Anomaly Detection in Raw GNSS Data

Critical infrastructure protection against GNSS spoofing

Maksim Barodzka
CEO @ GPSPATRON

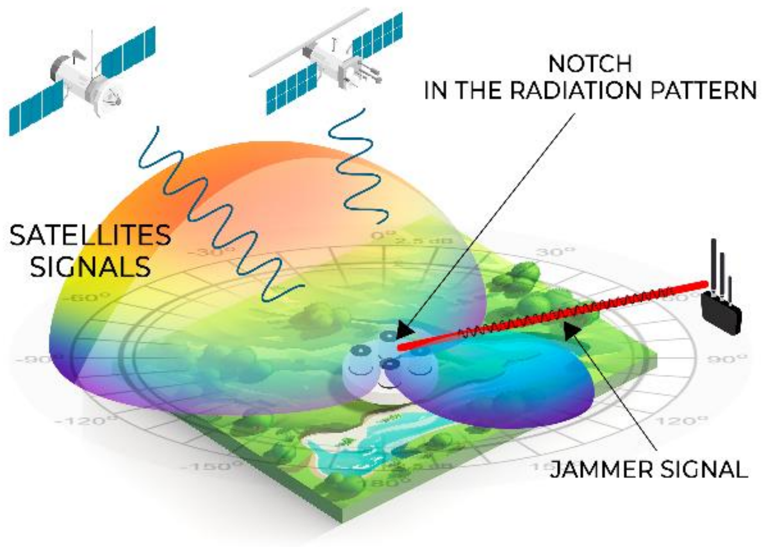
www.gpspatron.com www.youtube.com/c/GPSPATRON twitter.com/gpspatron

Techniques to protect a GNSS receiver from spoofing

Sophisticated Antenna Systems

Null Steering

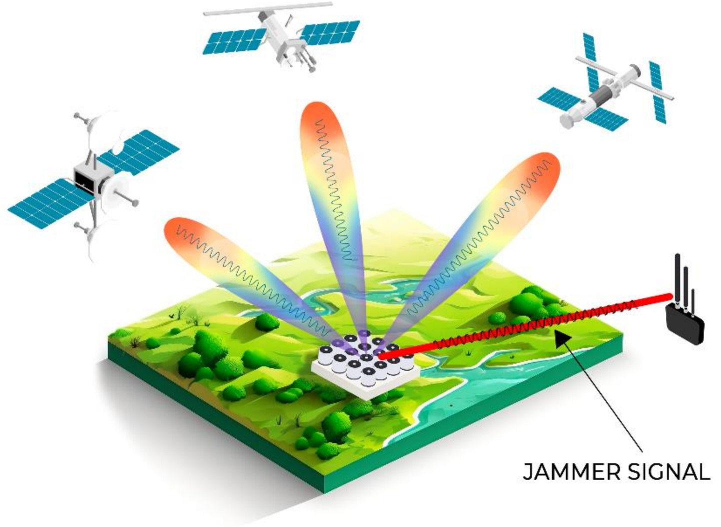
It creates "dead zones" to block fake signals.



- Real efficiency starts at 4 antenna elements.
- 40-60 dB interference suppression level.
- Effective against jamming and partially against spoofing

Beamforming

It strengthens authentic signals and weakens fake ones, making real signals clear.

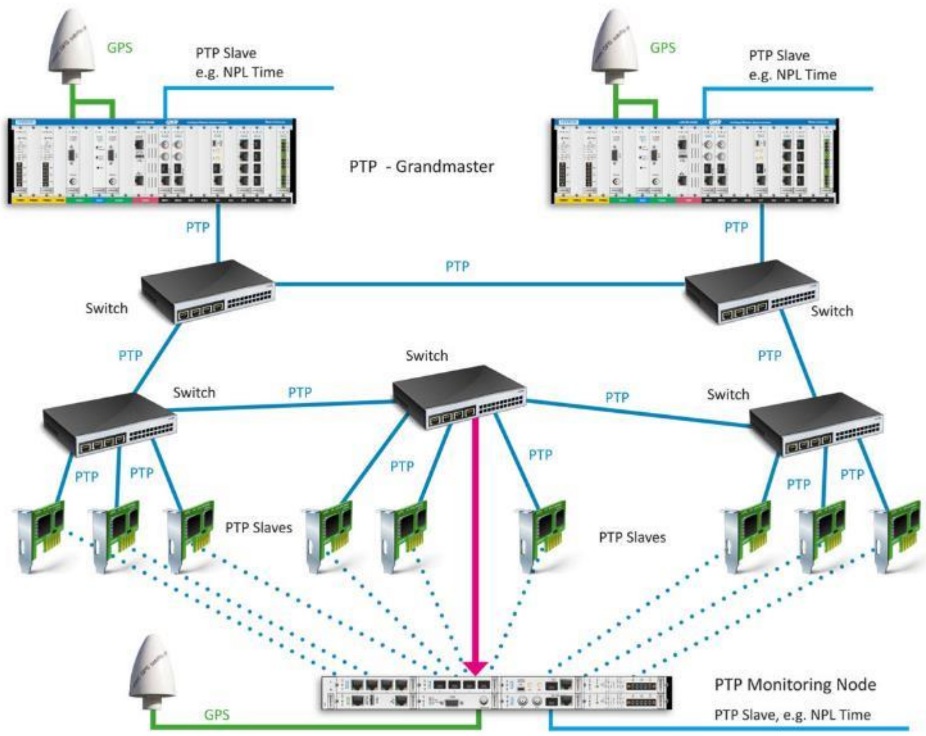


- Requires 8-16 antenna elements.
- High cost, large size and power consumption
- Acceptable technique to counteract low-power GNSS spoofing

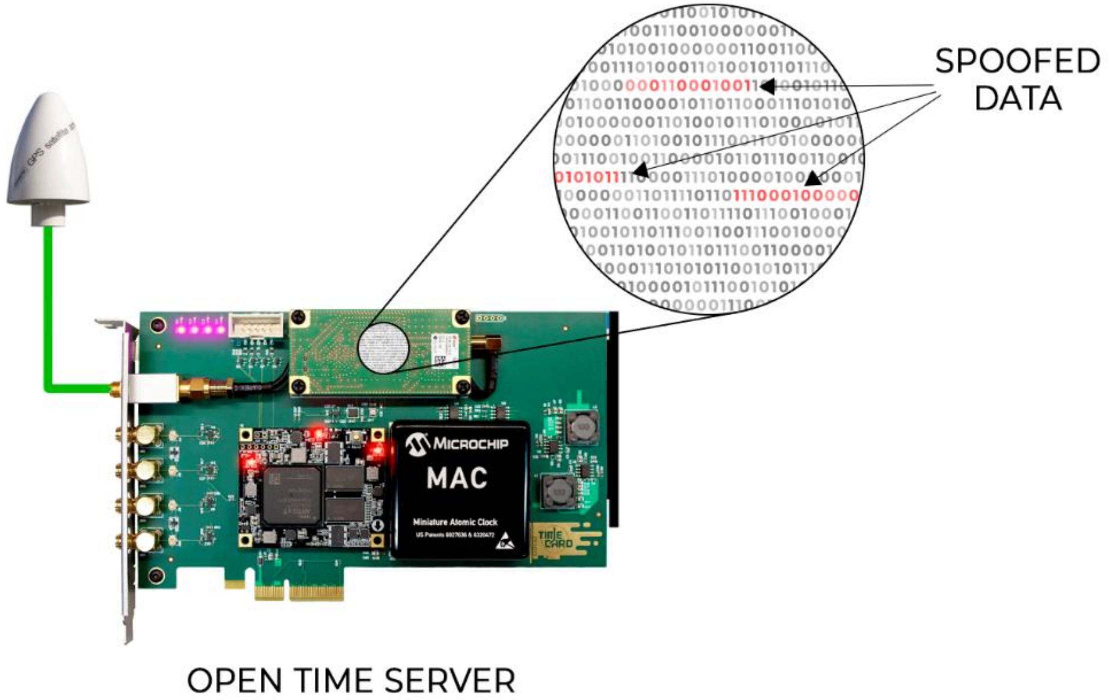
Techniques to protect a GNSS receiver from spoofing

Detect & Switch to Backup

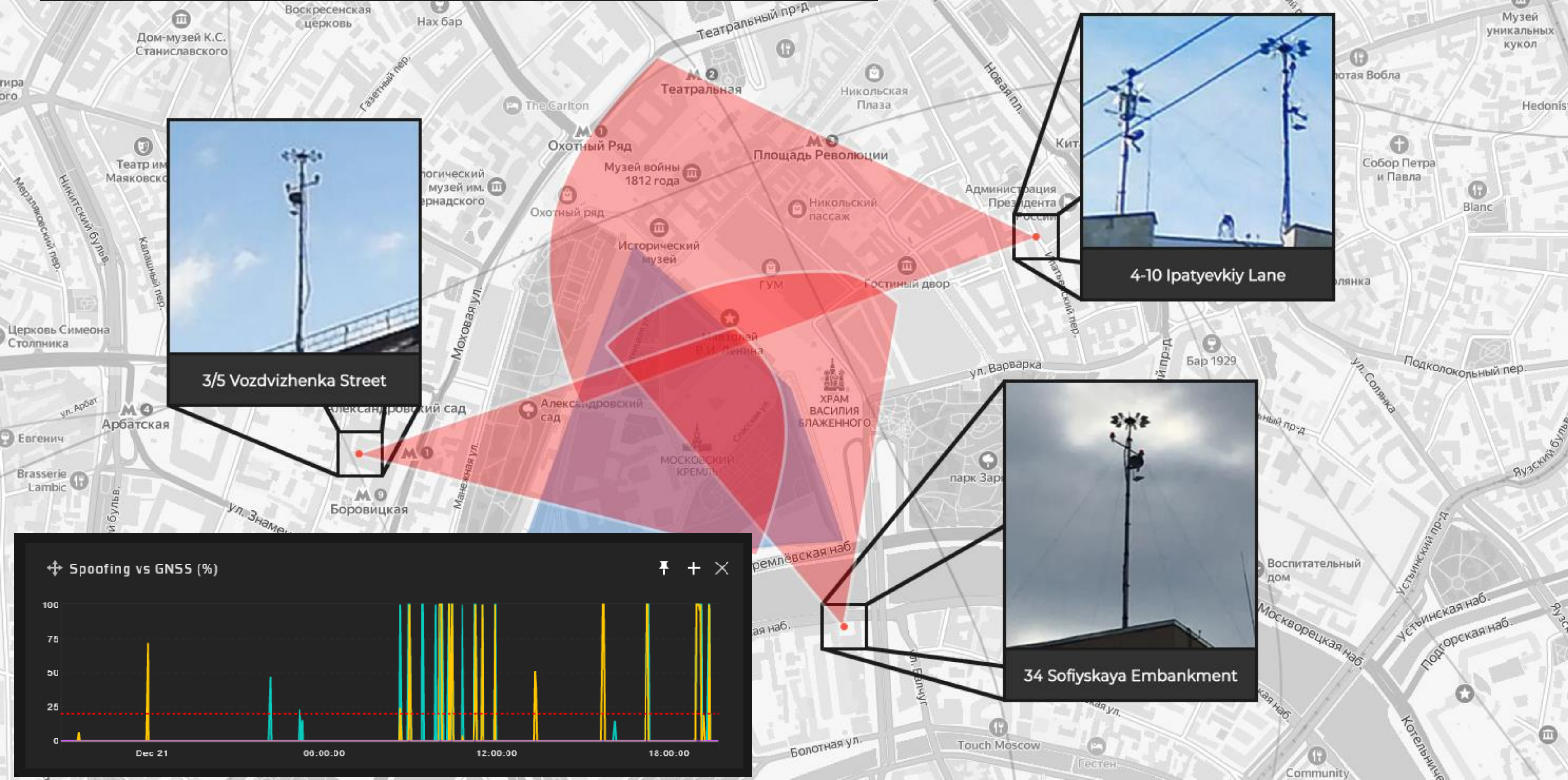
Synchronization systems with Grandmaster cross monitoring



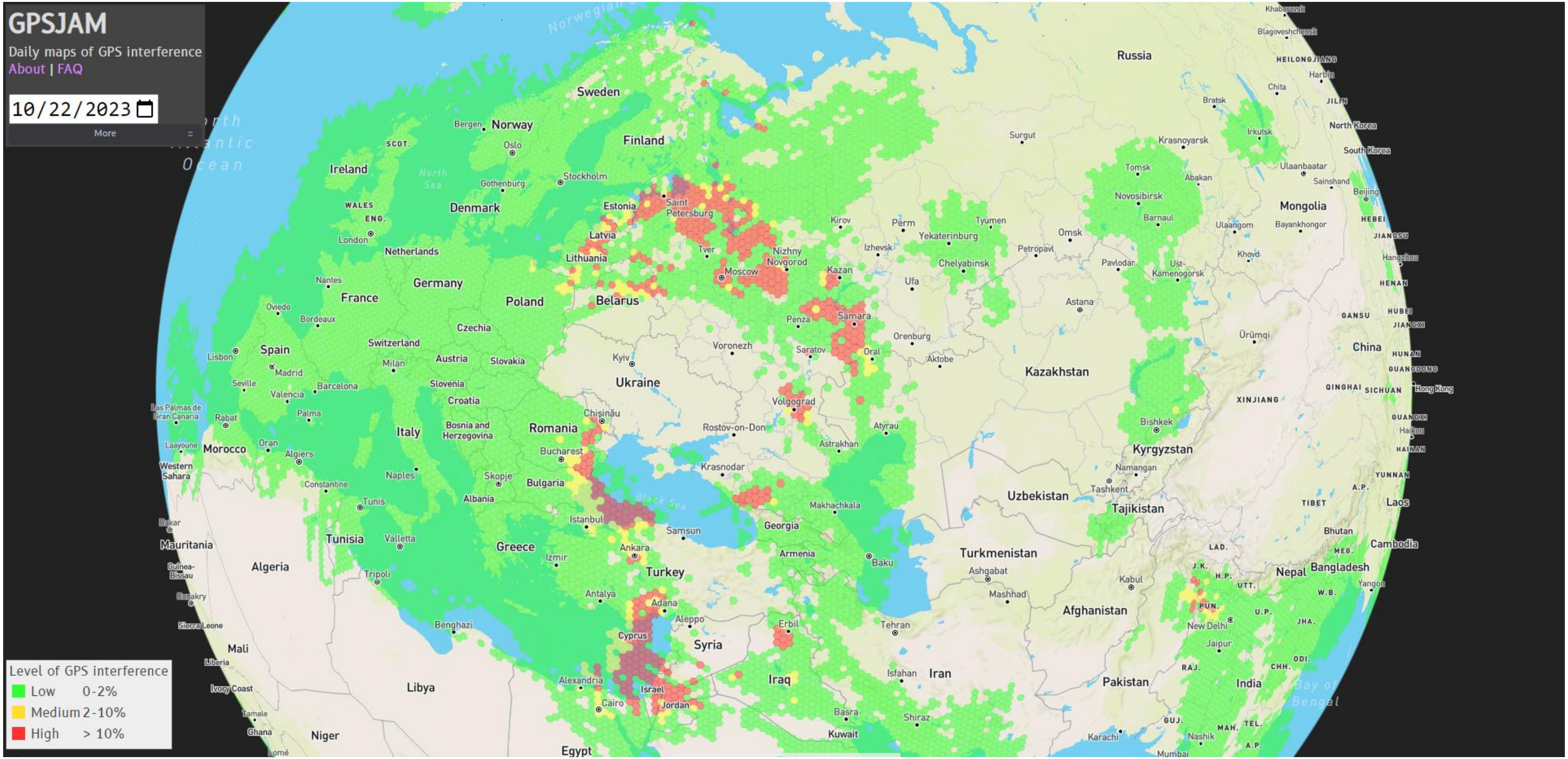
RAW GNSS data monitoring



GNSS spoofing in anti-drone systems

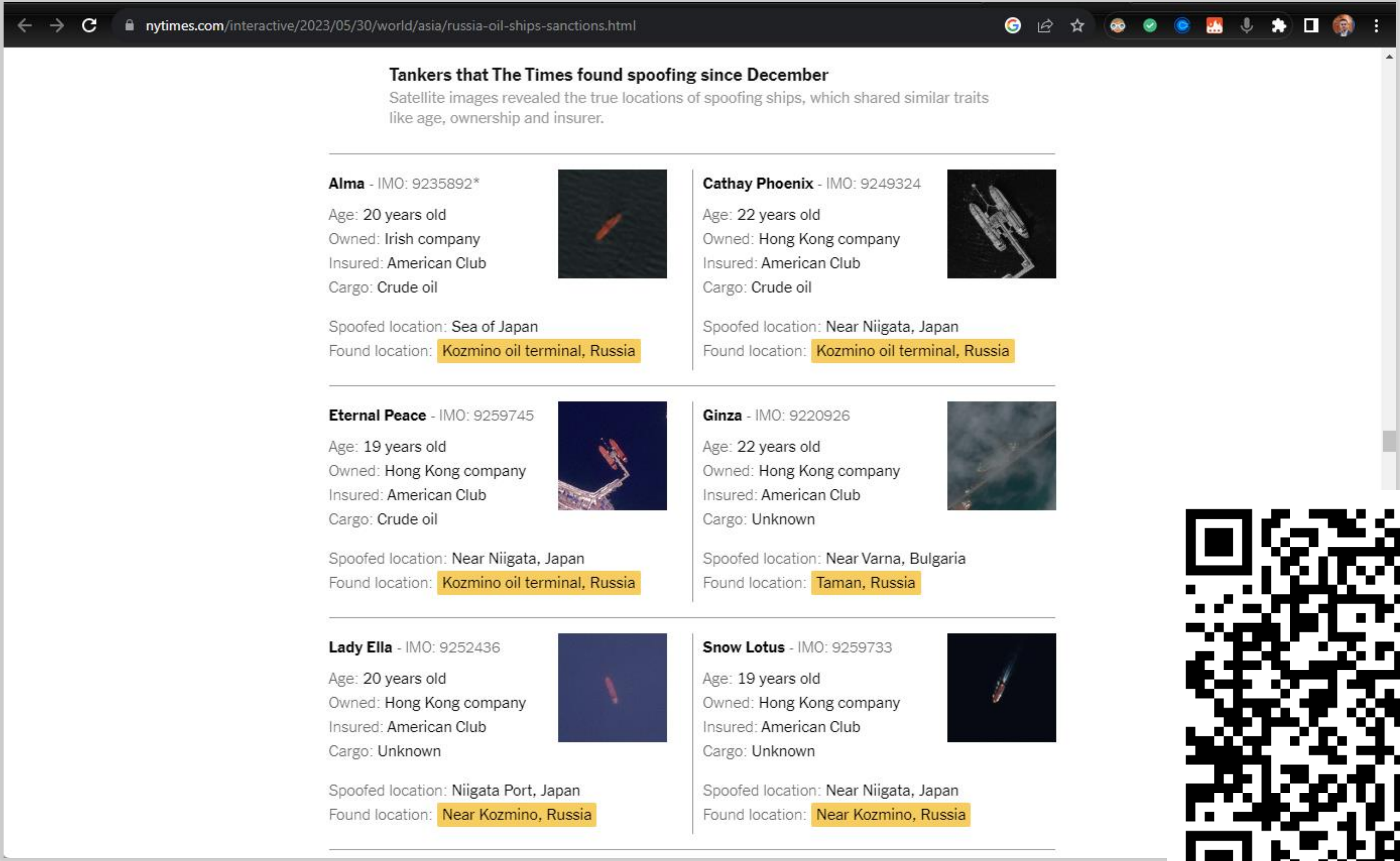


GNSS interference in 2023



Source: gpsjam.org

GNSS spoofing on vessels to avoid sanctions



nytimes.com/interactive/2023/05/30/world/asia/russia-oil-ships-sanctions.html

Tankers that The Times found spoofing since December

Satellite images revealed the true locations of spoofing ships, which shared similar traits like age, ownership and insurer.

Alma - IMO: 9235892*

Age: 20 years old
Owned: Irish company
Insured: American Club
Cargo: Crude oil

Spoofed location: Sea of Japan
Found location: Kozmino oil terminal, Russia

Cathay Phoenix - IMO: 9249324

Age: 22 years old
Owned: Hong Kong company
Insured: American Club
Cargo: Crude oil

Spoofed location: Near Niigata, Japan
Found location: Kozmino oil terminal, Russia

Eternal Peace - IMO: 9259745

Age: 19 years old
Owned: Hong Kong company
Insured: American Club
Cargo: Crude oil

Spoofed location: Near Niigata, Japan
Found location: Kozmino oil terminal, Russia

Ginza - IMO: 9220926

Age: 22 years old
Owned: Hong Kong company
Insured: American Club
Cargo: Unknown

Spoofed location: Near Varna, Bulgaria
Found location: Taman, Russia

Lady Ella - IMO: 9252436

Age: 20 years old
Owned: Hong Kong company
Insured: American Club
Cargo: Unknown

Spoofed location: Niigata Port, Japan
Found location: Near Kozmino, Russia

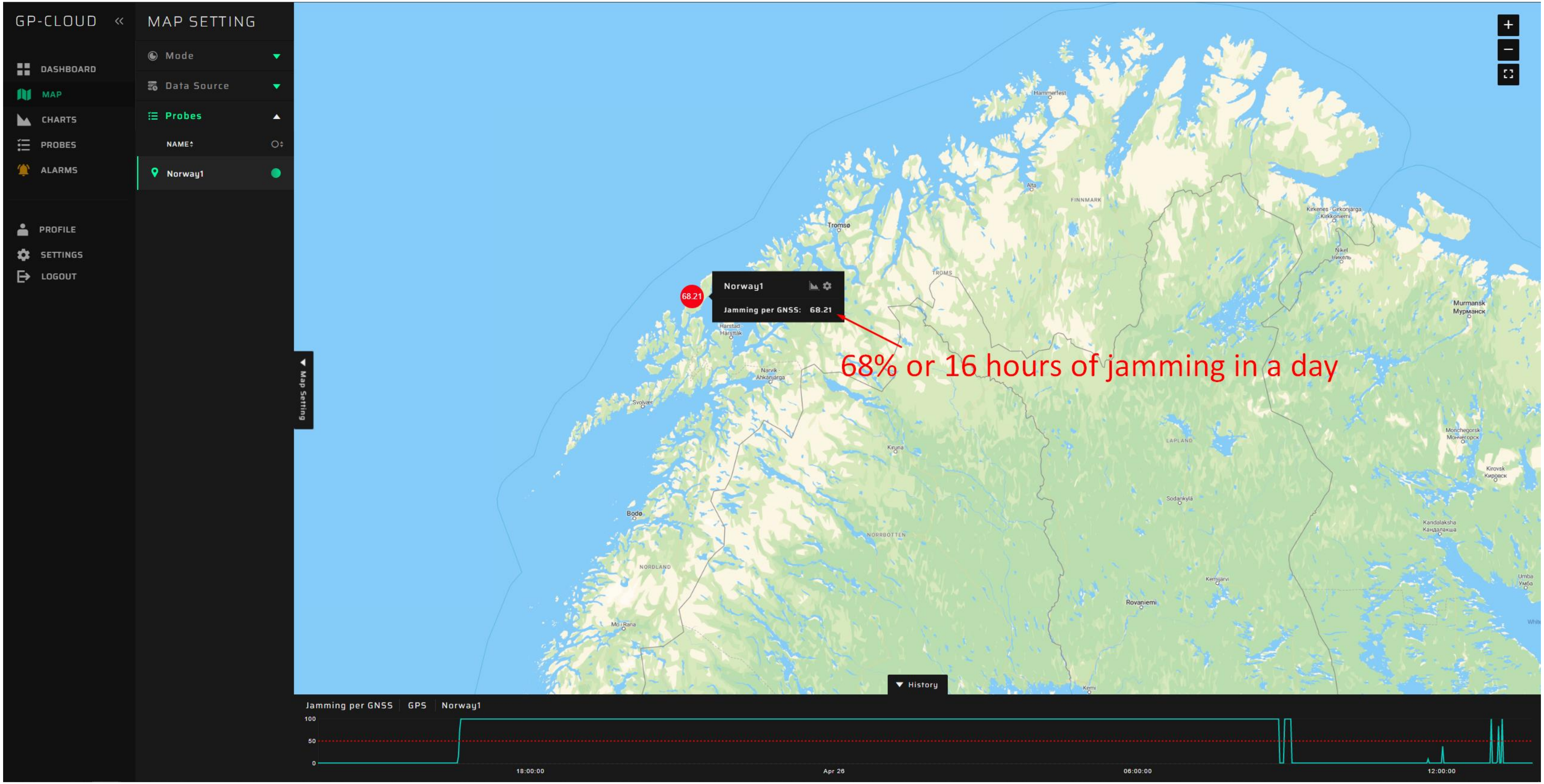
Snow Lotus - IMO: 9259733

Age: 19 years old
Owned: Hong Kong company
Insured: American Club
Cargo: Unknown

Spoofed location: Near Niigata, Japan
Found location: Near Kozmino, Russia

https://www.nytimes.com/interactive/2023/05/30/world/asia/russia-oil-ships-sanctions.html

GNSS jamming/spoofing on vessels



GNSS jamming/spoofing on vessels

Why is spoofing trending right now?

$319.95	$198.50	$346.29	$480

HackRF One Software Defined Radio (SDR) & ANT500 Antenna Bundle

★★★★☆ 29

$319.95

ANALOG DEVICES ADALM-Pluto SDR Software Defined Radio Active Learning Module PlutoSDR

★★★☆☆ 9

$198.50

LimeSDR Flexible, Next-generation, Open Source Software Defined Radio USB 3.0 100 kHz - 3.8 GHz

★★★★☆ 523

$346.29

bladeRF 2.0 micro xA4, 47MHz to 6GHz frequency range, 61.44MHz sampling rate, 2×2 MIMO channels USB 3.0 SuperSpeed Software Defined Radio.

★★★★☆ 17

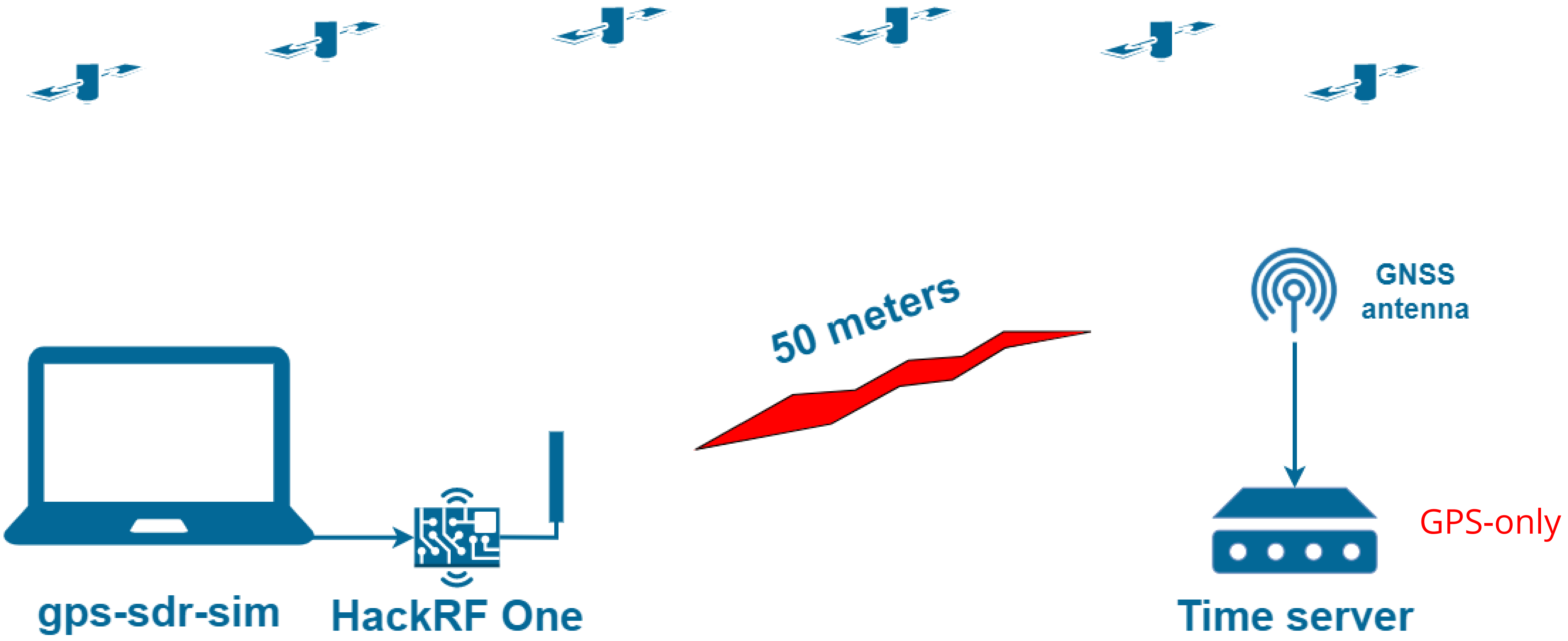
$480

680 Forks on GitHub for GPS Signal Simulation

gym487/GPS-SDR-SIM-realtime	Supports IQ data generation to the port for real-time playback via GNU Radio
osqzss/bladeGPS	Real-time signal generation with bladeRF
osqzss/LimeGPS	Real-time signal generation with LimeSDR
Microtronics/PLUTO-GPS-SIM	Real-time signal generation with ADALM-Pluto
Microtronics/multi-SDR-GPS-SIM	Real-time signal generation with HackRF One or ADALM-PLUTO. Has settings for over-the-air operation: Target distance [m], bearing [°], and height [m]. Parameters can be changed on the fly. We can assume that the application is designed to perform real attacks.

https://gpspatron.com/680-forks-on-github-for-gps-signal-simulation/

Attack scenarios. GPS spoofing with HackRF One



Attack cost - 320 USD
Attack time - from 15 seconds to 5 minutes

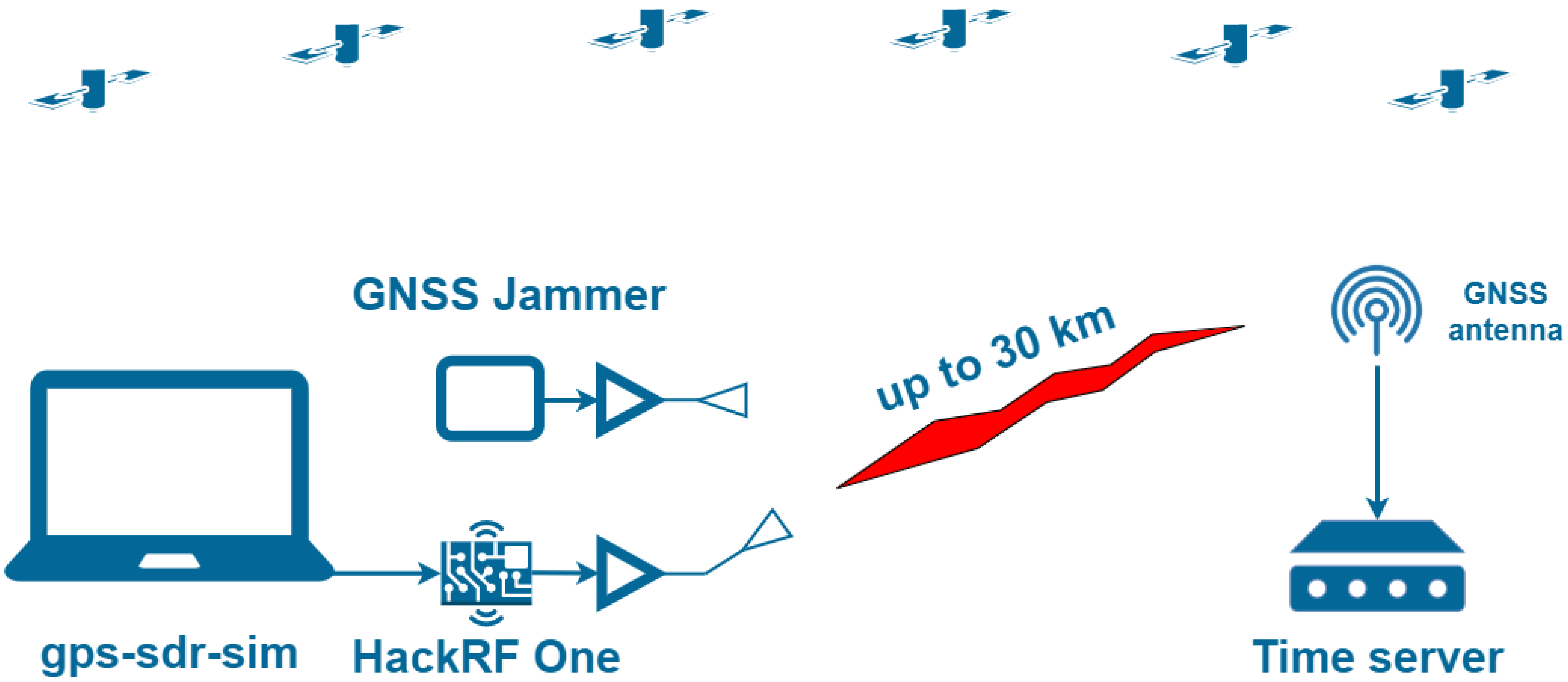
Protection - use multi-GNSS receivers
Detection at the system level is easy

RF Amplifier + directional antenna

Output power 10W

4 dB antenna gain

Attack Scenarios. GNSS spoofing with HackRF One, jammer and amplifier



Attack cost – 1.5k USD
Attack time - from 15 seconds to 5 minutes

System-level detection is not possible if all time servers are being covered

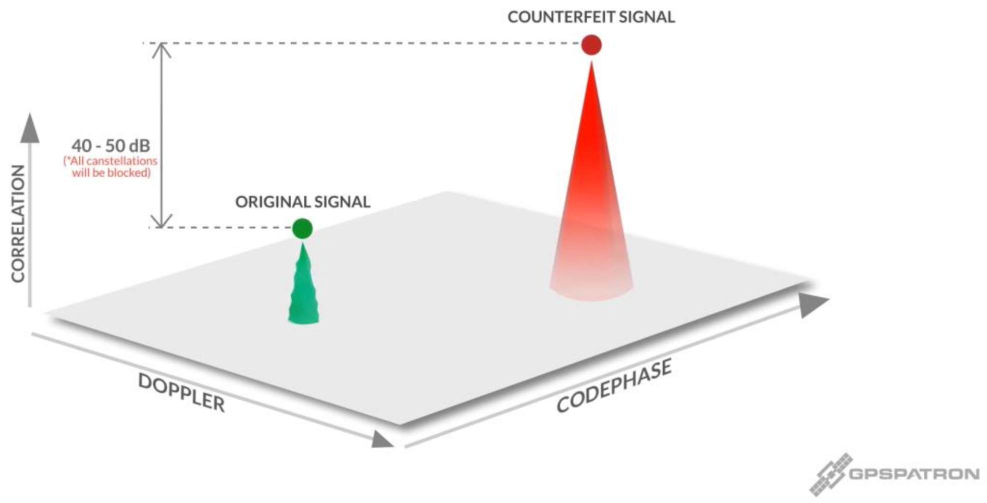
Types of GNSS Spoofing

Non-coherent

Generation of a fake GNSS signal not synchronized with the real one.

Incorrect coordinates, time, pseudo-distance, Doppler, etc.

The first step of the attack requires suppressing the real signals so that the receiver under attack goes into tracking mode and switches to the fake signals.



Coherent

Generation of a fake GNS signal that is **completely identical** to the real one.

Instant switching to a fake signal –> imperceptible, smooth drift of LLA or PPS phase

Non-Coherent Attack Example

Coherent attack example with gradual coordinate shift

Data Formats for Analysis

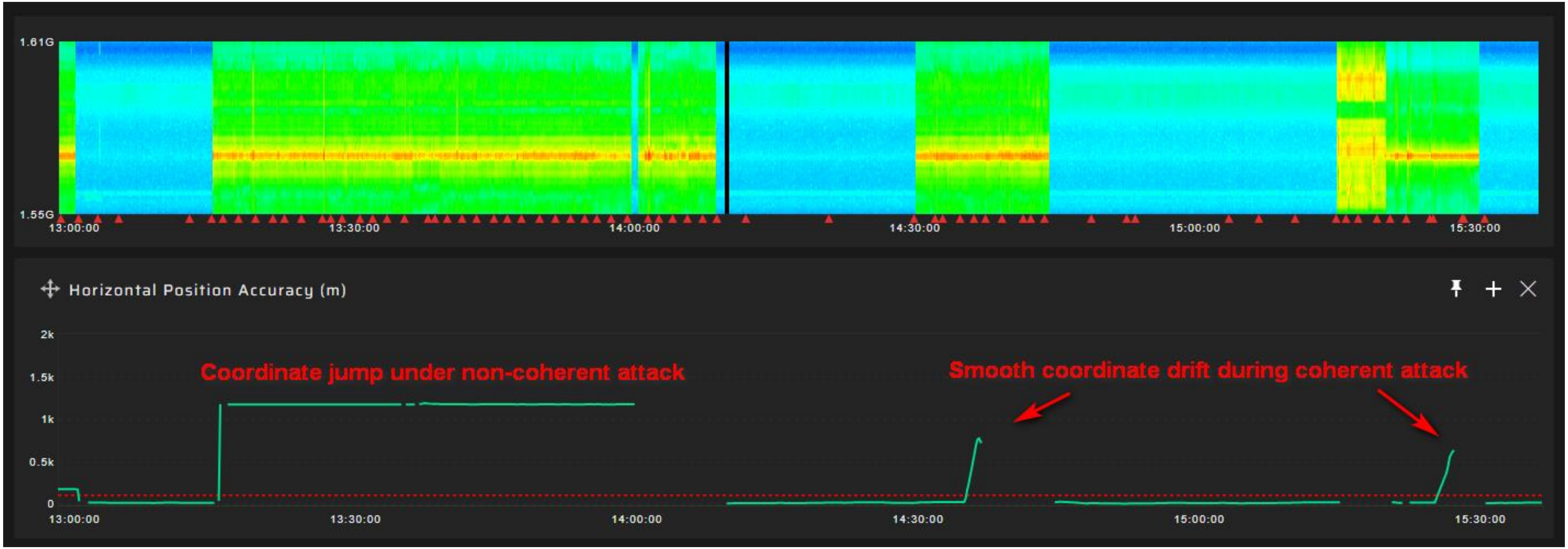
NMEA

- Timestamp
- Coordinates
- Velocity
- Signal to noise ratio
- Number of visible sats

Proprietary binary data format (UBX)

- Gain
- RF Spectrum
- Residuals
- Pseudorange
- Doppler
- Carrier Phase & Lock Time

Coordinate Monitoring

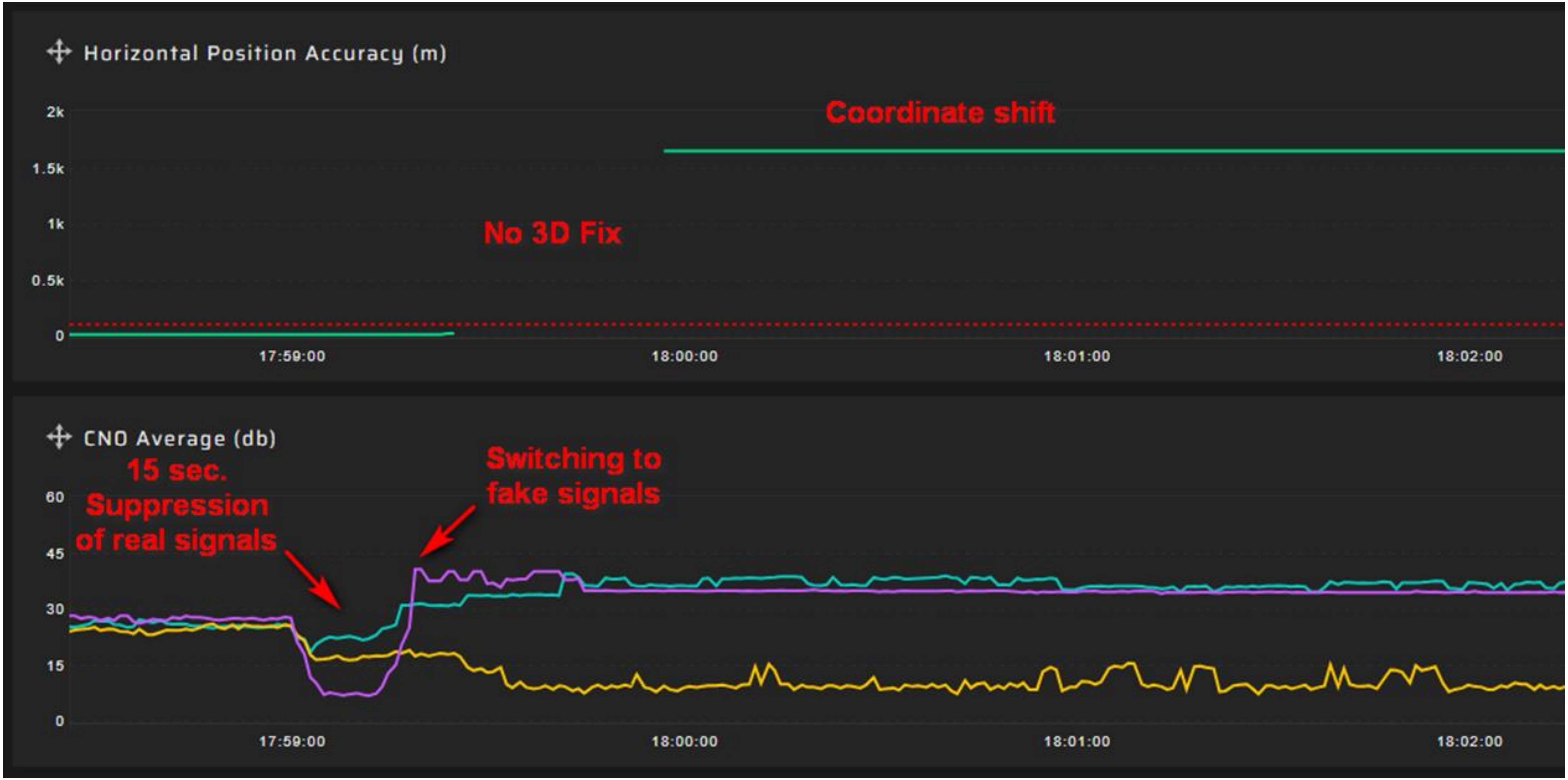


Advantages: the most simple algorithm

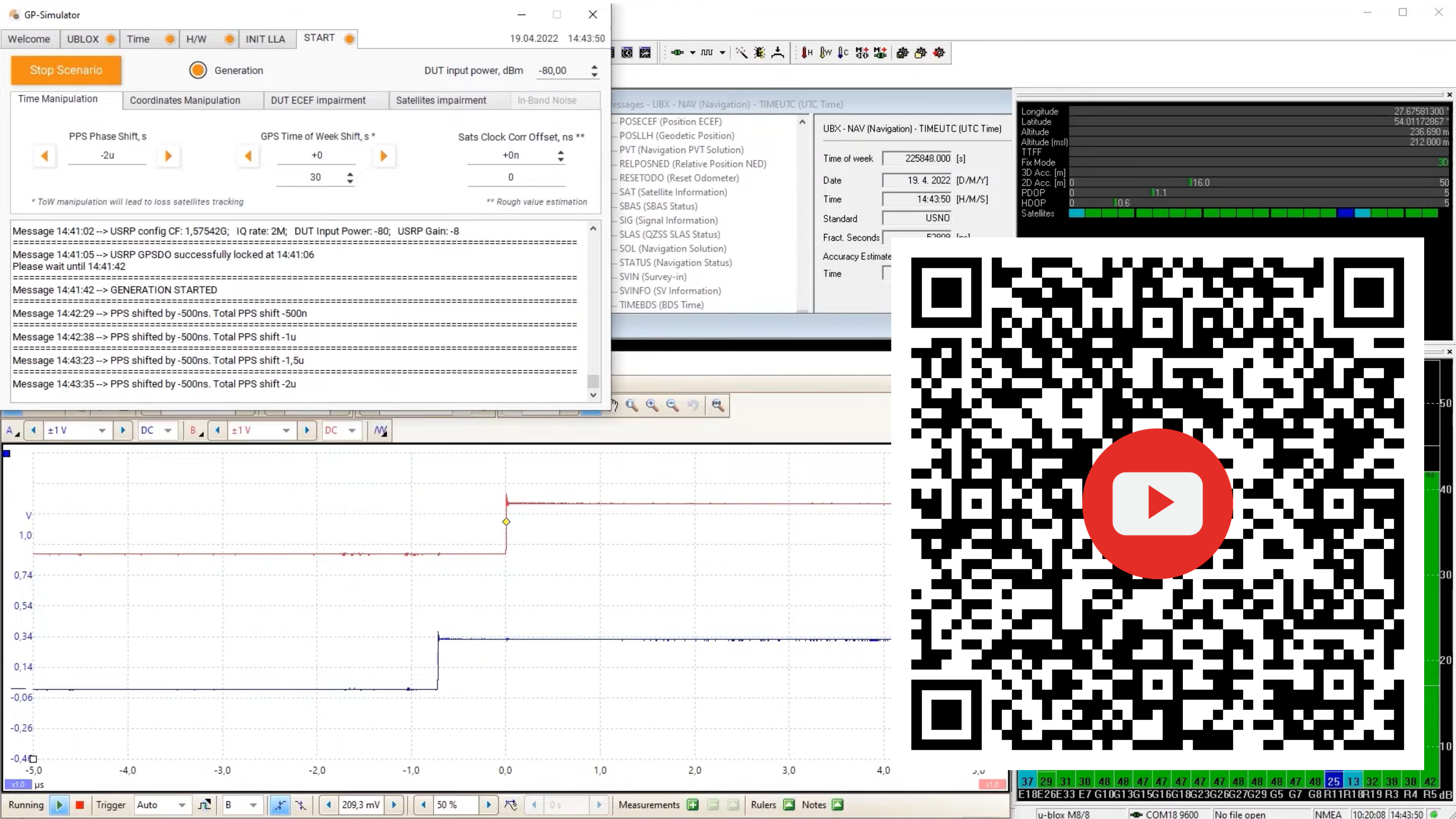
Disadvantages:

- late detection - you will only detect spoofing after your receiver has successfully spoofed.
- GNSS generator can simulate your coordinates

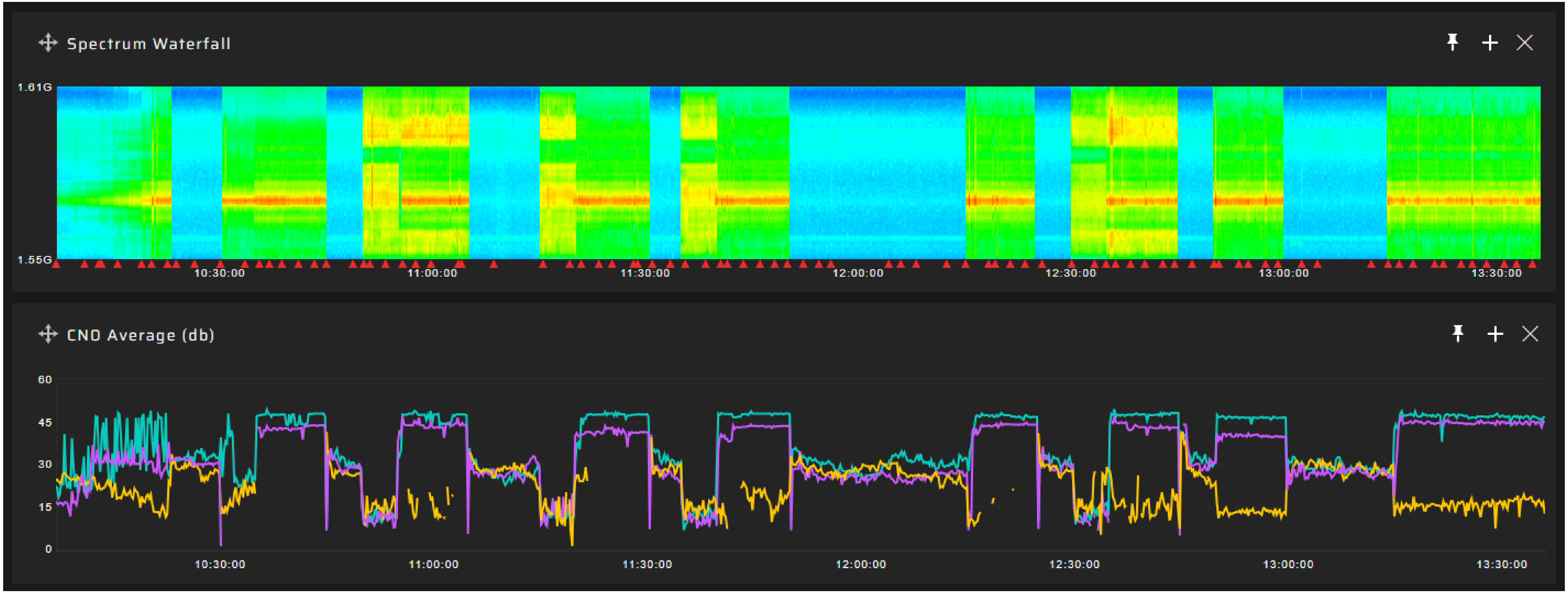
Coordinate Monitoring Weakness - Late Detection



Coordinate Monitoring Weakness - A time-only attack


GP-Simulator
Welcome
UBLOX
Time
H/W
INIT LLA
START
19.04.2022 14:43:50
Stop Scenario
Generation
DUT input power, dBm -80,00
Time Manipulation
Coordinates Manipulation
DUT ECEF impairment
Satellites impairment
In-Band Noise
PPS Phase Shift, s
-2u
GPS Time of Week Shift, s *
+0
30
Sats Clock Corr Offset, ns **
+0n
0
* ToW manipulation will lead to loss satellites tracking
** Rough value estimation
Message 14:41:02 --> USRP config CF: 1,57542G; IQ rate: 2M; DUT Input Power: -80; USRP Gain: -8
Message 14:41:05 --> USRP GPSDO successfully locked at 14:41:06
Please wait until 14:41:42
Message 14:41:42 --> GENERATION STARTED
Message 14:42:29 --> PPS shifted by -500ns. Total PPS shift -500n
Message 14:42:38 --> PPS shifted by -500ns. Total PPS shift -1u
Message 14:43:23 --> PPS shifted by -500ns. Total PPS shift -1,5u
Message 14:43:35 --> PPS shifted by -500ns. Total PPS shift -2u
essages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)
POSECEF (Position ECEF)
POSLLH (Geodetic Position)
PVT (Navigation PVT Solution)
RELPOSNED (Relative Position NED)
RESETODO (Reset Odometer)
SAT (Satellite Information)
SBAS (SBAS Status)
SIG (Signal Information)
SLAS (QZSS SLAS Status)
SOL (Navigation Solution)
STATUS (Navigation Status)
SVIN (Survey-in)
SVINFO (SV Information)
TIMEBDS (BDS Time)
UBX - NAV (Navigation) - TIMEUTC (UTC Time)
Time of week 225848.000 [s]
Date 19. 4. 2022 [D/M/Y]
Time 14:43:50 [H/M/S]
Standard USNO
Fract. Seconds
Accuracy Estimate
Time
Longitude 27.67581300 °
Latitude 54.01172867 °
Altitude 236.690 m
Altitude (msl) 212.000 m
TTFF
Fix Mode 3D
3D Acc. [m]
2D Acc. [m] 0 16.0 50
PDOP 0 1.1 5
HDOP 0 0.6 5
Satellites
±1 V
DC
±1 V
DC
V
1,0
0,74
0,54
0,34
0,14
-0,06
-0,26
-0,40
-5,0
-4,0
-3,0
-2,0
-1,0
0,0
1,0
2,0
3,0
4,0
µs
Running
Trigger
Auto
B
209,3 mV
50 %
Measurements
Rulers
Notes
37 29 31 30 48 48 47 47 47 47 47 48 48 48 47 48 25 13 32 38 38 42
E18 E26 E33 E7 G10 G13 G15 G16 G18 G23 G26 G27 G29 G5 G7 G8 R11 R18 R19 R3 R4 R5 dB
u-blox M8/8
COM18 9600
No file open
NMEA
10:20:08
14:43:50

CN0 Average Monitoring

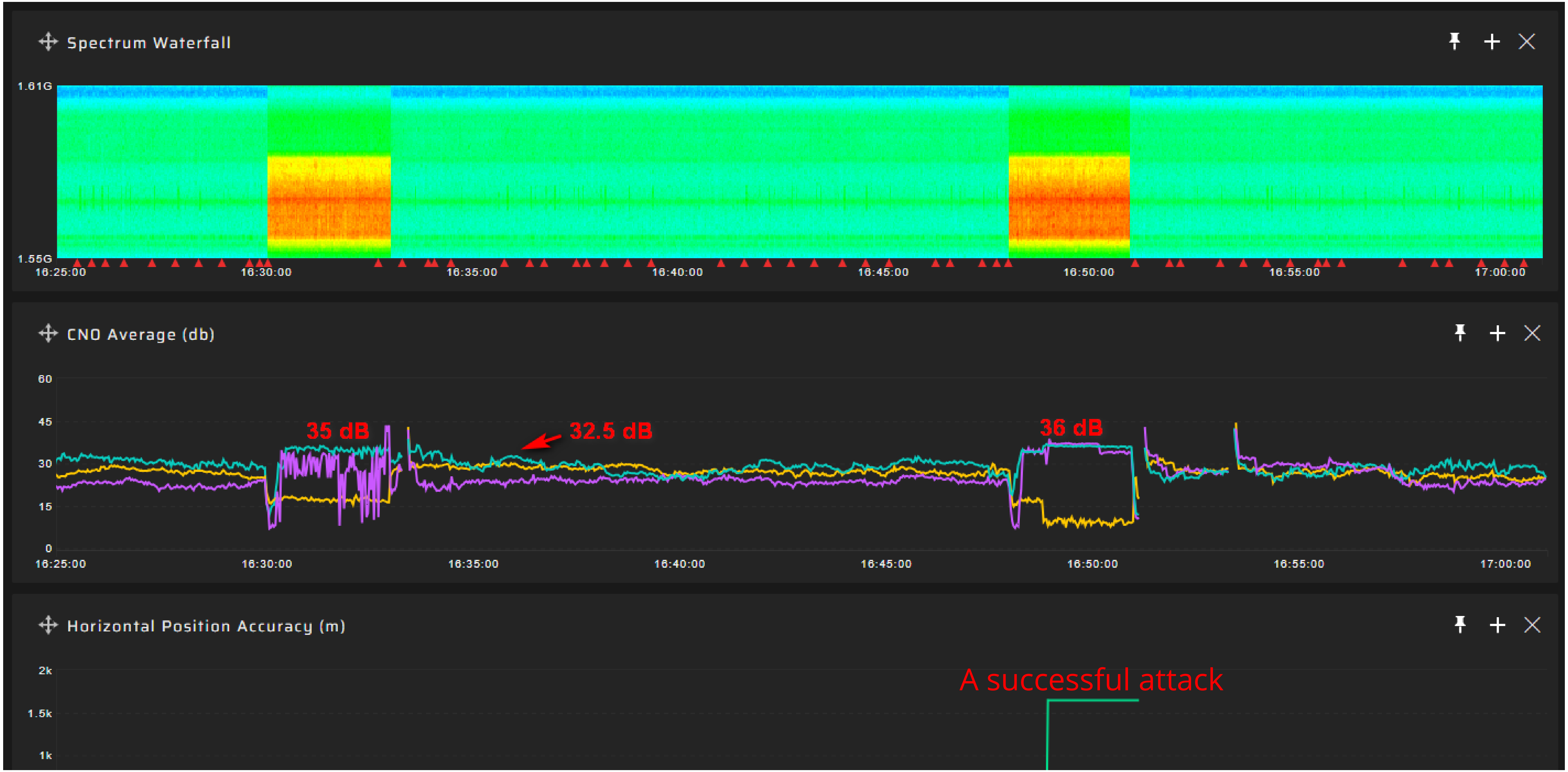


Advantages: Spoofing early detection. It is easy to set limits for powerful spoofing detection

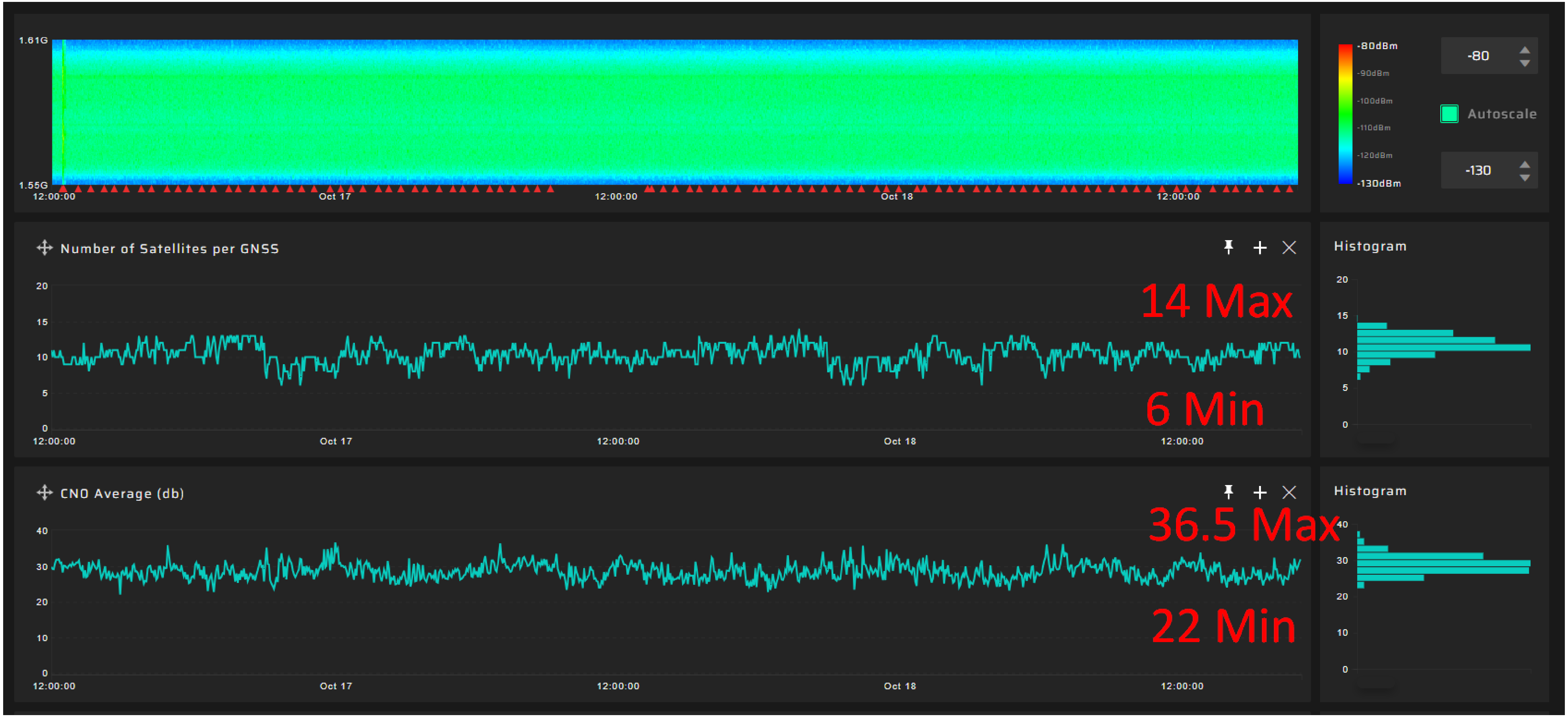
Disadvantages:

- GNSS generator can simulate any value of signal-to-noise ratio.
- It is difficult to set thresholds to detect low-power spoofing combined in combination with an acceptable false alarm rate.

CN0 Average Monitoring Weakness - Minor CN0 shift

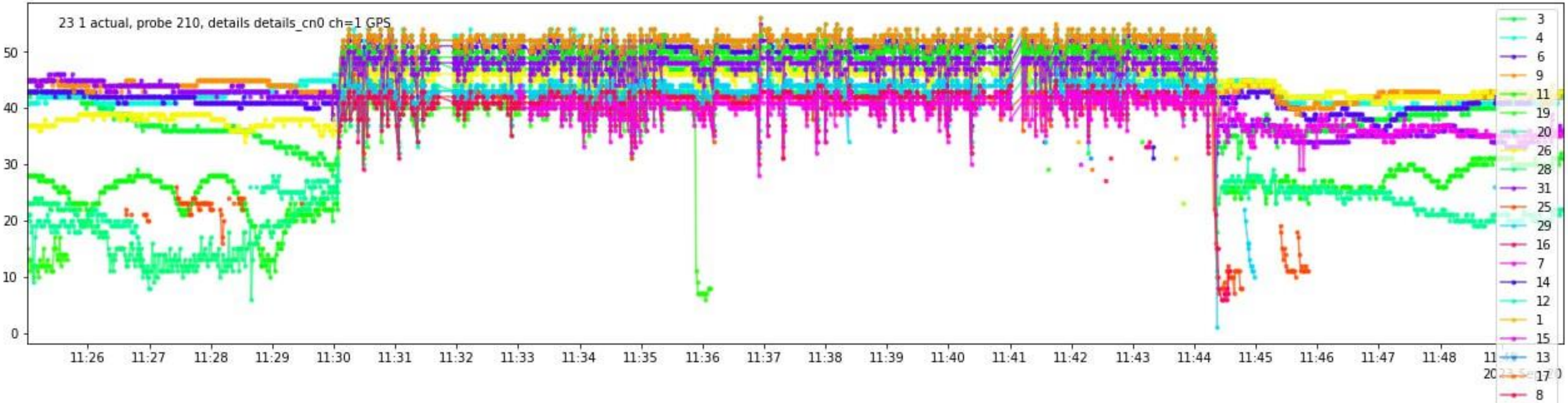


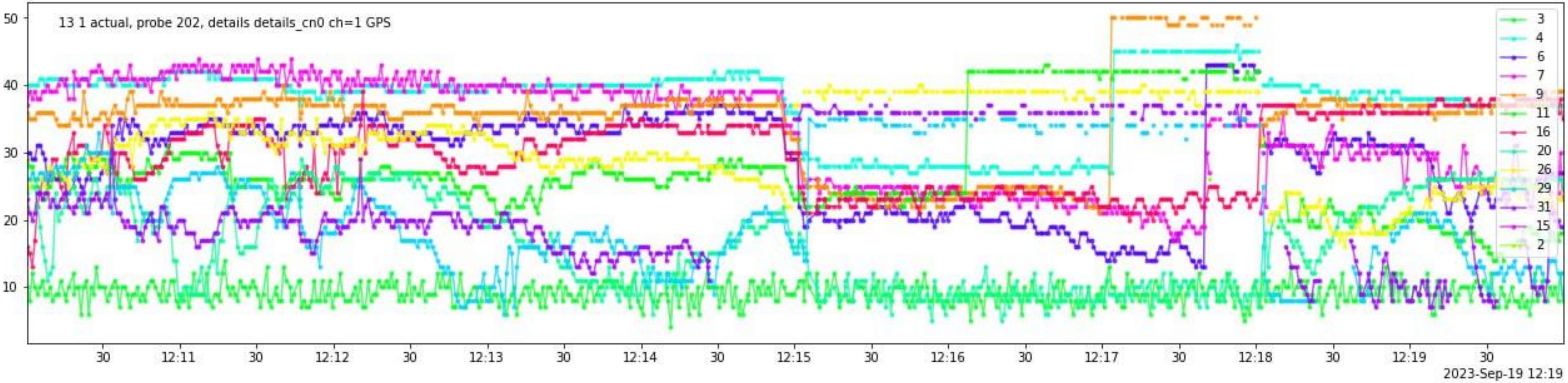
CN0 Average Monitoring Weakness - Large CN0 deviation under normal conditions



Monitoring of CN0 distribution between satellites

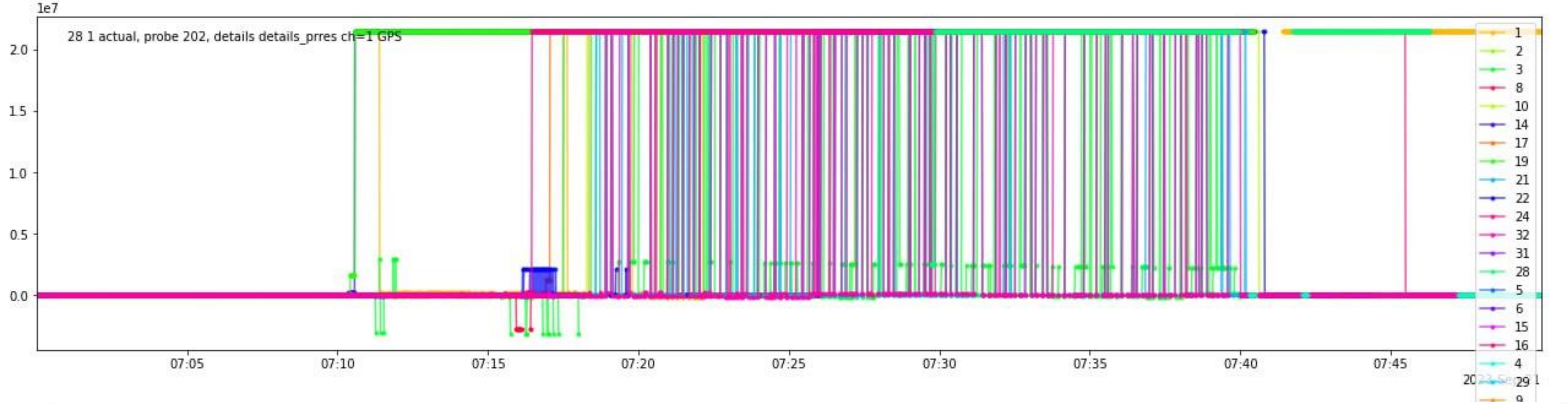
CN0 monitoring for each satellite

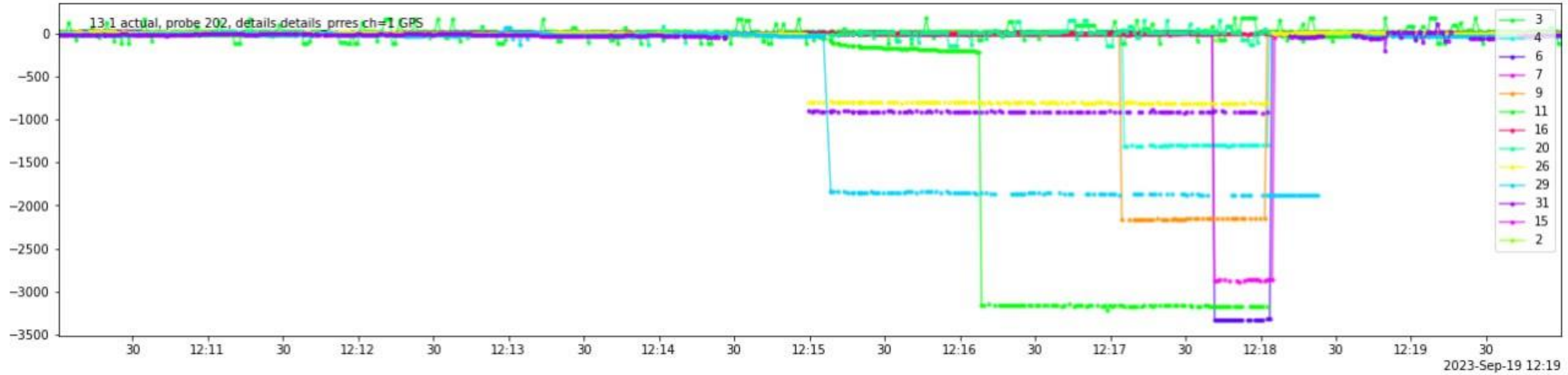




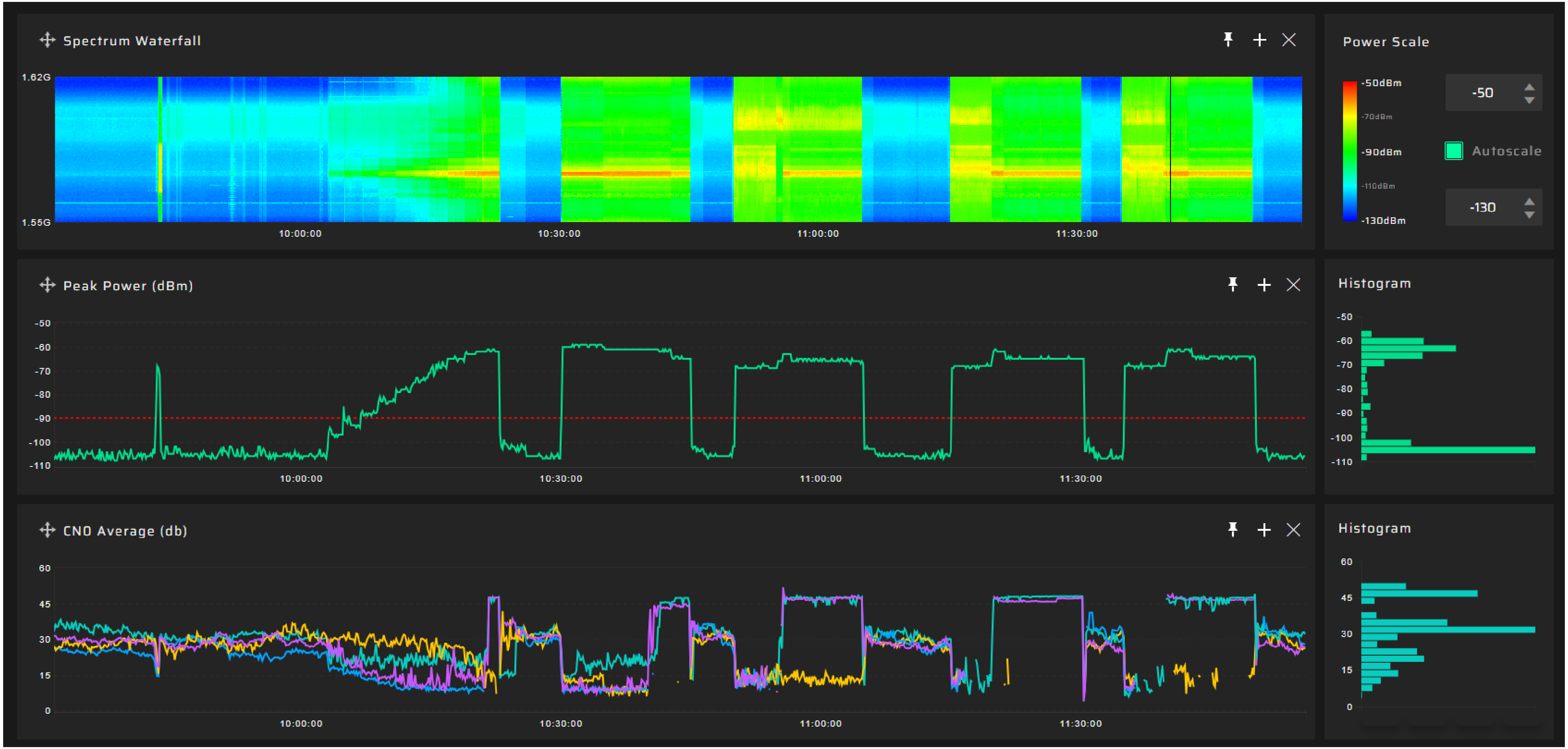
Pseudorange residuals monitoring for non-coherent spoofing detection

Pseudorange residuals monitoring for non-coherent spoofing detection



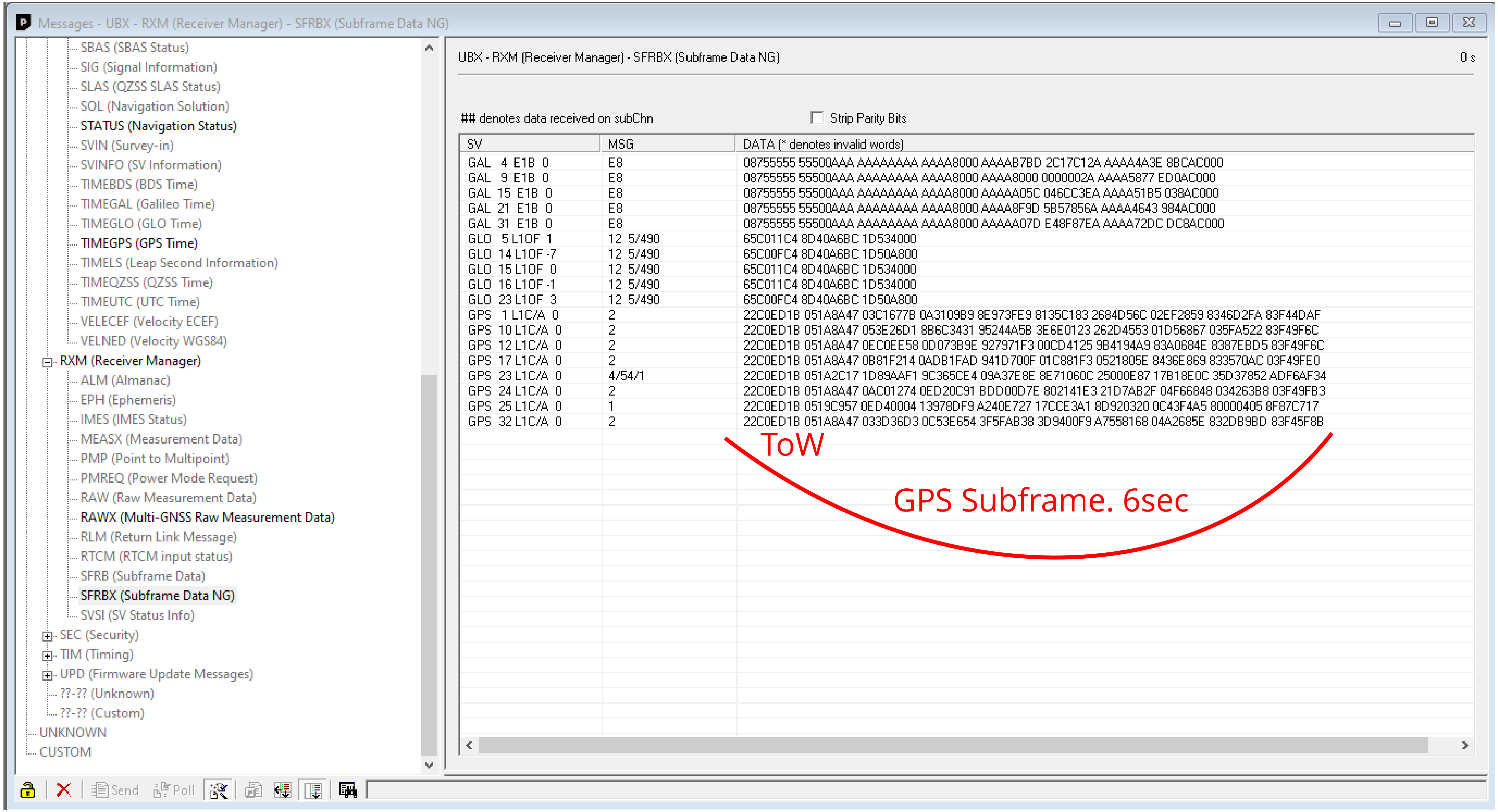


Spectrum, power & gain monitoring



Spectrum, power & gain monitoring

DataStream Authentication



GNSS receiver glitches due to spoofing

Dataset from Ublox

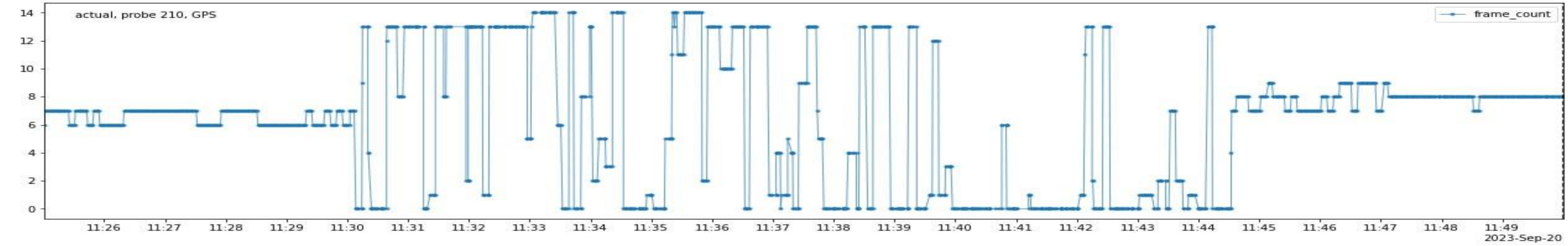

```
[
  {
    "AGC": 3354,
    "UTC": "2023-09-26T23:59:58Z",
    "gDOP": 1.51,
    "hAcc": 2.082,
    "hDOP": 0.81,
    "hMSL": 100.488,
    "magI": 150,
    "magQ": 156,
    "ofsI": 9,
    "ofsQ": 50,
    "pDOP": 1.31,
    "sAcc": 0.02,
    "tAcc": 5,
    "tDOP": 0.75,
    "vAcc": 2.001,
    "vDOP": 1.03,
    "velD": -0.029,
    "velE": -0.016,
    "velN": -0.027,
    "Noise": 100,
    "NumSV": 19,
    "Glo_N4": 7,
    "Glo_Nt": 1366,
    "Height": 134.793,
    "BDS_SOW": 259202,
    "FixType": 3,
    "Gal_Tow": 259216,
    "Gal_Wno": 1257,
    "Glo_TOD": 10798,
    "Jamming": 13,
    "BDS_Week": 925,
    "BDS_fSOW": -201329,
    "BDS_tAcc": 3341,
    "GPS_Week": 2281,
    "GPS_fTOW": -201329,
    "GPS_iTOW": 259216000,
    "GPS_tAcc": 5,
    "Gal_fTow": -201343,
    "Gal_tAcc": 6,
    "Glo_fTOD": -201381,
    "Glo_tAcc": 6,
    "Latitude": 52.1567885,
    "BDS_LeapS": 4,
    "BDS_Valid": true,
    "GPS_Valid": true,
    "GPS_leapS": 18,
    "Gal_Valid": true,
    "Gal_leapS": 18,
    "Glo_Valid": false,
    "Longitude": 21.075326099999998,
    "ChannelError": false,
    "ChannelNumber": 1,
```

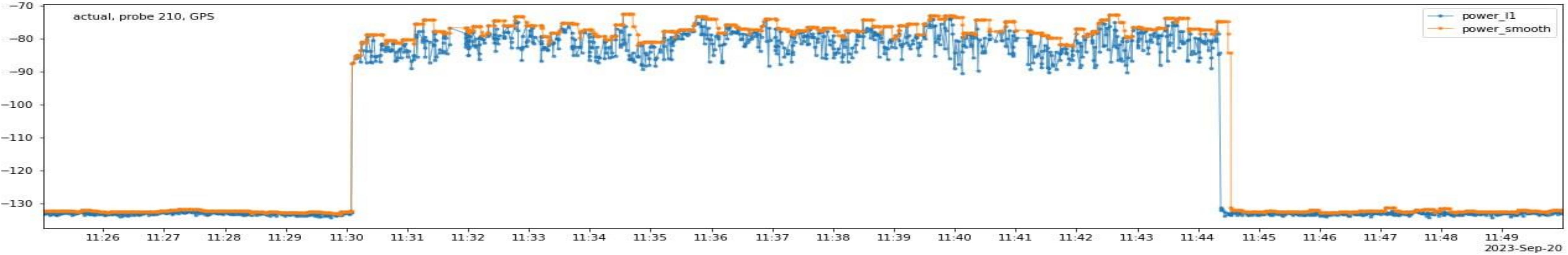

Common module data

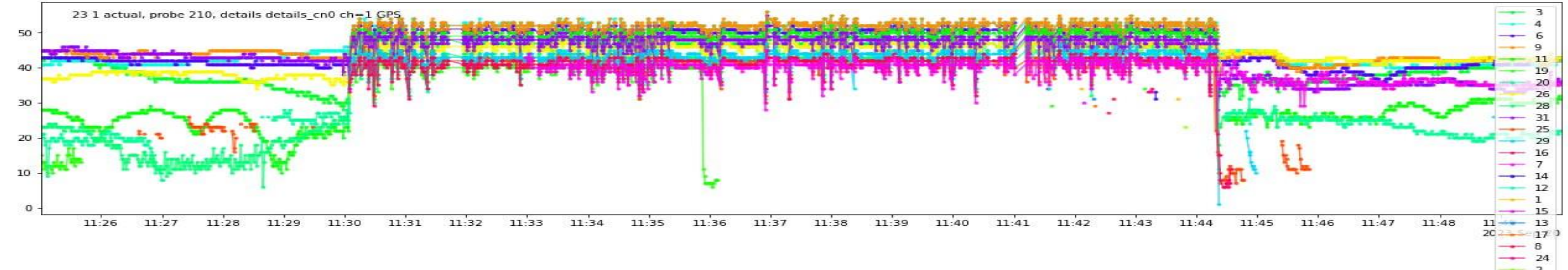

```
    "ChannelNumber": 1,
    "SpoofDetState": 1,
    "UBLOX_Reseted": false,
    "AntennaCurrent": 9.84,
    "ChannelEnabled": true,
    "MeasurementMode": 0,
    "ChannelPowerEnabled": true,
    "RAW": [
      {
        "CP": 114521463.55281612,
        "PR": 21792712.931179166,
        "CNO": 27,
        "SQI": 0,
        "Azim": 329,
        "Elev": 6,
        "SV_Id": 4,
        "prRes": 3.4700000000000006,
        "FreqId": 0,
        "svUsed": true,
        "Band_Id": 0,
        "Doppler": -473.7751159667969,
        "GNSS_Id": 0,
        "HalfCyc": false,
        "cpStdev": 0.02,
        "cpValid": true,
        "doStdev": 0.512,
        "prStdev": 2.56,
        "prValid": true,
        "AlmAvail": false,
        "EphAvail": true,
        "LockTime": 1460,
        "Smoothed": false,
        "svHealth": 1,
        "TimeValid": 1,
        "SubHalfCyc": false,
        "crCorrUsed": false,
        "doCorrUsed": false,
        "prCorrUsed": false,
        "OrbitSource": 1,
        "FrameReceived": false,
      },
      {
        "CP": 0,
        "PR": 0,
        "CNO": 19,
        "SQI": 0,
        "Azim": 94,
        "Elev": 26,
        "SV_Id": 5,
        "prRes": 8.38,
        "FreqId": 0,
        "svUsed": false,
```


Data per satellite

Data correlation example



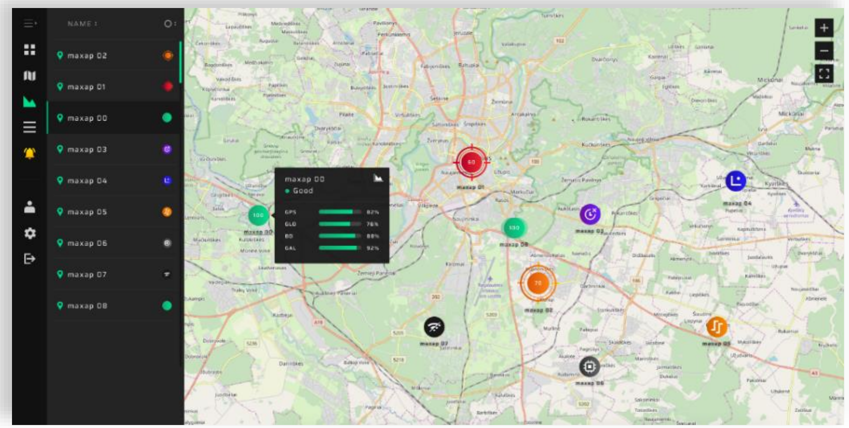




GPSPATRON Concept of Operation

GP-Probe conducts GNSS signal measurements and transmits raw data to the GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly detection and classification algorithms.

GP-Cloud



Statistics
User notification
API for integration

Data streams

High-performance 3-channel probe

One-channel probe

GP-Probe DIN L1

Designed for telecom to monitor GNSS interference and synchronization quality

Cost-effective GNSS probe with built-in RF blocker, onboard GNSS interference/anomaly detection and LUA scripting.

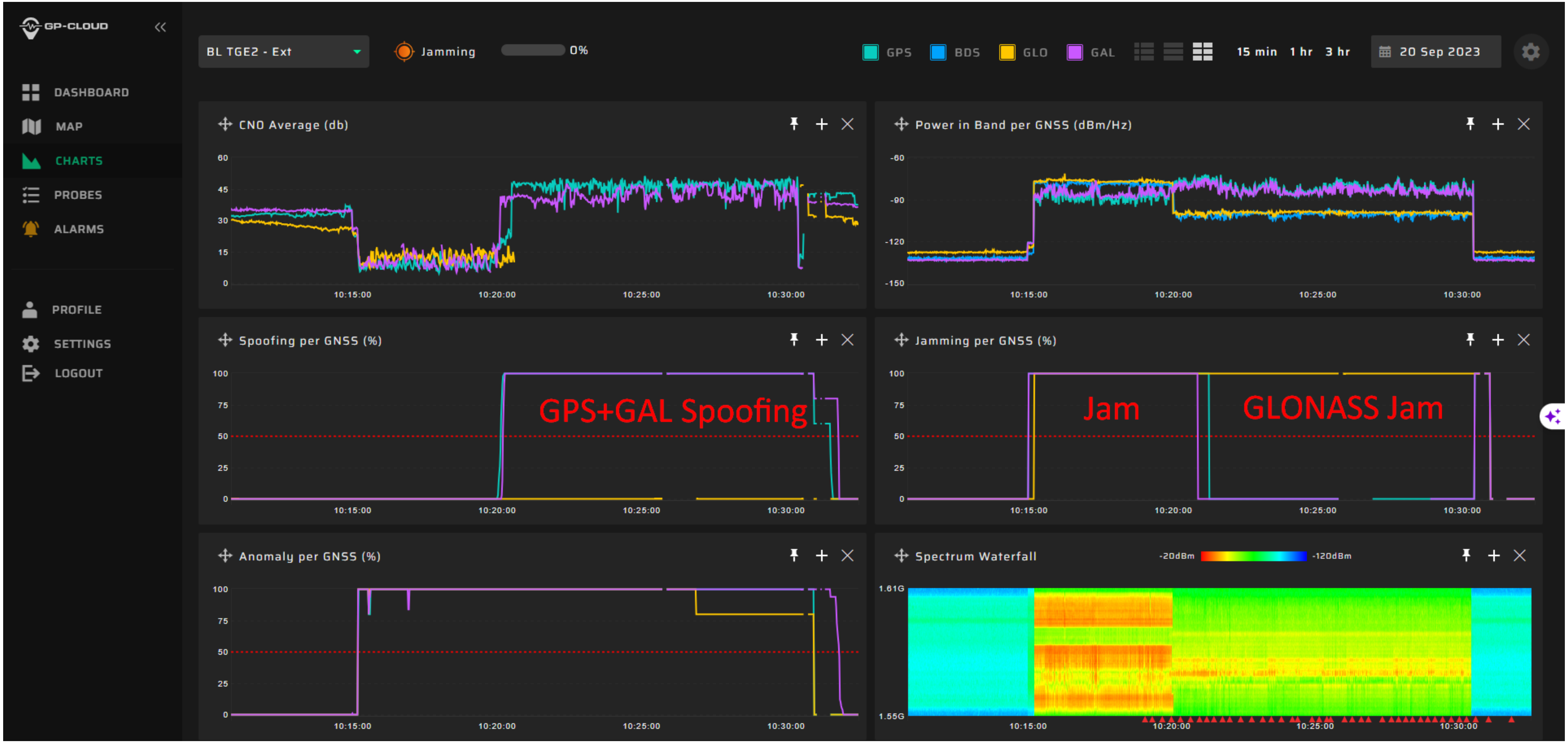
GP-Probe TGE2

Three-channel GNSS probe with an embedded RF signal analyzer

- Three RF channels enable spatial signal analysis to ensure detection of all sophisticated GNSS spoofing attack scenarios.
- 60 MHz real-time RF signal analyzer for spectrum monitoring, interference classification and localization with TDOA.

An example of proper classification

5 minutes of initial jamming. Then spoofing GPS + Galileo in combination with GLONASS jamming



Low power spoofing detection

GPSPATRON

THANK YOU
for your attention

Maksim Barodzka
CEO @ GPSPATRON

Contacts

www.gpspatron.com

mb@gpspatron.com

www.youtube.com/c/GPSPATRON

twitter.com/gpspatron