaan 1, 2201 AZ Noordwijk, the Netherlands.
[‡]National Instrument NI-EMERSON.
[*]noori.bnilam@ext.esa.int

***Abstract*—In this paper, we present an experimental analysis of multiple jamming and spoofing mitigation techniques. The techniques have been applied to a real-life jamming and spoofing attacks on the Global Navigation Satellite Systems (GNSS) services. The experimental setup constitutes Uniform Rectangular Array (URA) that was connected to fully coherent 4 RF-chains (to convert the RF signals to the base-band IQ samples). Various mitigation techniques, that depend on the spatial-only diversity and the Space Time Adaptive Processing (STAP), have been adopted. The spatial-only techniques are the Eigen subspace decomposition and the Minimum Variance distortionless response (MVDR) techniques; while the STAP techniques are the Power Inversion (PI-STAP) and the Linear Constraint (LC-STAP) techniques. The results shows the STAP techniques have outperform the spatial-only techniques; furthermore, the LC-STAP has provided the most jamming and spoofing signal attenuation compared to the other three techniques.**

***Index Terms*—Space-Time Adaptive Processing (STAP), Array antennas, Controlled Reception Pattern Antennas, CRPA, GNSS, GPS, Galileo, resilient navigation, jamming and spoofing attacks, Jammertest in Norway.**

I. Introduction

Over the past decades, the Global Navigation Satellite System (GNSS) has become a corner stone to many industries that facilitate our modern life style. Therefore, the GNSS technology has been adopted by many systems such as the United States' Global Navigation System (GPS), the European Galileo, the Russian Global Navigation Satellite System (GLONASS), and the Chinese BeiDou Satellite System (BDS) [1]. As we become more dependent on this technology, we also become more vulnerable to its limitations. For instance, the satellites of these systems are mainly located in the Medium Earth Orbit (MEO), which is at an altitude of approximately 20,000 km; therefore, due to the long communication link, the Signal to Noise Ratio (SNR) of the received signals is very low. As a result, the GNSS services degrade in indoor environments, dense cities, canyons, and forest-like environments. Furthermore, the GNSS systems share the same frequency bands, therefore, GNSS signals are susceptible to interference signals (including spoofing attacks) [2]–[4]. Accordingly, several solutions have been proposed in the literature to overcome the GNSS limitations using array antennas [5].

The ability of exploiting the spatial dimensions has allowed array antennas to be exploited in various applications, e.g., multipath and interference mitigation; spatial diversity; and localization [6]–[10]. Consequently, over the past years, array antennas have been deployed in GNSS receivers either to provide a spatial filter or to improve the SNR level using beamforming techniques.

In this paper, we exploit the array antenna system to protect GNSS signals against jamming and spoofing attacks. The paper presents an experimental analysis of four beamforming techniques to mitigate the effect of the jamming and spoofing signals on the genuine GNSS signals. The experimental data sets have been collected during the jammertest 2024 campaign in Norway [11]. The results of two elaborate scenarios have been considered, the first scenario represents a 3 simultaneous jammers attack for 10 minutes (the jammers were placed at 50 meters away around the receiver); while the second scenario represents a GPS spoofing attack for 20 minutes, where the spoofer and the receiver were dynamic and the spoofing location was static.

In the following, the experimental analysis is presented; followed by the paper's conclusions; but first, we present in the following section the adopted array signal processing techniques.

II. Array Signal Processing

In this section, we present a thorough theoretical background of the array signal model and the interference mitigation techniques.

A. Signal Model

Assume a GNSS signal impinges on an array antenna system that is constructed of N antenna elements. Then the received sampled signal vector, at the time index k, can be expressed as

$$\mathbf{x}(k) = [x_1(k) \dots x_n(k) \dots x_N(k)]^T , \qquad (1)$$

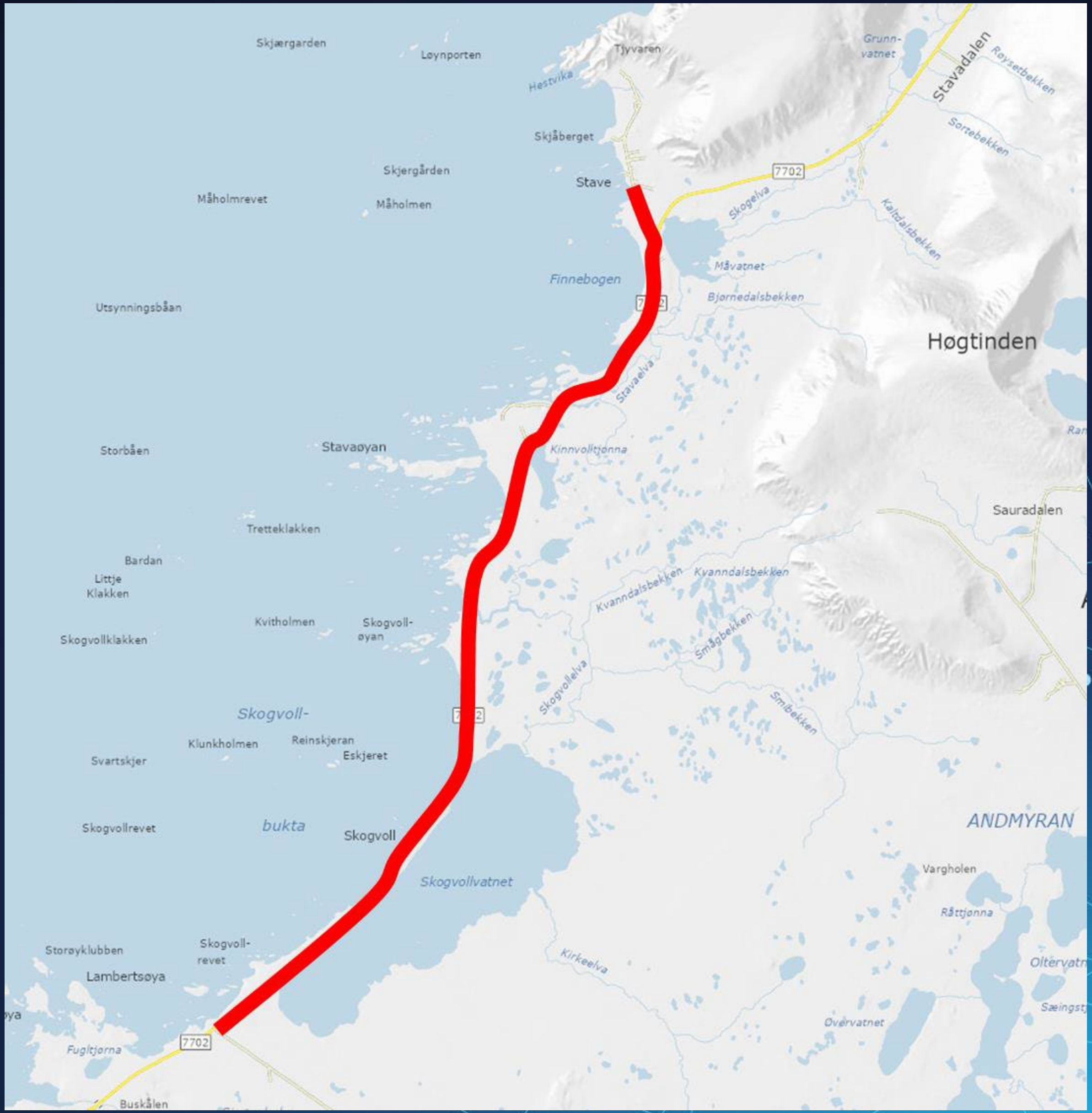
in which

$$x_n(k) = r_m s_m(k - \tau_m) e^{i(2\pi \Delta f_m k + \Theta_m)} e^{i\psi_n(\phi,\theta)} + \Omega_n(k), \qquad (2)$$

where $()^T$ is the transpose notation, r_m and s_m are respectively the received signal's amplitude and the transmitted GNSS signal from the m^{th} satellite. s_m is a CDMA signal

Andoya Jammertest - Motorcade

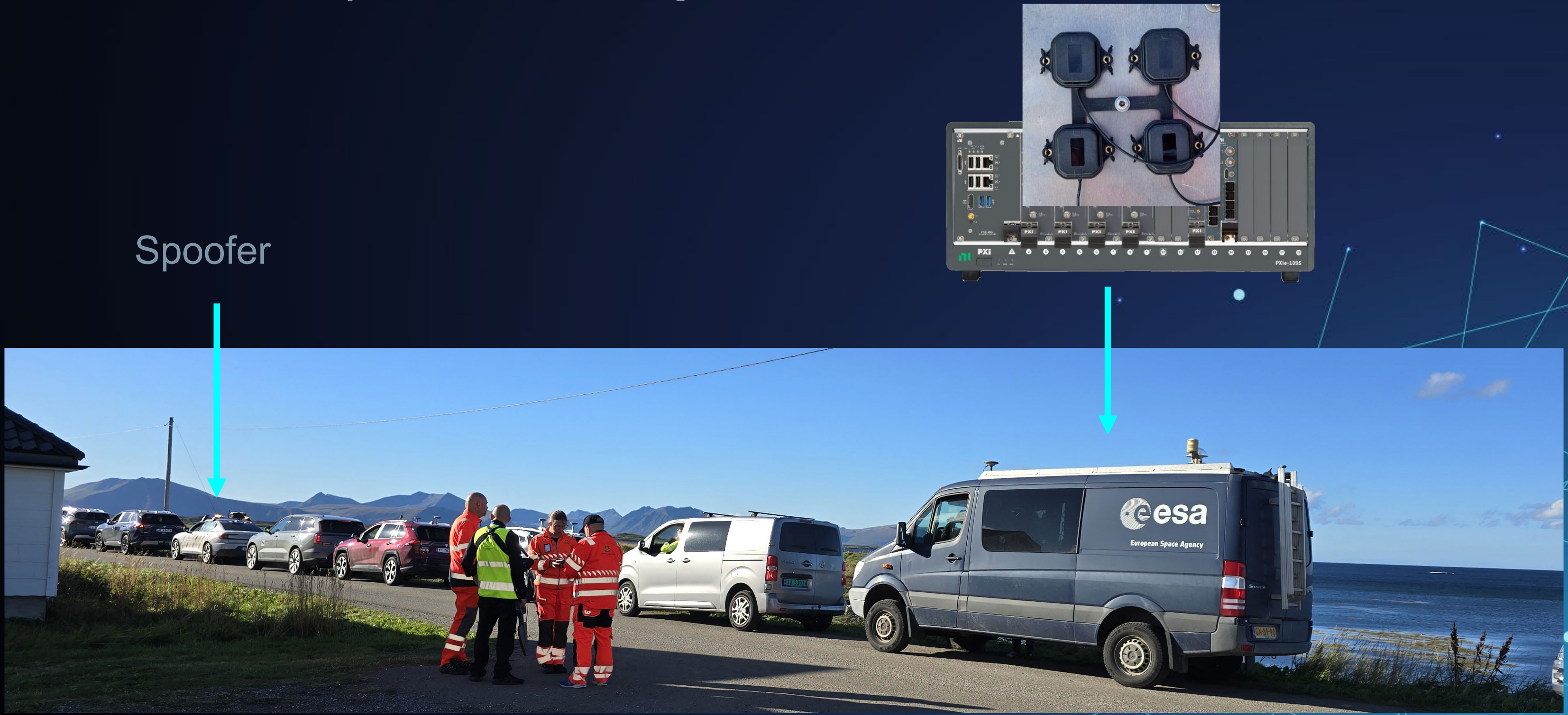
- Mobile spoofer, the spoofer in the middle of the motorcade
- Static spoofing location
- Static with a large jump spoofing location
- Mobile spoofing car with a different trajectory
- …



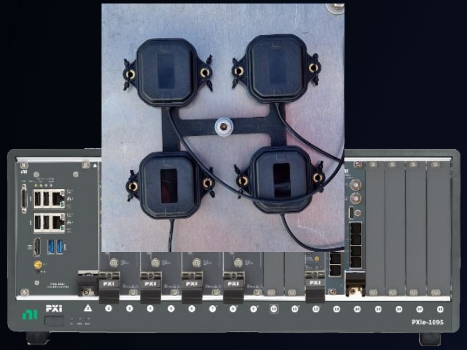
Motorcade jamming and spoofing

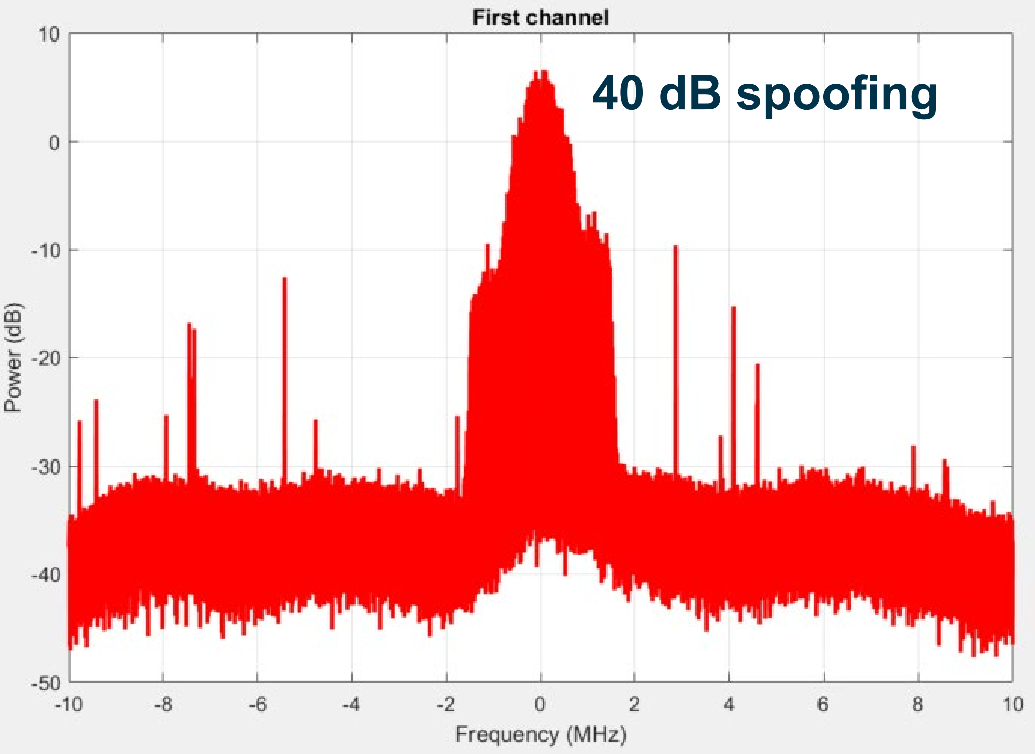
Spoofing L1 GPS – scenario 2.6.2

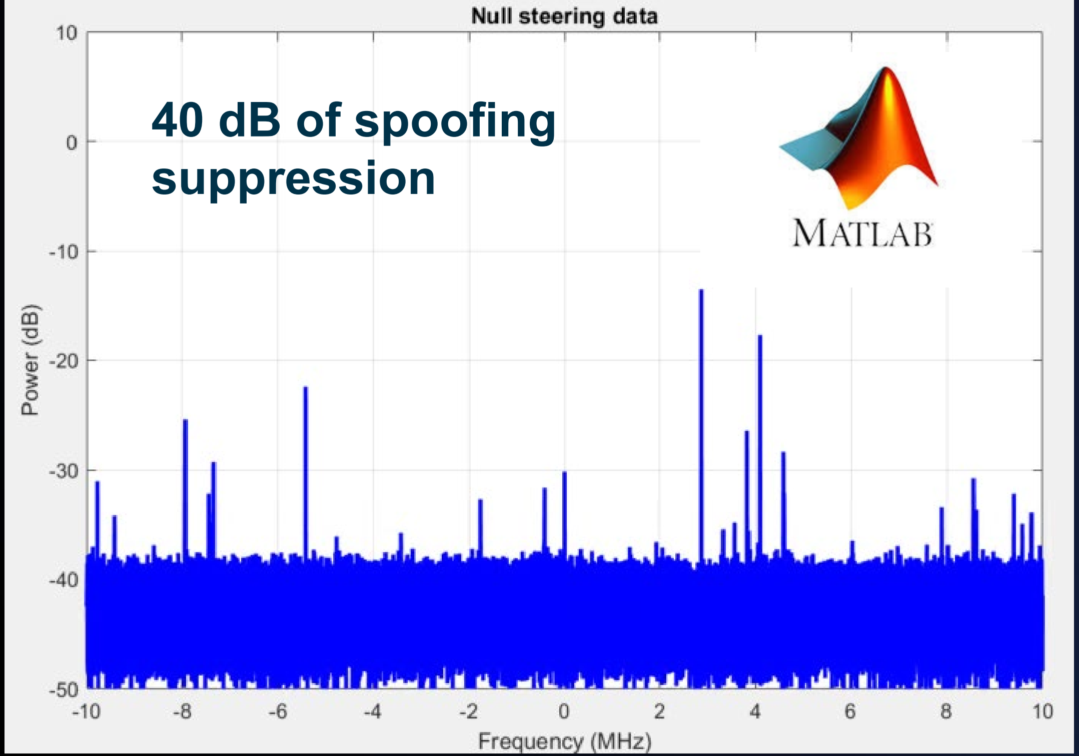
- The spoofer moves in the middle of the motorcade
- The spoofer deploy GPS L1 spoofing only
- Spoofing location is static, and it is the same as the start point
- 10 minutes static followed by 10 minutes driving



Spoofing L1 GPS – scenario 2.6.2



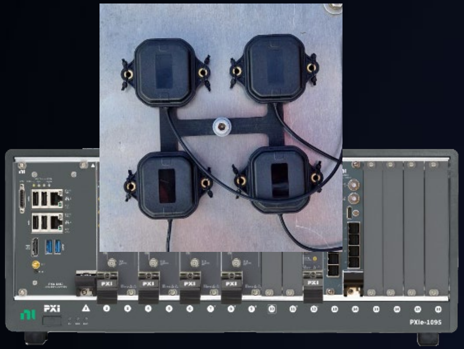


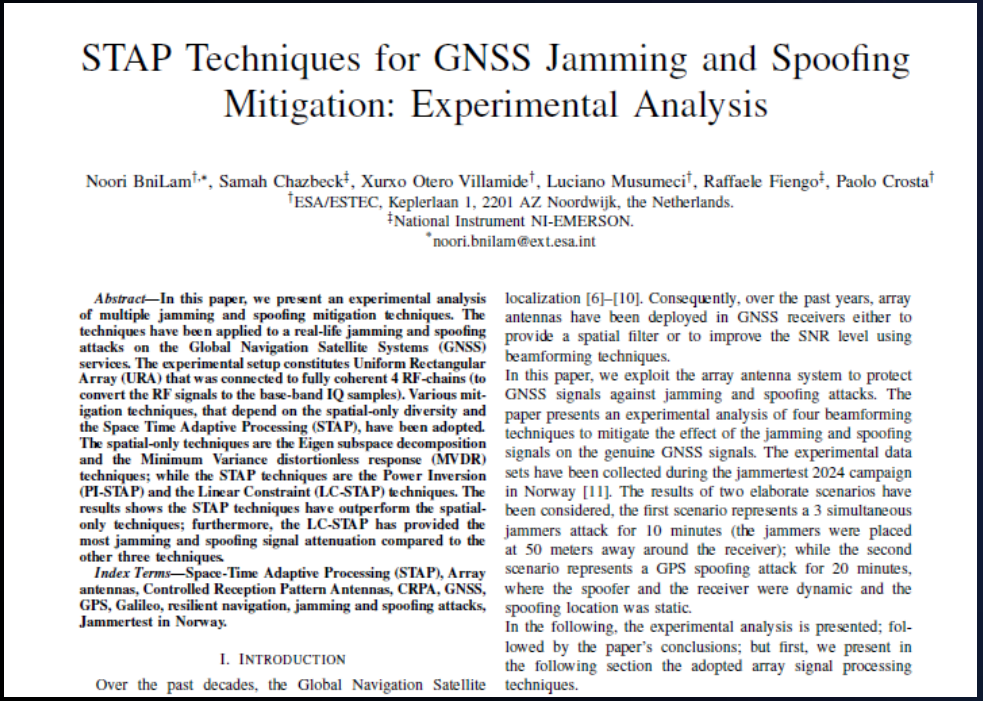


E1 only - 20 MHz BW – STAP 20TDL

O. L. Frost, "An algorithm for linearly constrained adaptive array processing," Proceedings of the IEEE, vol. 60, no. 8, pp. 926–935, 1972.

Spoofing L1 GPS – scenario 2.6.2





STAP Techniques for GNSS Jamming and Spoofing Mitigation: Experimental Analysis

Noori BniLam[†,*], Samah Chazbeck[‡], Xurxo Otero Villamide[†], Luciano Musumeci[†], Raffaele Fiengo[‡], Paolo Crosta[†]
[†]ESA/ESTEC, Keplerlaan 1, 2201 AZ Noordwijk, the Netherlands.
[‡]National Instrument NI-EMERSON.
[*]noori.bnilam@ext.esa.int

***Abstract*—In this paper, we present an experimental analysis of multiple jamming and spoofing mitigation techniques. The techniques have been applied to a real-life jamming and spoofing attacks on the Global Navigation Satellite Systems (GNSS) services. The experimental setup constitutes Uniform Rectangular Array (URA) that was connected to fully coherent 4 RF-chains (to convert the RF signals to the base-band IQ samples). Various mitigation techniques, that depend on the spatial-only diversity and the Space Time Adaptive Processing (STAP), have been adopted. The spatial-only techniques are the Eigen subspace decomposition and the Minimum Variance distortionless response (MVDR) techniques; while the STAP techniques are the Power Inversion (PI-STAP) and the Linear Constraint (LC-STAP) techniques. The results shows the STAP techniques have outperform the spatial-only techniques; furthermore, the LC-STAP has provided the most jamming and spoofing signal attenuation compared to the other three techniques.**

***Index Terms*—Space-Time Adaptive Processing (STAP), Array antennas, Controlled Reception Pattern Antennas, CRPA, GNSS, GPS, Galileo, resilient navigation, jamming and spoofing attacks, Jammertest in Norway.**

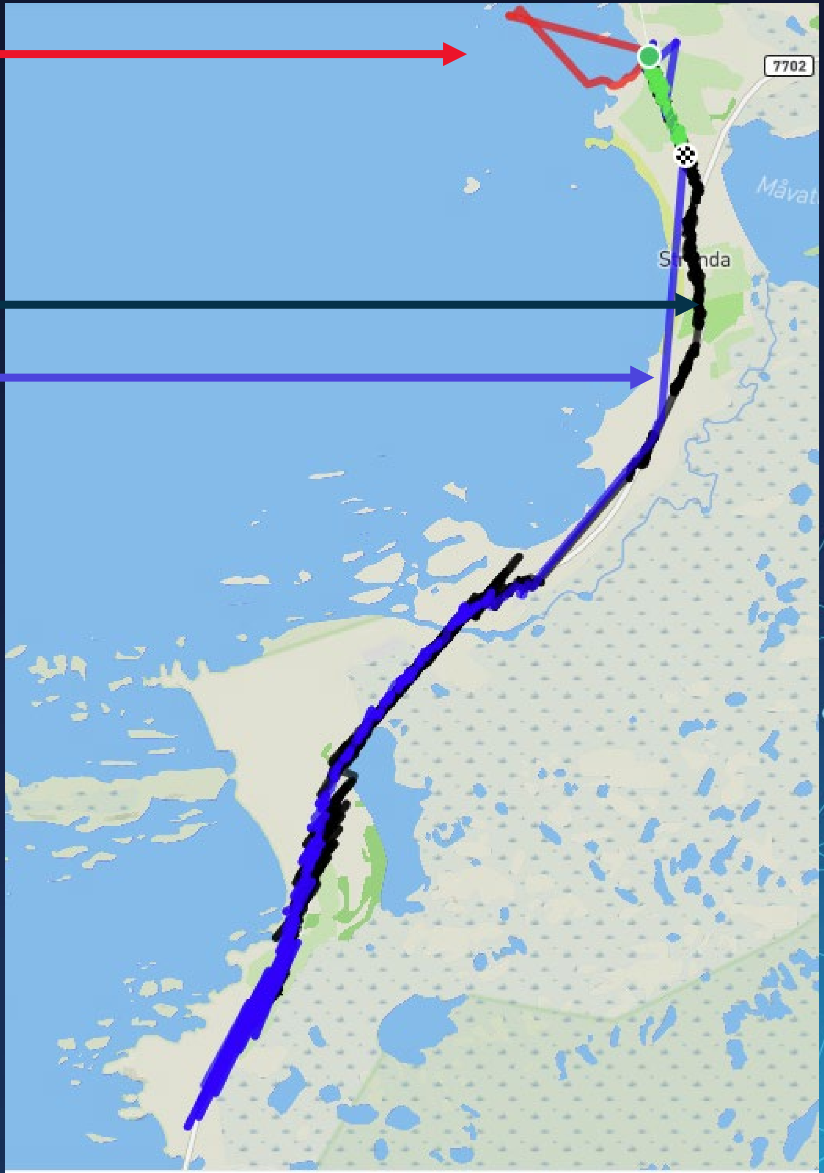
I. Introduction

Over the past decades, the Global Navigation Satellite

localization [6]–[10]. Consequently, over the past years, array antennas have been deployed in GNSS receivers either to provide a spatial filter or to improve the SNR level using beamforming techniques.

In this paper, we exploit the array antenna system to protect GNSS signals against jamming and spoofing attacks. The paper presents an experimental analysis of four beamforming techniques to mitigate the effect of the jamming and spoofing signals on the genuine GNSS signals. The experimental data sets have been collected during the jammertest 2024 campaign in Norway [11]. The results of two elaborate scenarios have been considered, the first scenario represents a 3 simultaneous jammers attack for 10 minutes (the jammers were placed at 50 meters away around the receiver); while the second scenario represents a GPS spoofing attack for 20 minutes, where the spoofer and the receiver were dynamic and the spoofing location was static.

In the following, the experimental analysis is presented; followed by the paper's conclusions; but first, we present in the following section the adopted array signal processing techniques.



Spoofed single antenna

Trajectory

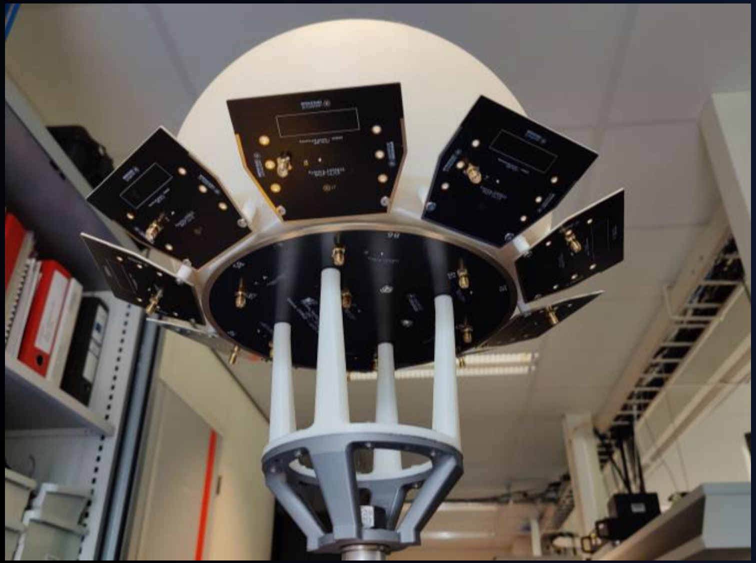
Null steering

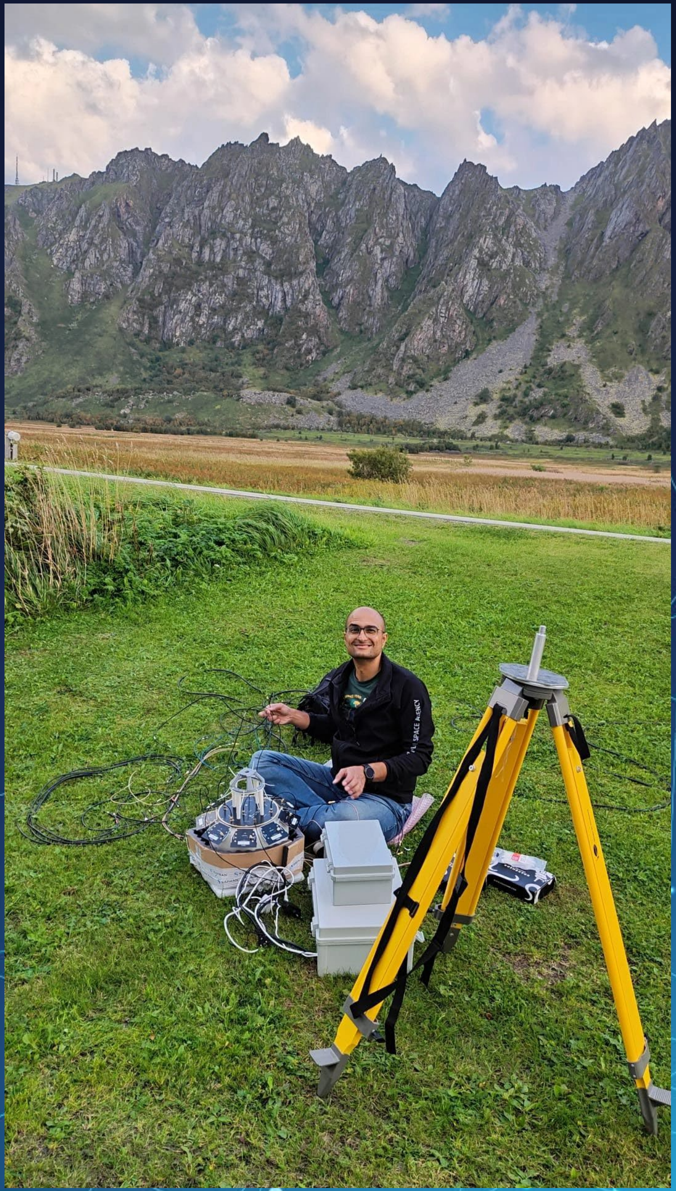
Presentation Outline

- Jammertest 2024 → Program & Locations
- ESA Jammertest → Logistics and setups
- Resilient Navigation → Scenarios, Mobile and **Sensor station**

Analog Beamforming

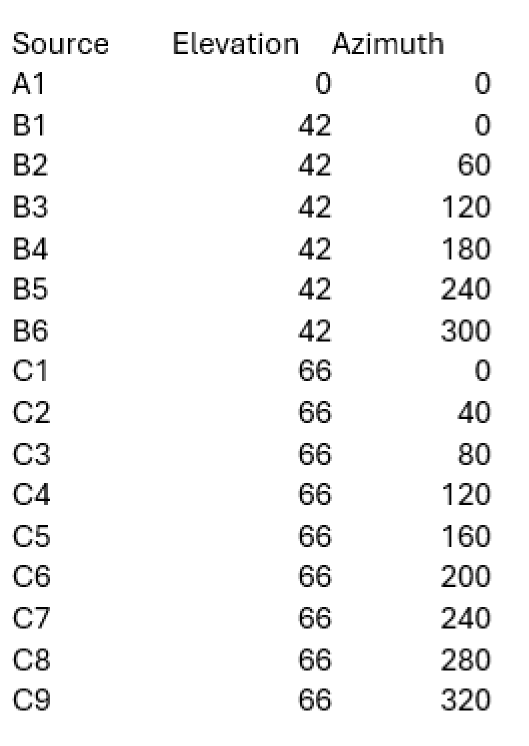
- 16 beams Luneburg lens antenna system with dual frequency sources
- Antenna centre looks at the zenith direction, 5 inner circle antennas, and 9 tilted outer circle antennas
- The antennas have RHCP polarization
- 16 GNSS receivers



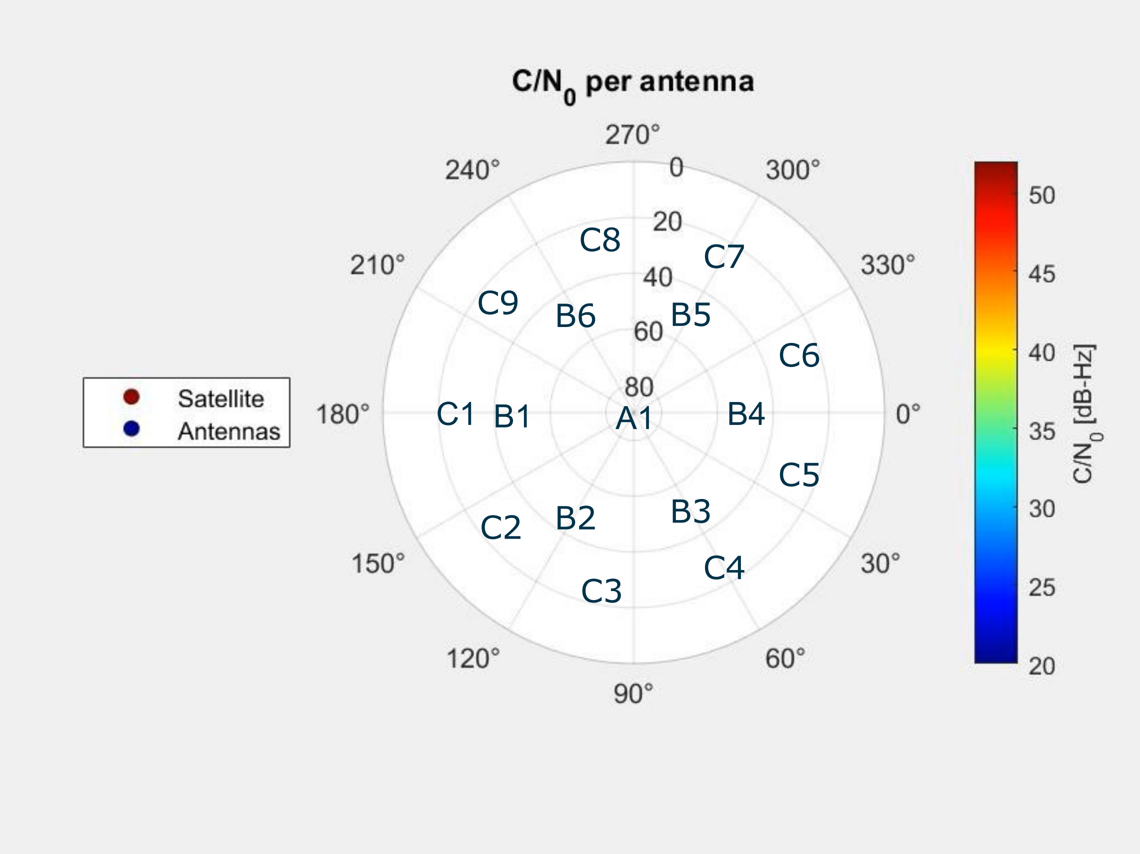


Look directions

- 16 beams in 3 orders with a symmetry of revolution
- Every beam covers a region of the sky view

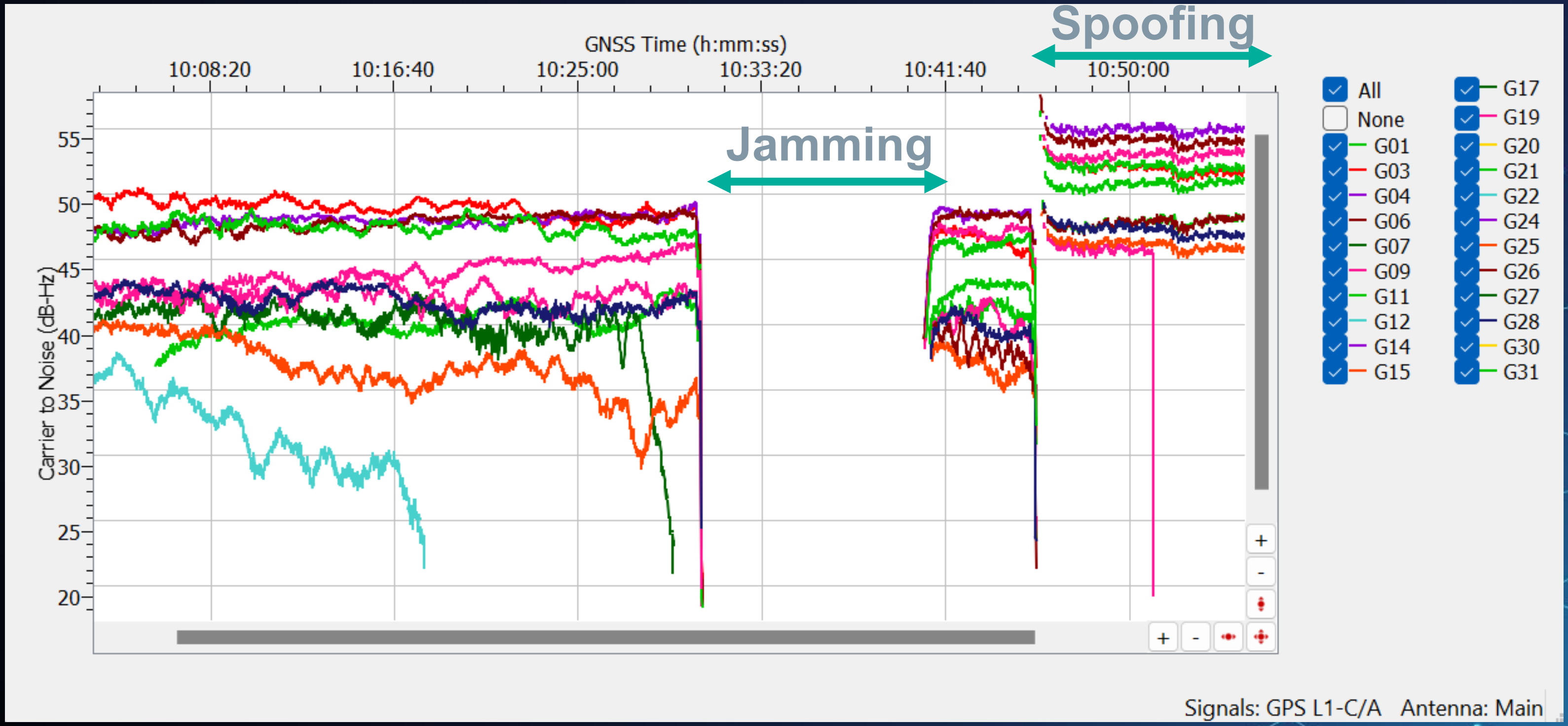


Source	Elevation	Azimuth
A1	0	0
B1	42	0
B2	42	60
B3	42	120
B4	42	180
B5	42	240
B6	42	300
C1	66	0
C2	66	40
C3	66	80
C4	66	120
C5	66	160
C6	66	200
C7	66	240
C8	66	280
C9	66	320



Jamming and spoofing scenario

- The scenario starts in nominal conditions (i.e. only with genuine signals)
- Then, the transmission of a PRN like signal with a power of 1W starts in L1
- After that, the transmission of the signal is stopped
- Finally, after few minutes, spoofing signals are transmitted
- Results below from Test User Receiver (SSN) + NavX 3G+C antenna

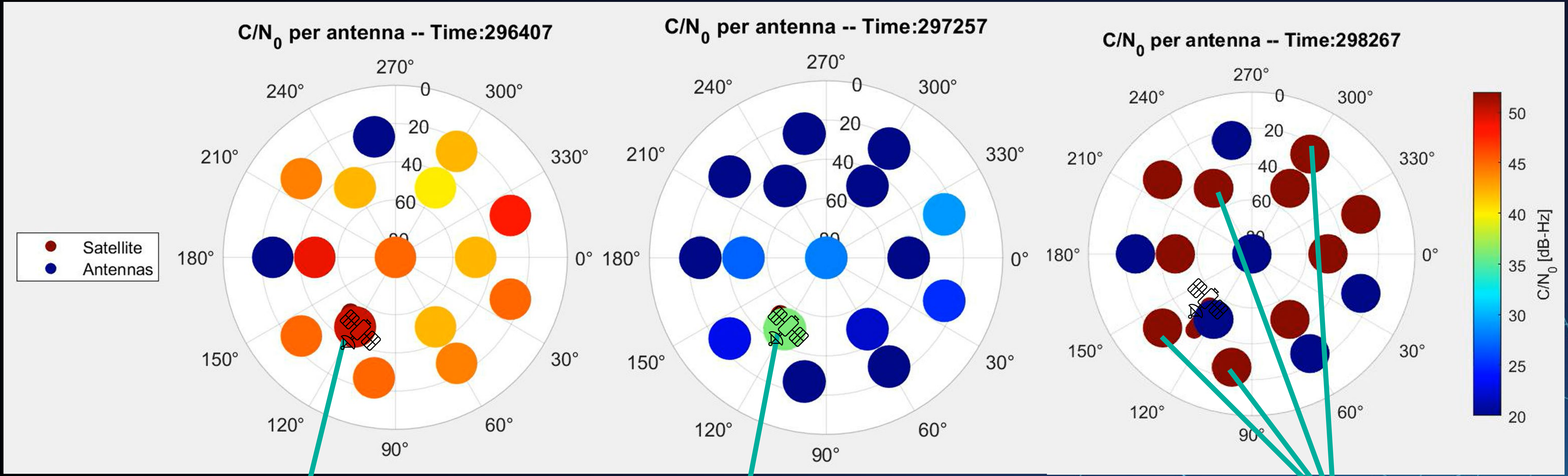


Jamming and spoofing attacks

Genuine

Jamming

Spoofing+Genuine



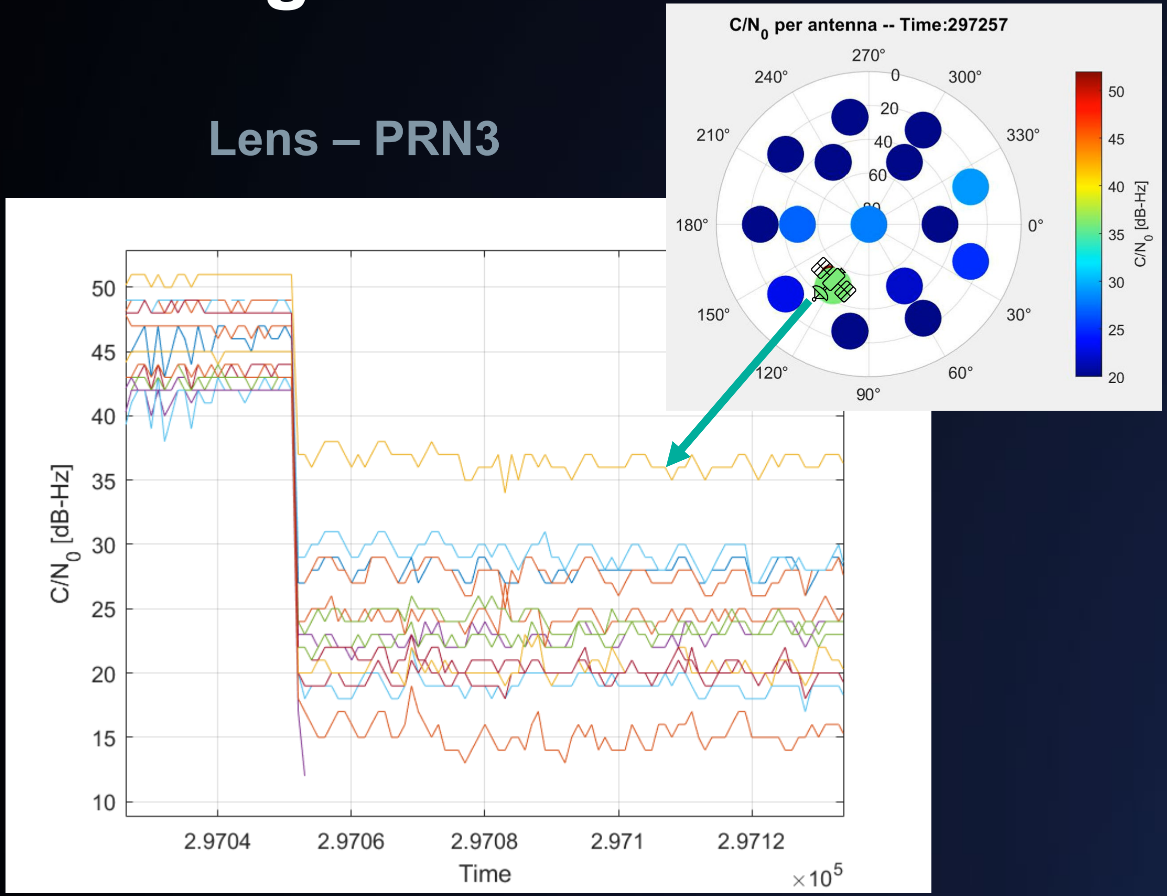
In nominal conditions, the Rx pointing to the satellite shows the highest C/N0

The Rx pointing to the satellite shows higher resilience against jamming

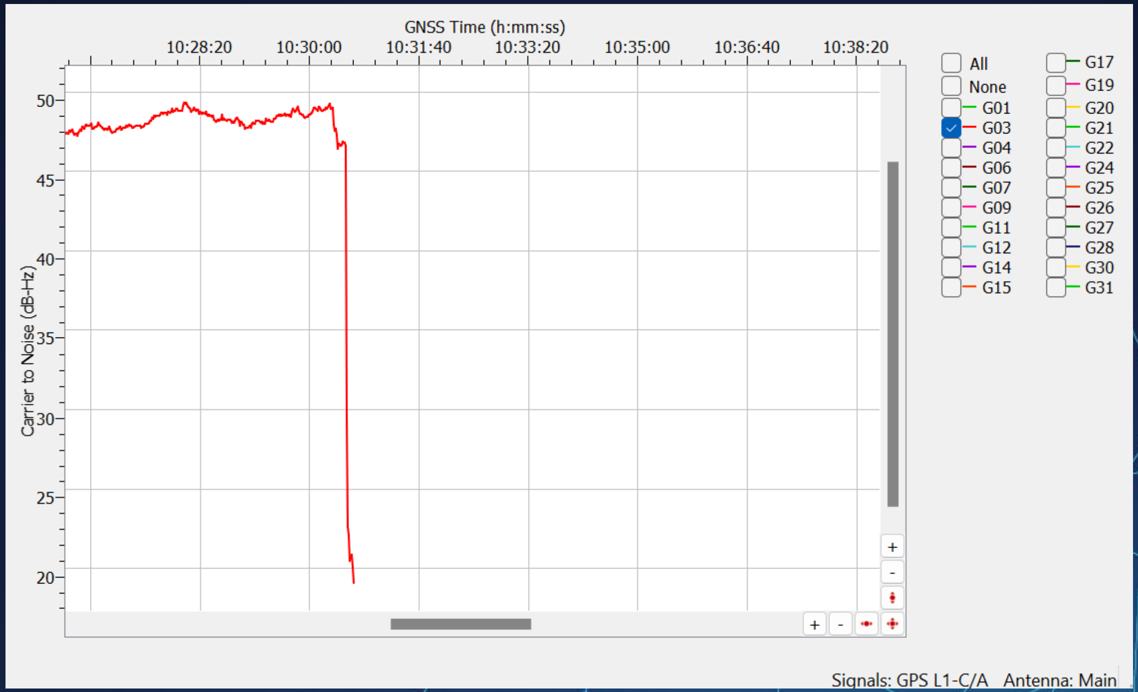
In the presence of a spoofer, several beams pointing to different directions show the highest magnitudes. This reaction can help to estimate the presence of the spoofer

Jamming attack - lens vs omnidirectional

Lens – PRN3



Omnidirectional NavX – PRN3



Signals: GPS L1-C/A   Antenna: Main

The lens provides protection against spoofing attacks

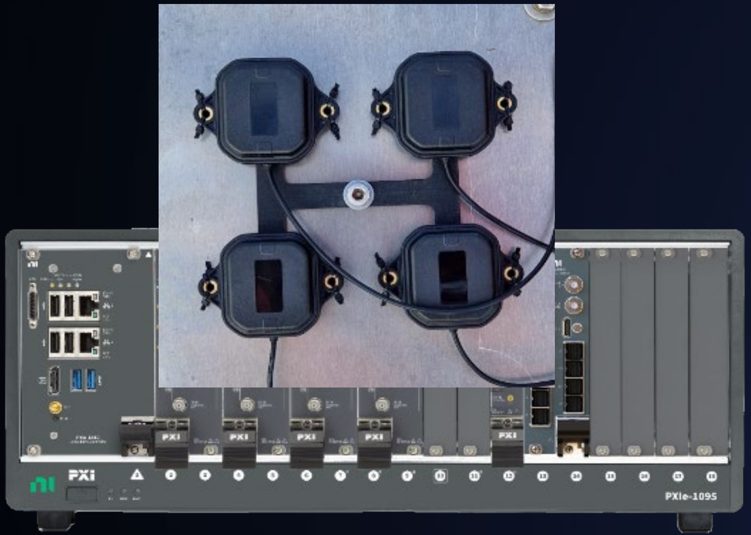
When the jamming starts, the signal is completely lost

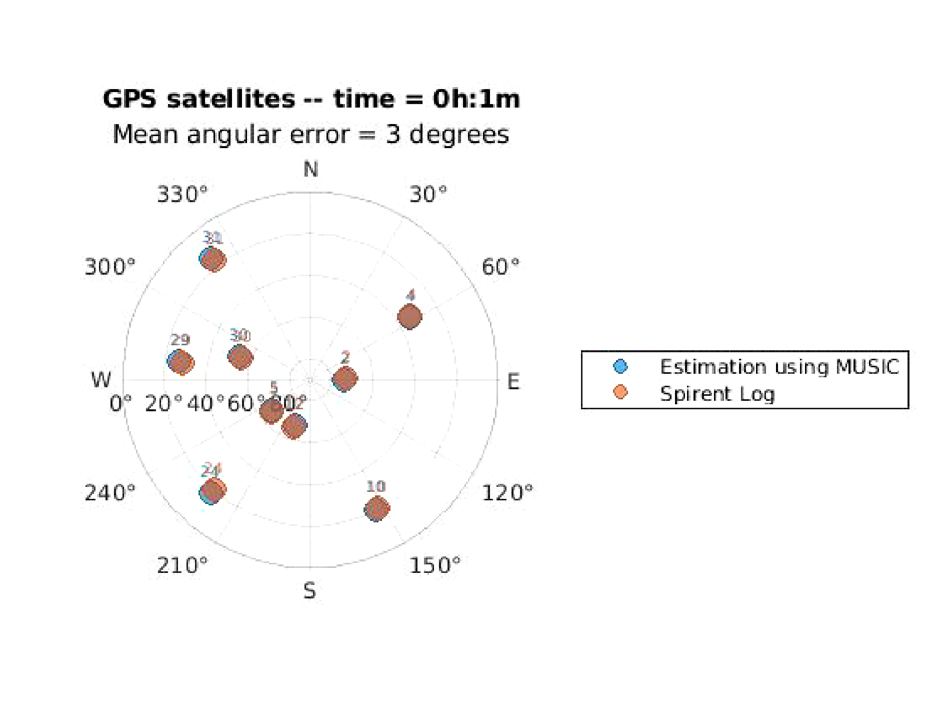
Presentation Outline

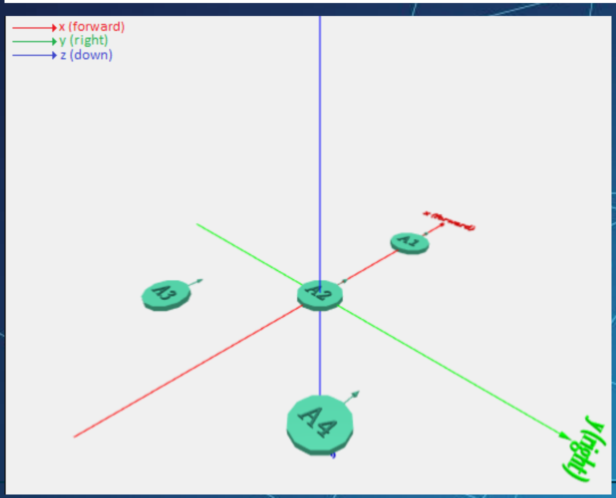
- Jammertest 2024 → Program & Locations
- ESA Jammertest → Logistics and setups
- Resilient Navigation → Scenarios, Results and Analysis.
- Technology Level → NAVISP

Support Technology Programs (NAVISP)

- We have tested the ADGIL HW (NAVISP EL3-027 project)







Phase Mean <0.5°
Phase STD <0.05°
Amplitude Mean <0.1dB
Amplitude STD <0.01 dB

Support Technology Programs (NAVISP)

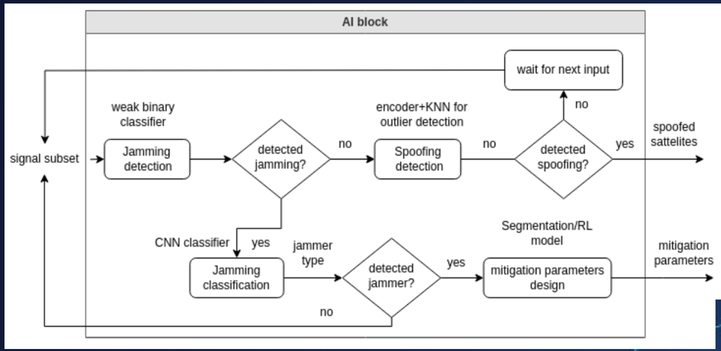
NAVISP EL1–064 (BlockBox)

Main HW features

- 3U Rack-mountable case (HxWxD 13x48x45 cm)
- 100-240 VAC power input, 70 W
- Based on Zynq Ultrascale+ MPSoC ZCU102 (XCZU9EG)
  - Quad-core ARM Cortex A53, Dual-core Cortex R5F, Mali-400 GPU
  - FPGA
  - DDR4, PCIe gen 2 x4, SATA, USB 3.0, SGMII, UART, CAN
- AD9082-FMCA-EBZ ADC/DAC board
  - 2 ADC (6 GSPS), 4 DAC (12 GSPS)
  - 8 channel channelizer (DDC, DUC)
  - HMC7044 clock management
- 2 RF inputs, 5 V antenna feed provided
- 4 RF outputs (2 in use)
- 2 TB internal SSD storage
- 1 Gb/s Ethernet

Tested in the lab with data recorded during Jammertest in the field (live interference plus environmental effects like multipath)

Test setup:


AI block

signal subset

weak binary classifier

Jamming detection

detected jamming?

no

encoder+KNN for outlier detection

Spoofing detection

no

detected spoofing?

no

wait for next input

yes

spoofed sattelites

CNN classifier

yes

Jamming classification

jammer type

detected jammer?

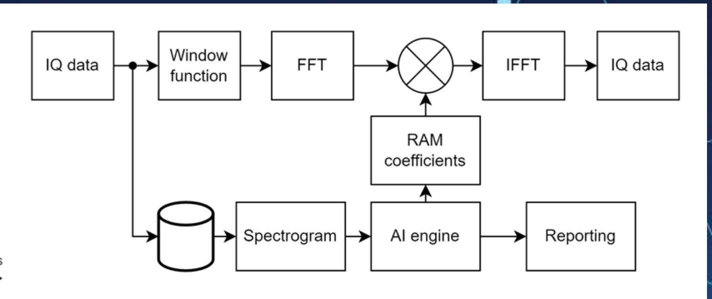
no

yes

Segmentation/RL model

mitigation parameters design

mitigation parameters


IQ data

Window function

FFT

IFFT

IQ data

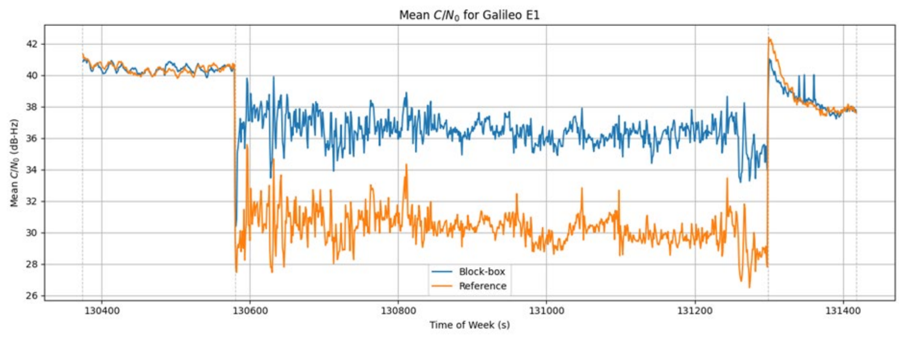
RAM coefficients

Spectrogram

AI engine

Reporting

BlockBox vs standard Rx under Wide Band RFI

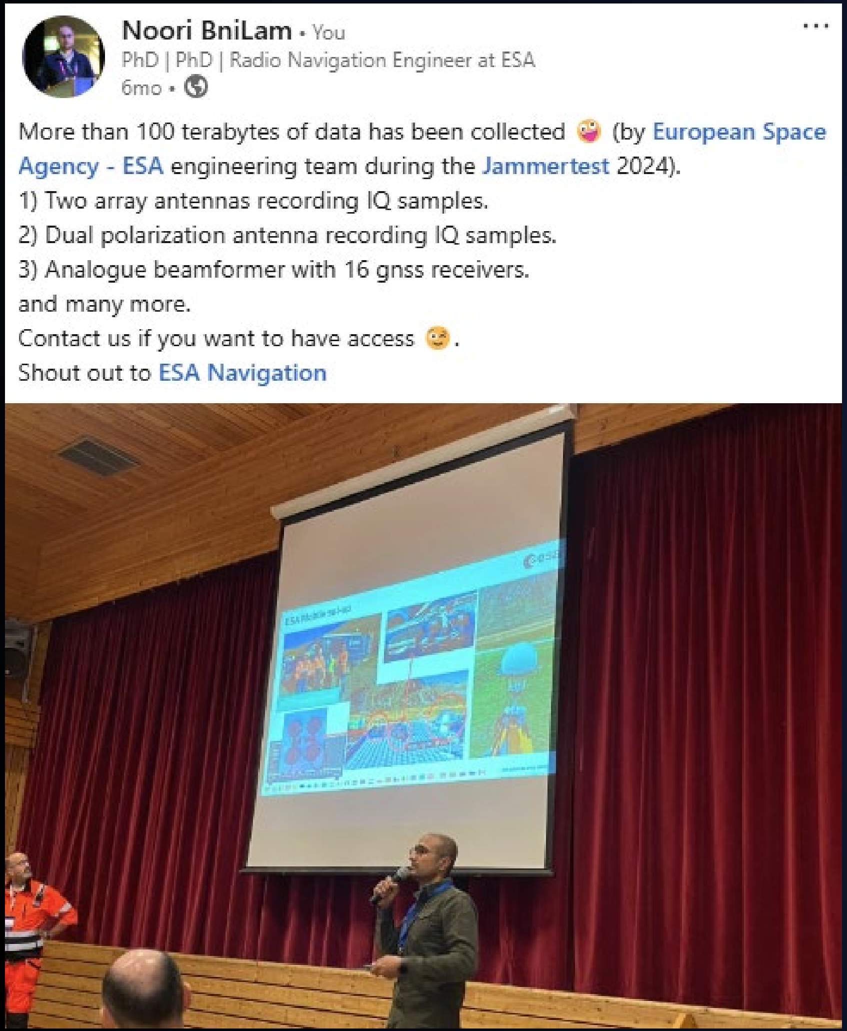


Presentation Outline

- Jammertest 2024 → Program & Locations
- ESA Jammertest → Logistics and setups
- Resilient Navigation → Scenarios, Results and Analysis.
- Technology Level → NAVISP
- Exposure → Achievements and public relations

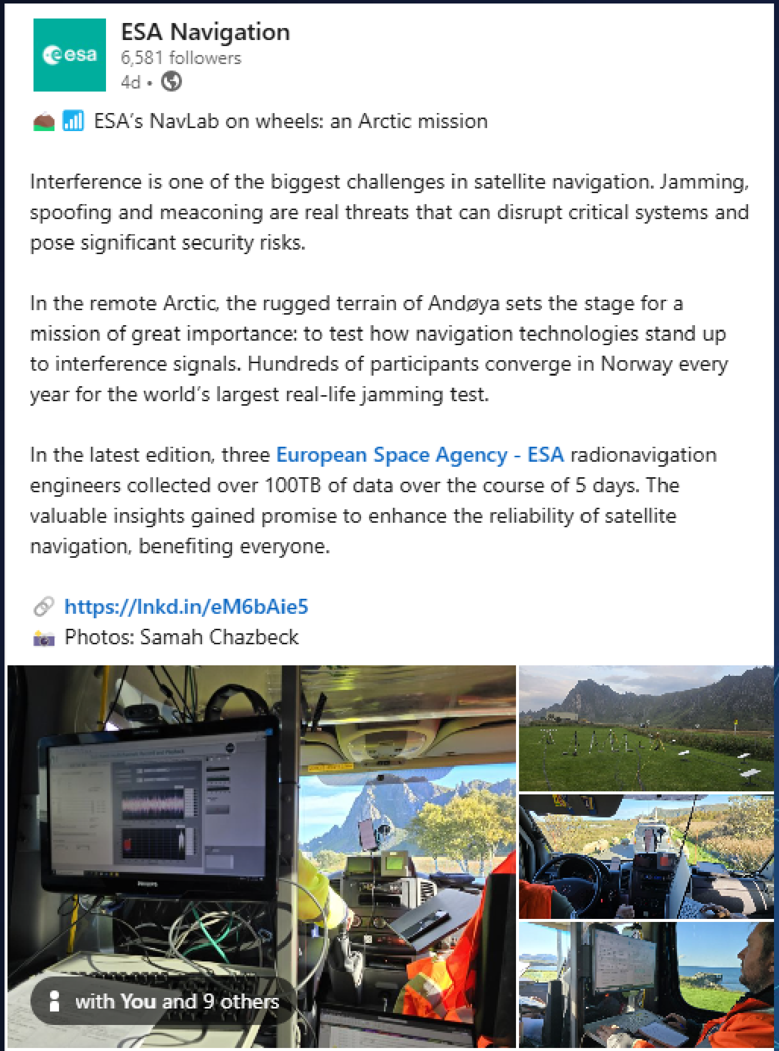
Support to ESTEC Nav-Lab

100 TB of data have been collected!



Noori BniLam • You
PhD | PhD | Radio Navigation Engineer at ESA
6mo •

More than 100 terabytes of data has been collected 🤪 (by European Space Agency - ESA engineering team during the Jammertest 2024).
1) Two array antennas recording IQ samples.
2) Dual polarization antenna recording IQ samples.
3) Analogue beamformer with 16 gnss receivers.
and many more.
Contact us if you want to have access 😉.
Shout out to ESA Navigation



ESA Navigation
6,581 followers
4d •

🏔️ 📶 ESA's NavLab on wheels: an Arctic mission

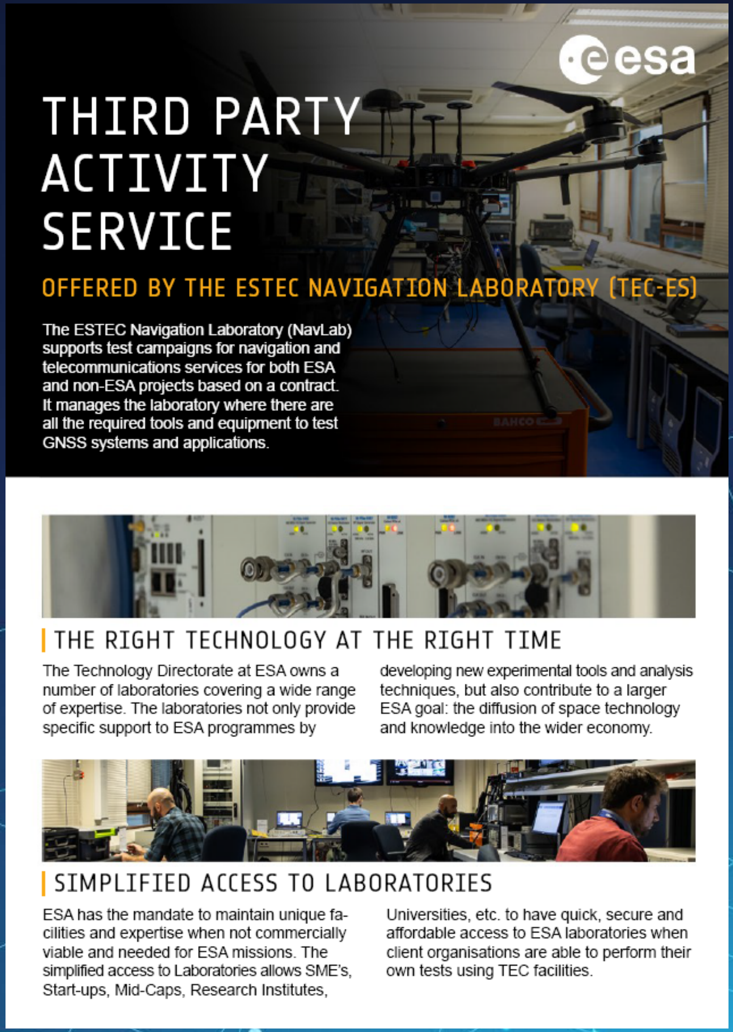
Interference is one of the biggest challenges in satellite navigation. Jamming, spoofing and meaconing are real threats that can disrupt critical systems and pose significant security risks.

In the remote Arctic, the rugged terrain of Andøya sets the stage for a mission of great importance: to test how navigation technologies stand up to interference signals. Hundreds of participants converge in Norway every year for the world's largest real-life jamming test.

In the latest edition, three European Space Agency - ESA radionavigation engineers collected over 100TB of data over the course of 5 days. The valuable insights gained promise to enhance the reliability of satellite navigation, benefiting everyone.

🔗 https://lnkd.in/eM6bAie5
📷 Photos: Samah Chazbeck

with You and 9 others



THIRD PARTY ACTIVITY SERVICE

OFFERED BY THE ESTEC NAVIGATION LABORATORY (TEC-ES)

The ESTEC Navigation Laboratory (NavLab) supports test campaigns for navigation and telecommunications services for both ESA and non-ESA projects based on a contract. It manages the laboratory where there are all the required tools and equipment to test GNSS systems and applications.

THE RIGHT TECHNOLOGY AT THE RIGHT TIME

The Technology Directorate at ESA owns a number of laboratories covering a wide range of expertise. The laboratories not only provide specific support to ESA programmes by developing new experimental tools and analysis techniques, but also contribute to a larger ESA goal: the diffusion of space technology and knowledge into the wider economy.

SIMPLIFIED ACCESS TO LABORATORIES

ESA has the mandate to maintain unique facilities and expertise when not commercially viable and needed for ESA missions. The simplified access to Laboratories allows SME's, Start-ups, Mid-Caps, Research Institutes, Universities, etc. to have quick, secure and affordable access to ESA laboratories when client organisations are able to perform their own tests using TEC facilities.

Thanks for your attention!

- Info: navisp.esa.int / www.linkedin.com/company/navisp-esa
- Questions: navisp@esa.int
- Subscribe to **navisp** newsletter!