GNSS Jamming and Spoofing: how serious can it be?

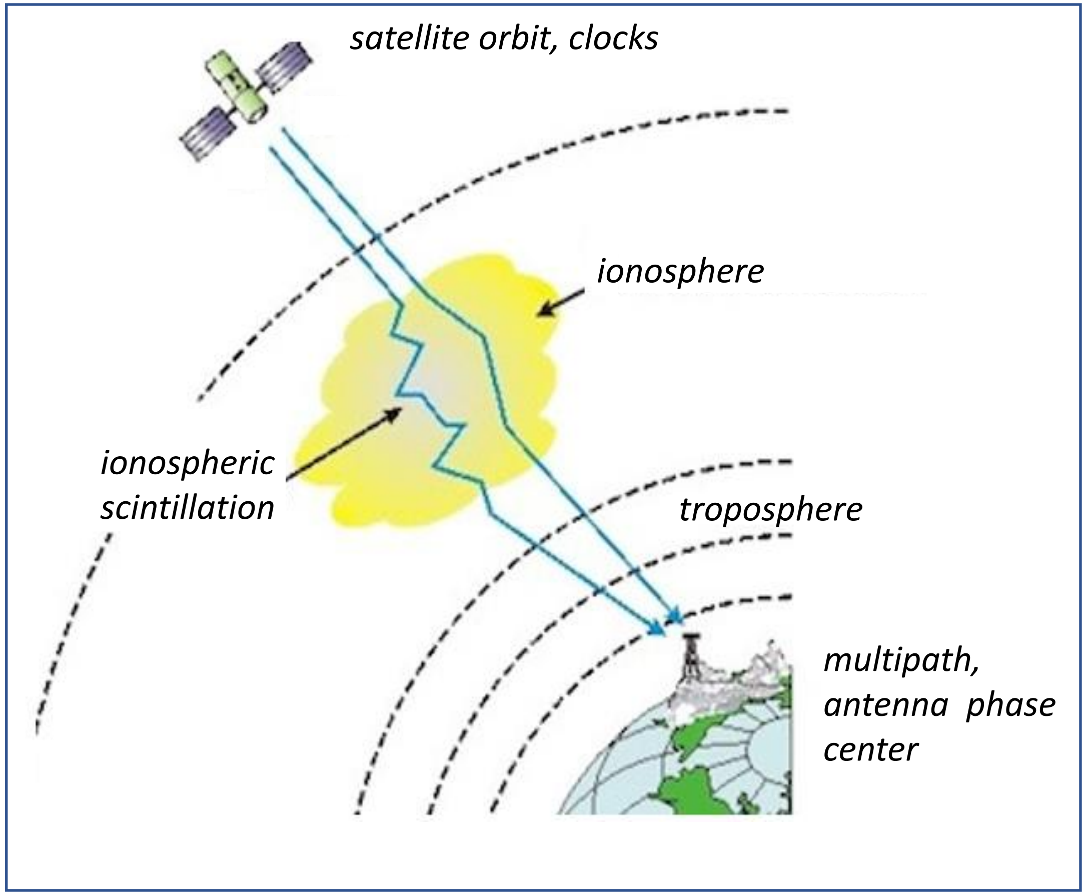
Polona Pavlovčič Prešeren

University
of Ljubljana
Faculty
of Civil and Geodetic
Engineering

Contents

- GNSS Bias Sources
- Deliberate Interference
- Jamming (field experiments & results: case from Slovenia)
- Spoofing (field experiments & results: case from Austria)
- Discussion

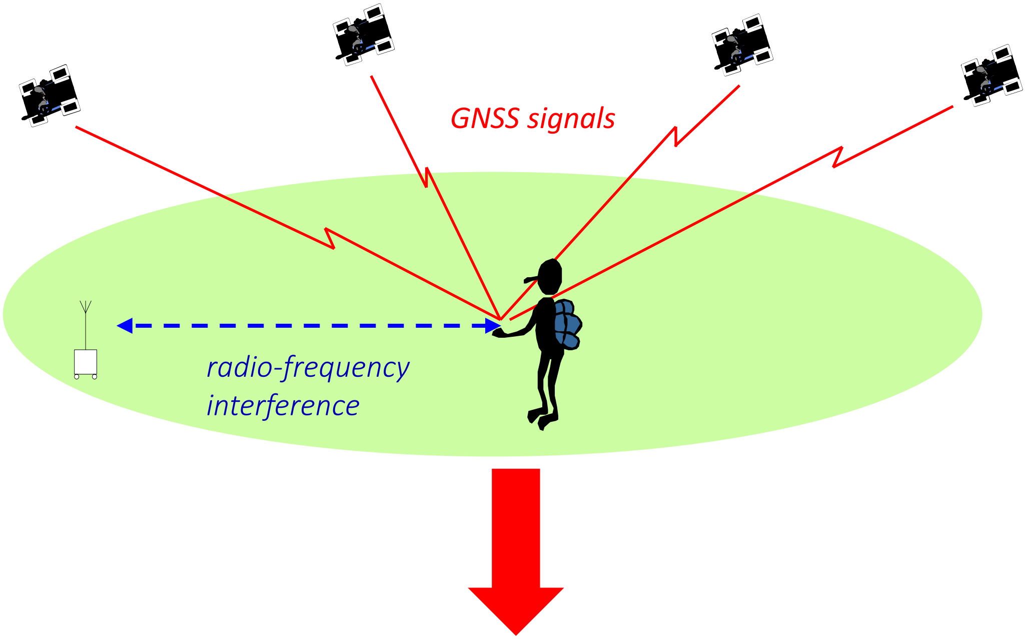
GNSS Biases Sources



Error Sources
Satellite Errors: • Satellite Clock (~ 2 m) • Satellite Orbit • Satellite Ephemerides (< 2 m)
Atmospheric Errors: • Ionospheric refraction (~ 4 – 6 m) • Troposphere (~ 0.7 m)
Receiver‘s Errors: • Multipath (~ 1.5 m) • Noise of the receiver (~ 0.5 m)
Interference = **unpredictable/unknown/variable**

Motivation

The received GNSS signals at ground level are very weak (**approx. –130 dBm**):

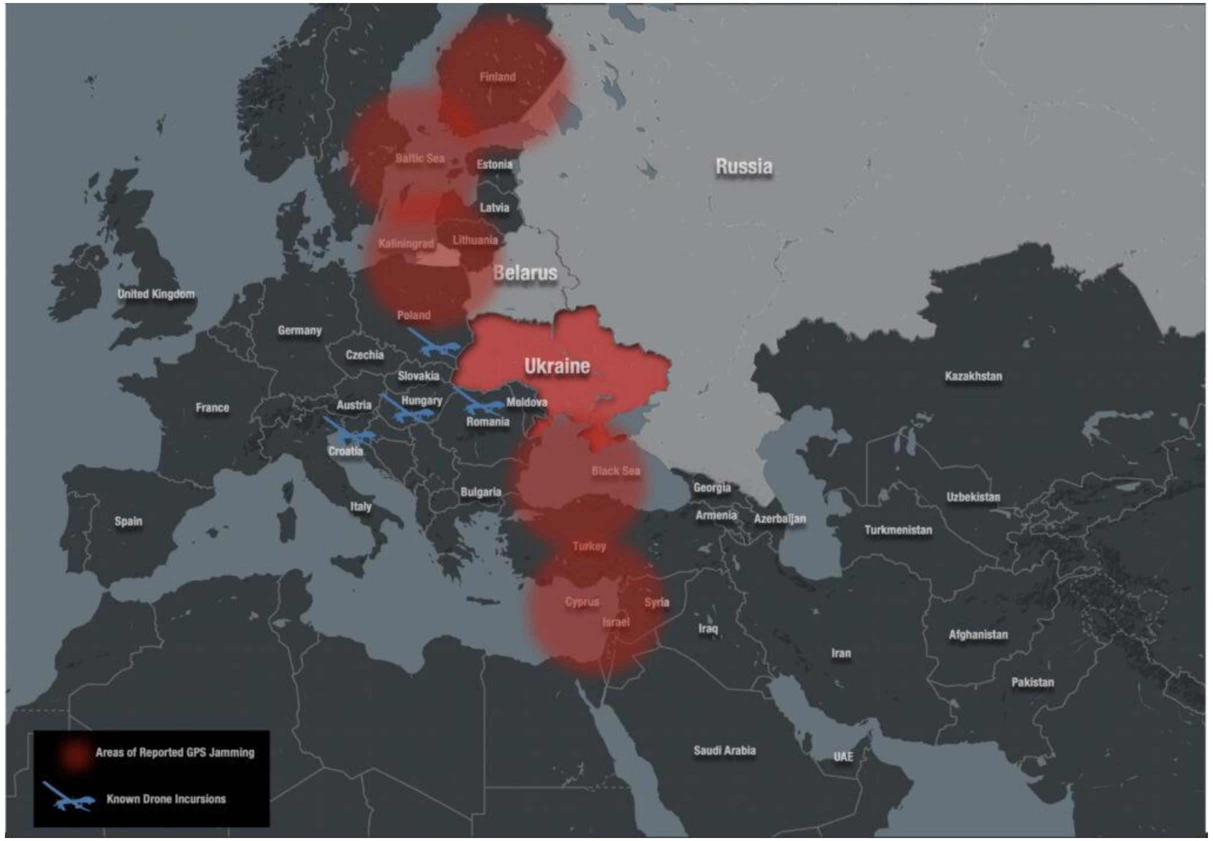


The weakness makes the signals sensitive to interference.

Radio Frequency Interference (RFI)			
Unintentional		**Intentional**	
Wideband modulation	- TV transmitter‘s harmonic - microwave link transmitters	**Wideband Gaussian**	Intentional noise jammers
Wideband pulse	- Radars (burst transmitter's) - ultrawideband	**Wideband spread spectrum**	Intentional spectrum jammers or pseudolites
		Narrowband continuous wave (CW)	Intentional CW jammers

Current Jamming Risks in Europe

Thousands of GNSS jamming and spoofing incidents are reported in each year.



Source: https://ops.group/blog/spill-over-effect-new-airspace-risks-in-europe/

Some of reported GNSS attacks

Thousands of GNSS jamming and spoofing incidents are reported in each year (how many more are unreported)?

Reported GNSS Attacks

2009 and 2012:
At Newark Airport in 2009 and 2012, interference to a new, GPS-based landing system was traced to lorries travelling along the adjacent New Jersey Turnpike.

February 2016:
GNSS error caused satellites to provide incorrect time information, impacting operations of several companies

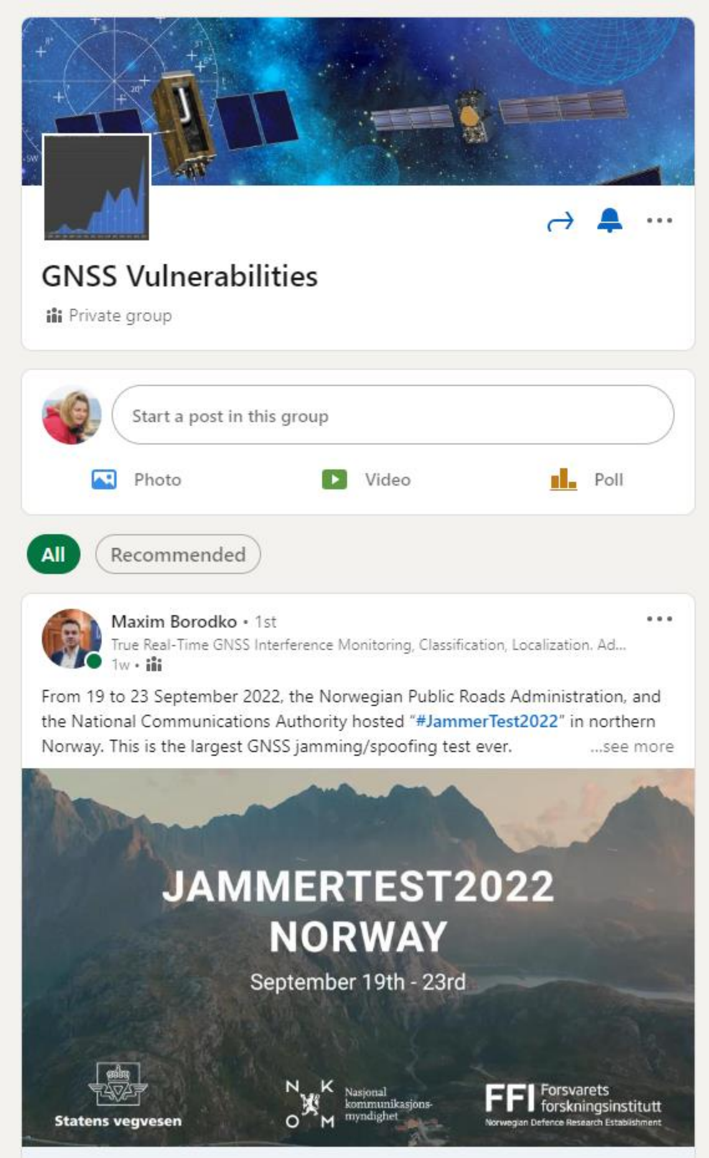
March 2016:
The fourth round of GPS jamming by North Korea since 2010.

November 2018:
During NATO military exercises, airspace in Finland was disturbed by GNSS jamming.

June 2019:
Jamming caused disturbances of operations at Israeli airport, source unknown.

March 2022:
GNSS permanent attacks especially on **Ukrainian critical network infrastructure**.

GNSS Vulnerabilities LinkedIn group



GNSS Vulnerabilities

Private group

Maxim Borodko • 1st
True Real-Time GNSS Interference Monitoring, Classification, Localization, Ad...
1w •

From 19 to 23 September 2022, the Norwegian Public Roads Administration, and the National Communications Authority hosted "#JammerTest2022" in northern Norway. This is the largest GNSS jamming/spoofing test ever.

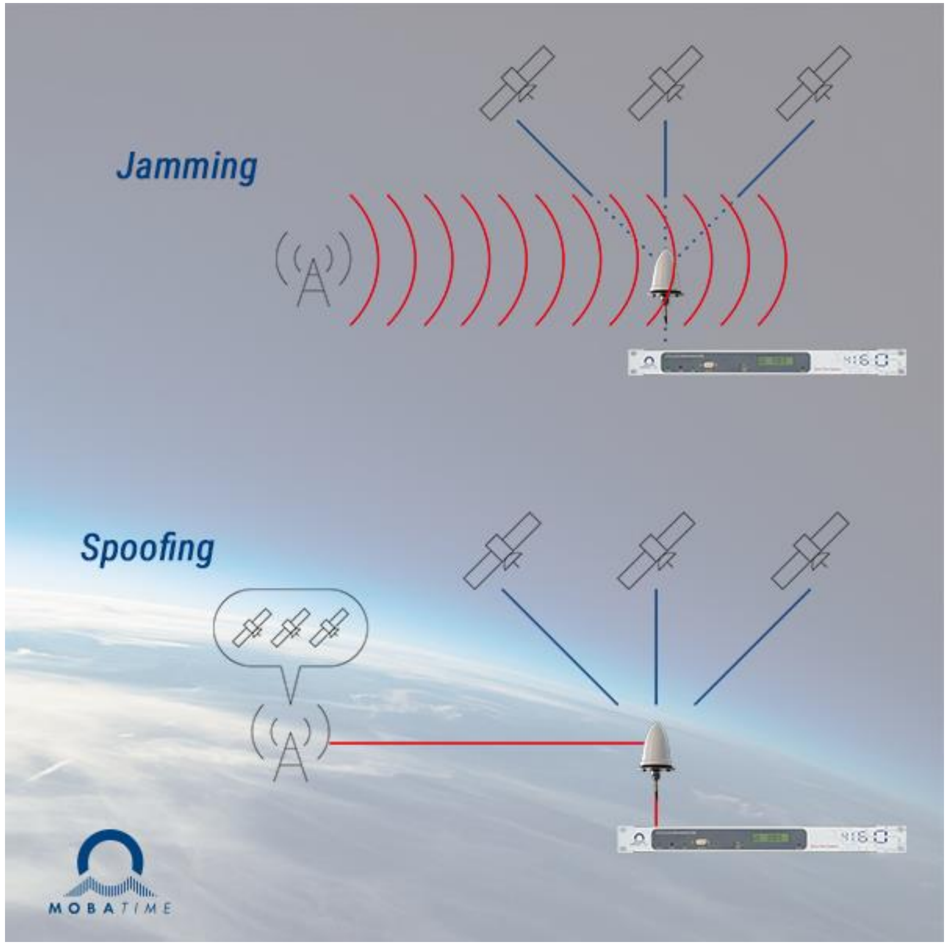
JAMMERTEST2022
NORWAY
September 19th - 23rd

Statens vegvesen

NKOM Nasjonal kommunikasjons-myndighet

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

Deliberate interference



Source: https://www.mobatime.com/article/jamming/

Jamming

„white noise interference“

Effects:

- loss of accuracy
- loss of GNSS positioning/timing

Spoofing

„intelligent form of interference“

Effects:

- fooling the user into wrong position
- misleading the user into wrong time

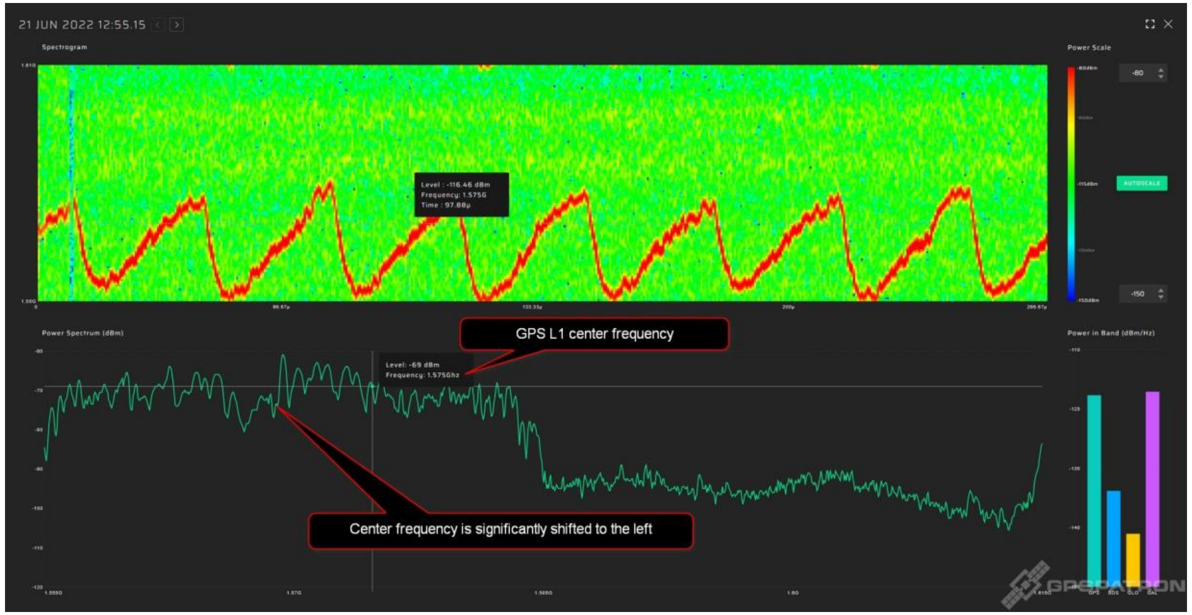
Source: https://www.ohb-digital.at

EUPOS
European Position Determination System

Jamming

- Jammers significantly deteriorate GNSS performance in terms of accuracy, integrity, availability.

Chirp jammer‘s properties:
- almost constant amplitude
- almost periodic frequency
- working at single or multi-frequency level



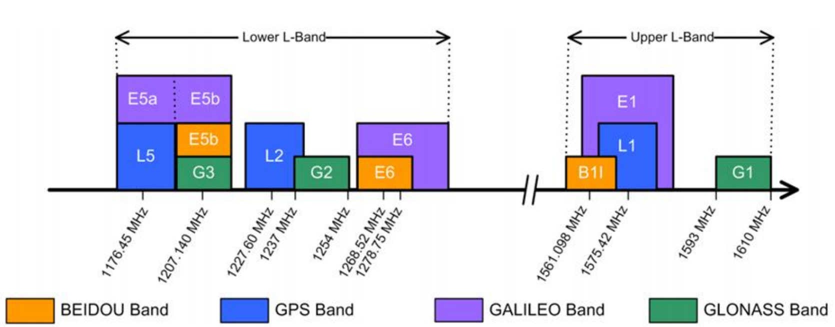
Level : -116.46 dBm
Frequency: 1.5756
Time : 97.88μ

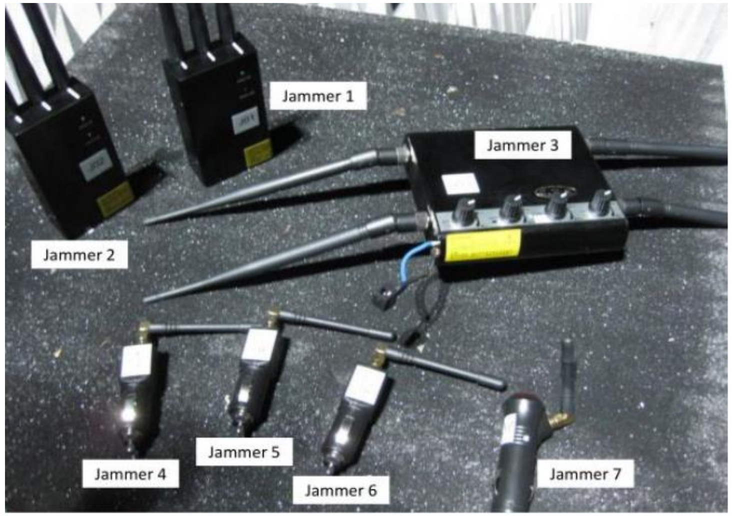
GPS L1 center frequency

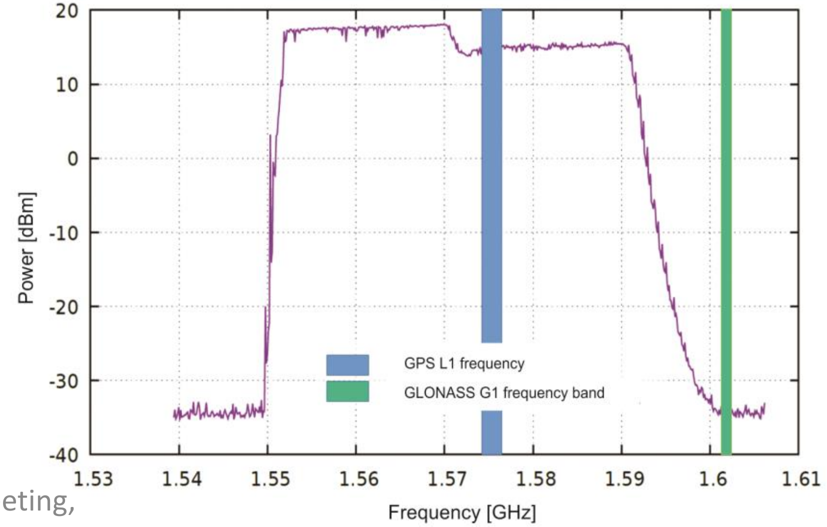
Level: -69 dBm
Frequency: 1.5756Ghz

Center frequency is significanty shifted to the left

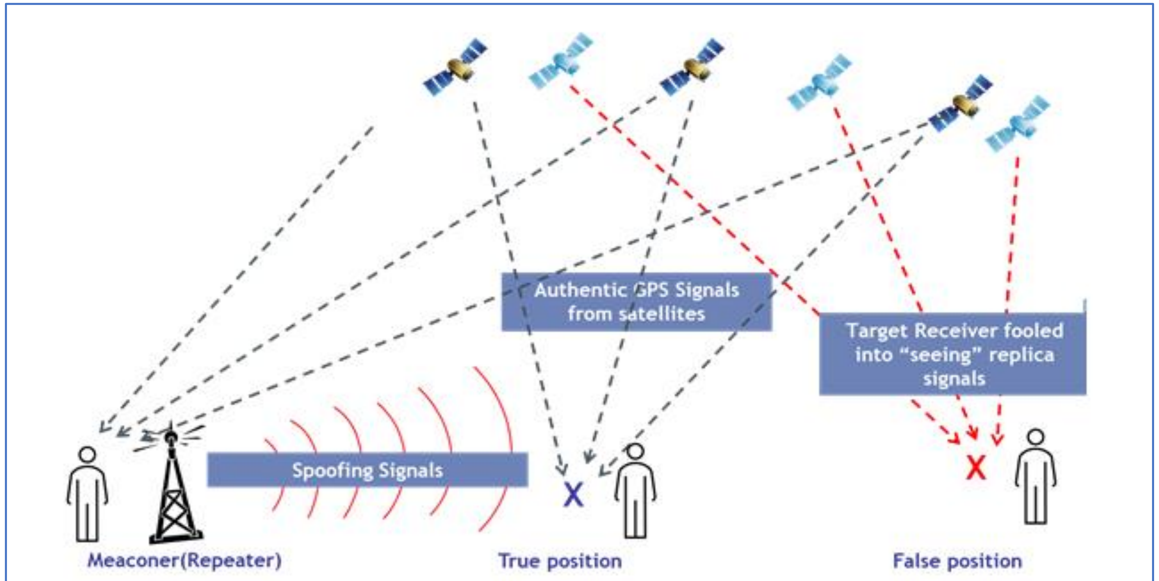
Source: gpspatron.com



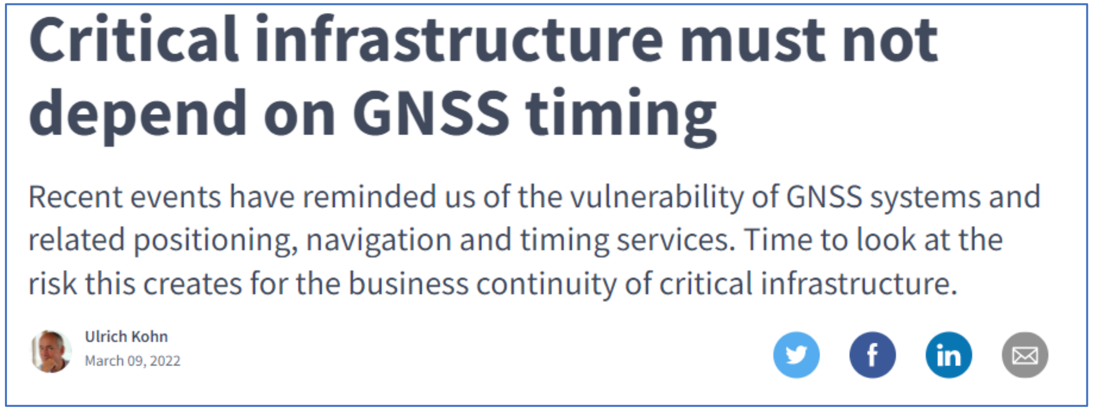




GNSS attacks‘ influences on critical infrastructure


Authentic GPS Signals from satellites
Target Receiver fooled into "seeing" replica signals
Spoofing Signals
X
X
Meaconer(Repeater)
True position
False position

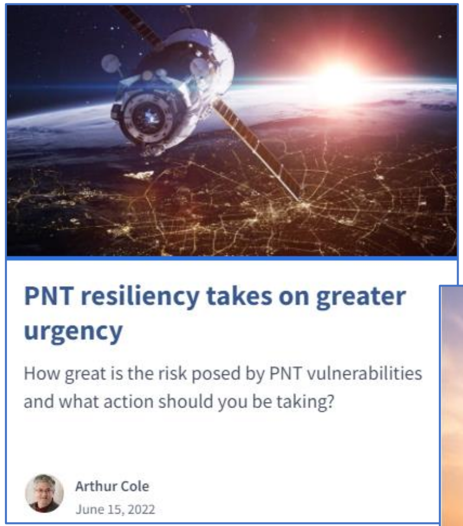
Source: https://www.thegpstime.com/gnss-receiver-meaconing-or-spoofing-scenarios/



Critical infrastructure must not depend on GNSS timing

Recent events have reminded us of the vulnerability of GNSS systems and related positioning, navigation and timing services. Time to look at the risk this creates for the business continuity of critical infrastructure.

Ulrich Kohn
March 09, 2022



PNT resiliency takes on greater urgency

How great is the risk posed by PNT vulnerabilities and what action should you be taking?

Arthur Cole
June 15, 2022

The future of smart grid networking

How is new innovation helping utility network operators keep pace with quickly changing energy markets?

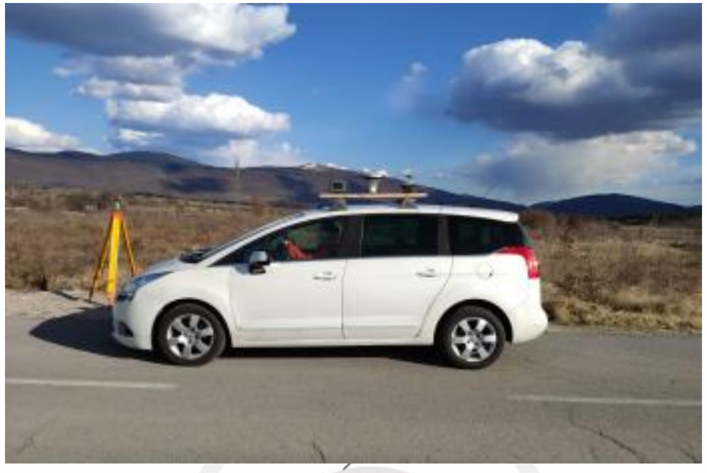
Ulrich Kohn
June 10, 2022

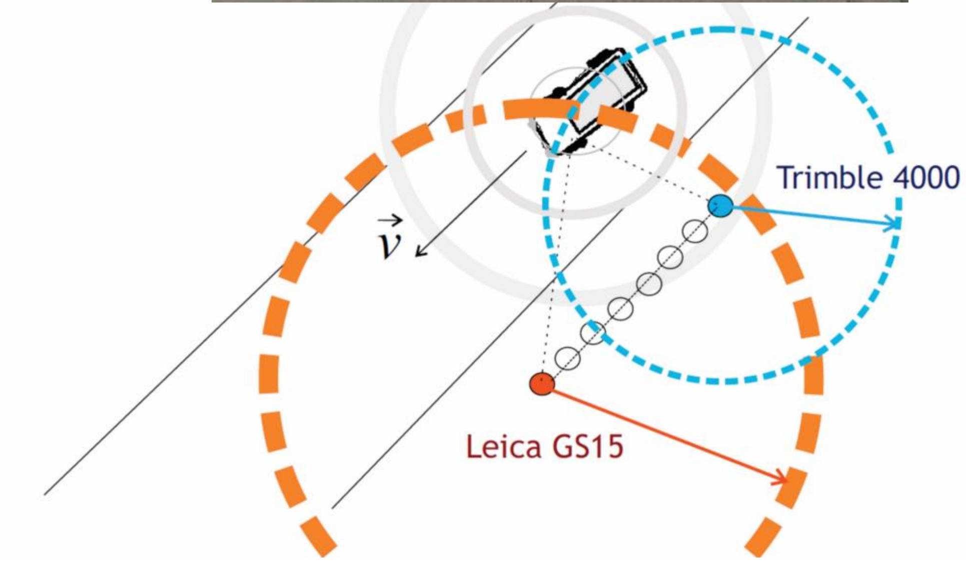
Talking sync strategies for smart grids

How can utility networks achieve the assured PNT services they need to stay operational and online? Time to consider the future of ...

Nino De Falcis
March 11, 2022

Jamming experiments in Slovenia

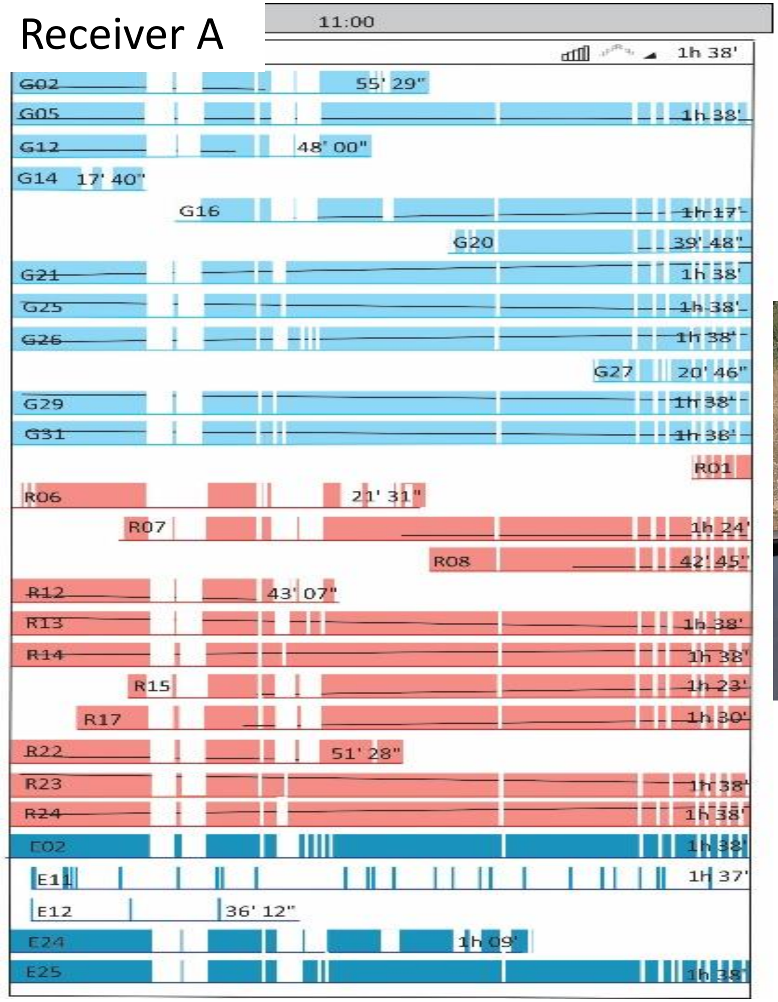


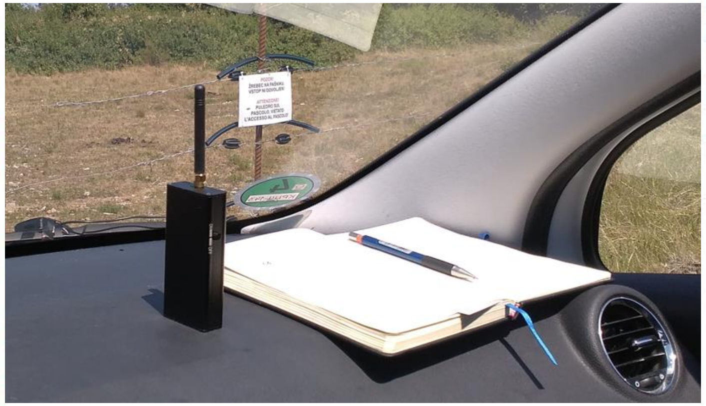


Approved by **Agency for Communication Network and Services of the Republic of Slovenia (AKOS).**

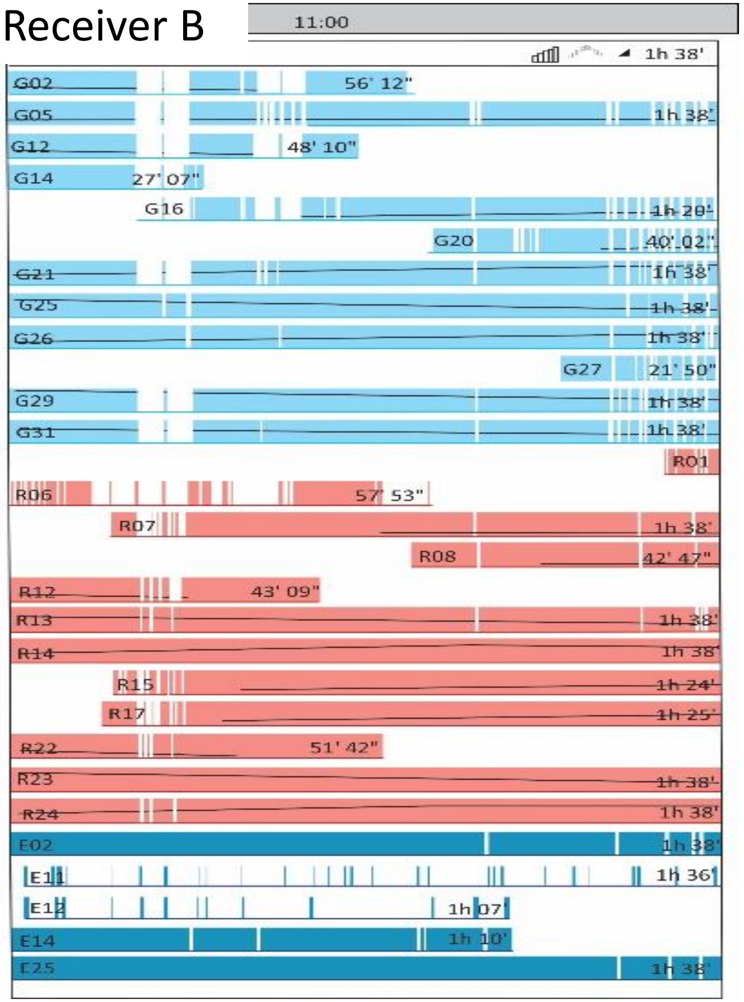
L1/E1 Chirp Jammer:
Response of two receivers #1

Receiver A



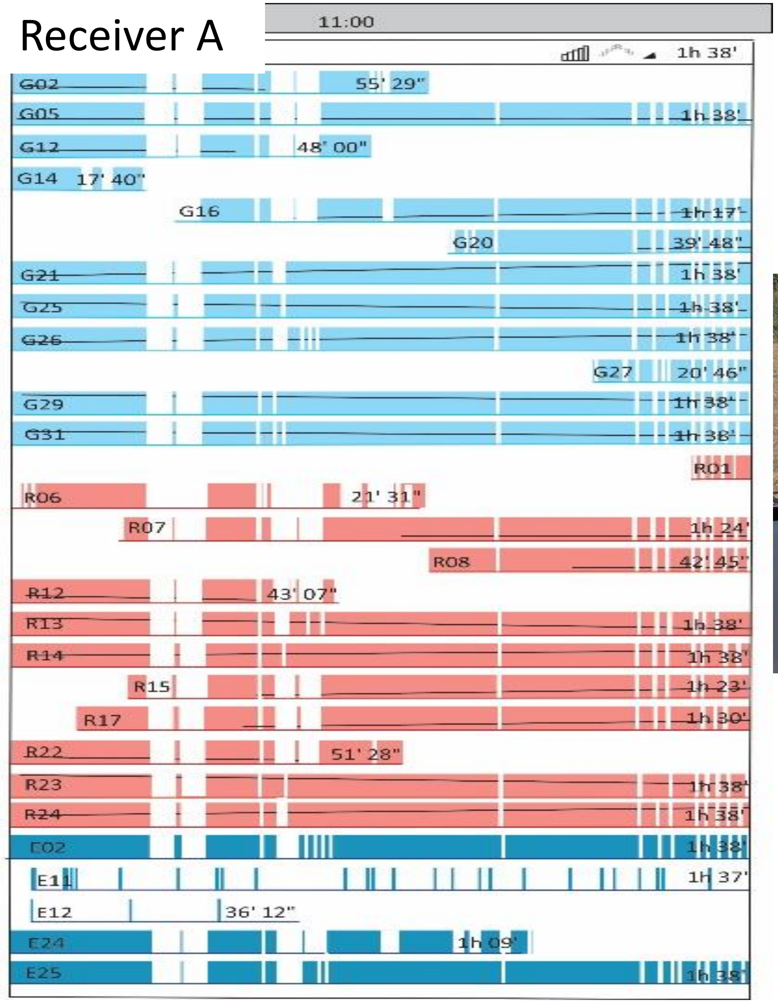


Receiver B

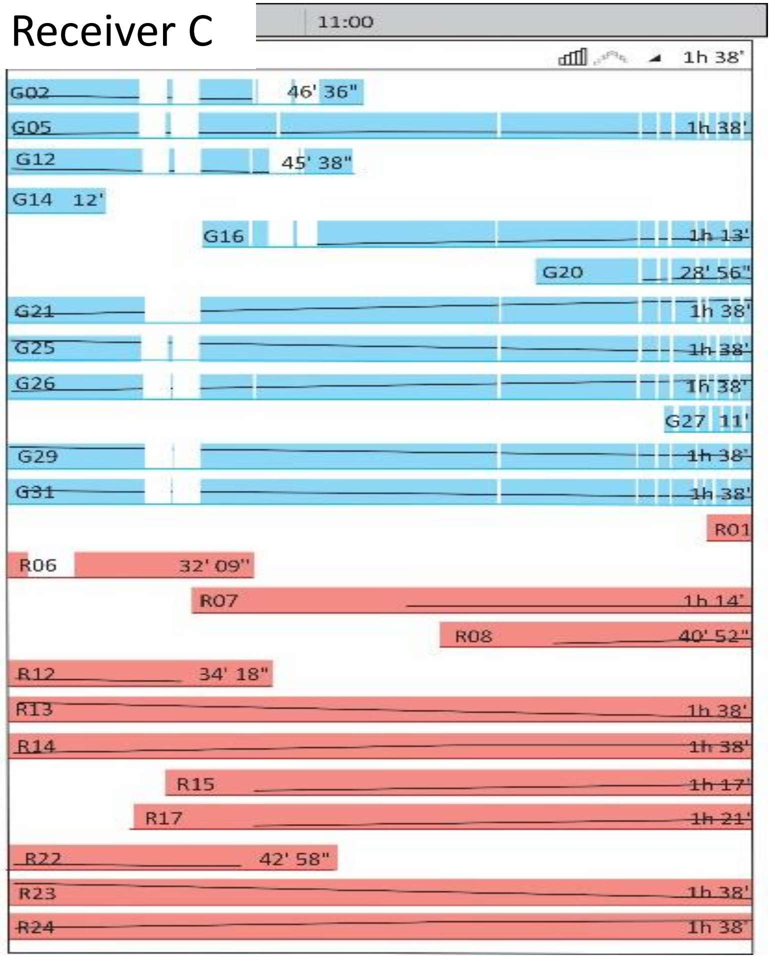


L1/E1 Chirp Jammer: Response of receivers #2

Receiver A

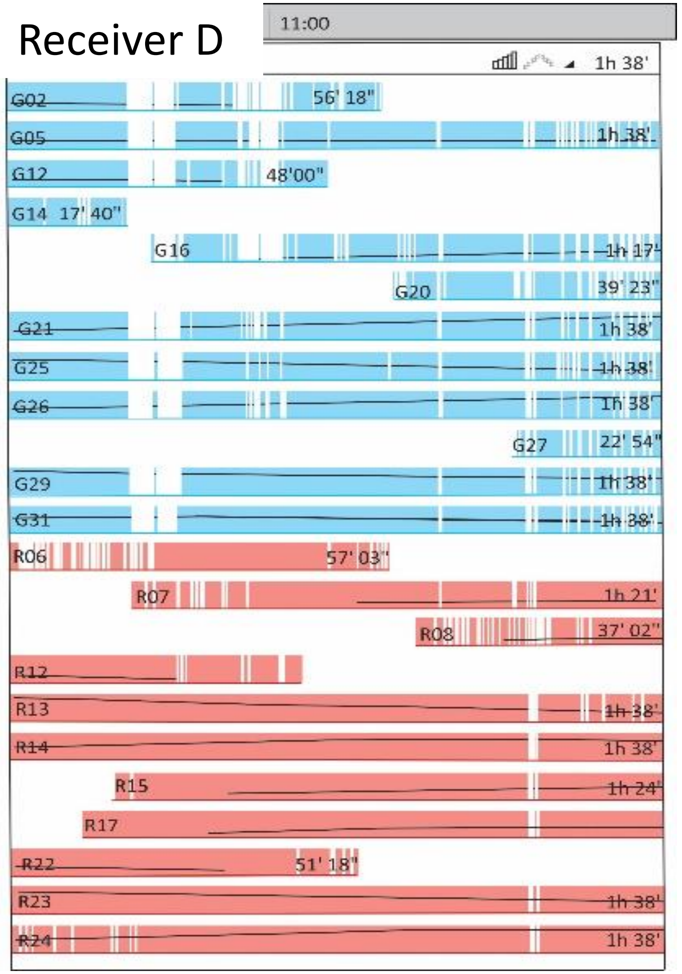


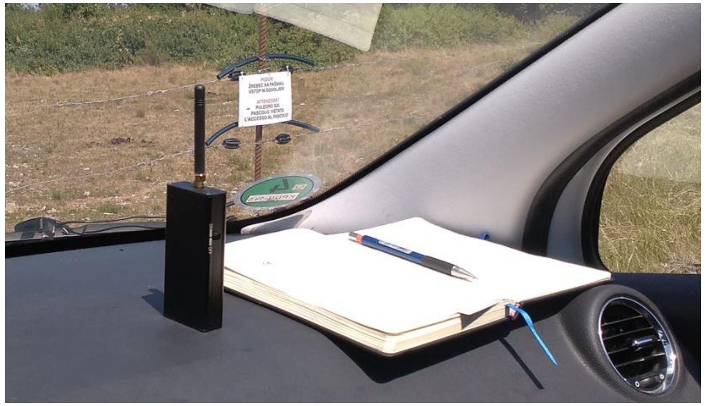
Receiver C



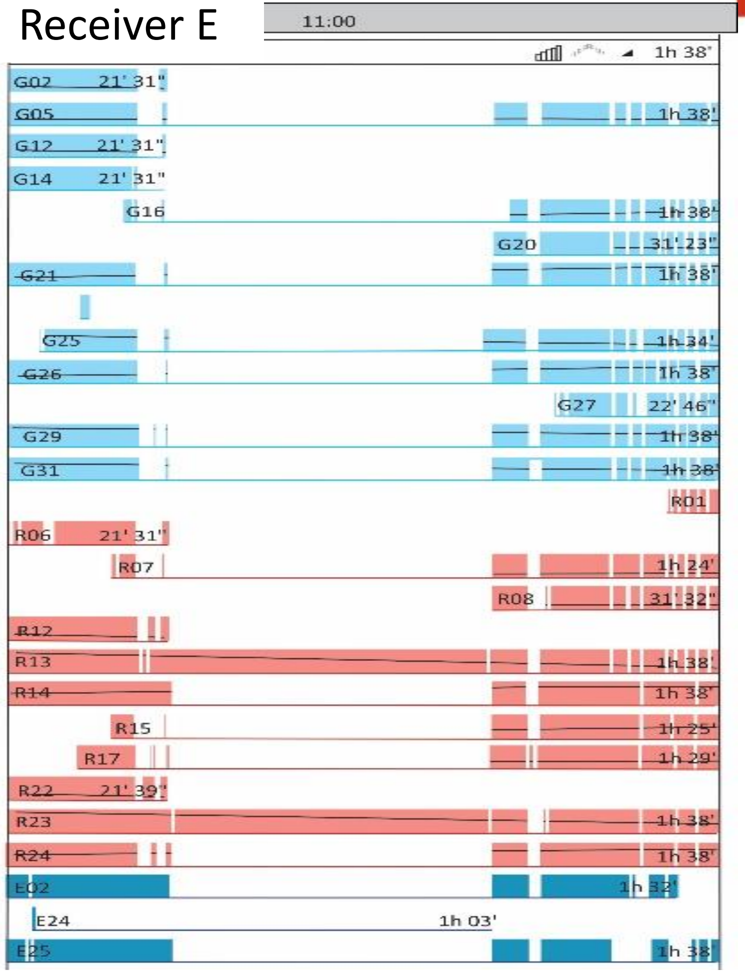
L1/E1 Chirp Jammer: Response of receivers #3

Receiver D

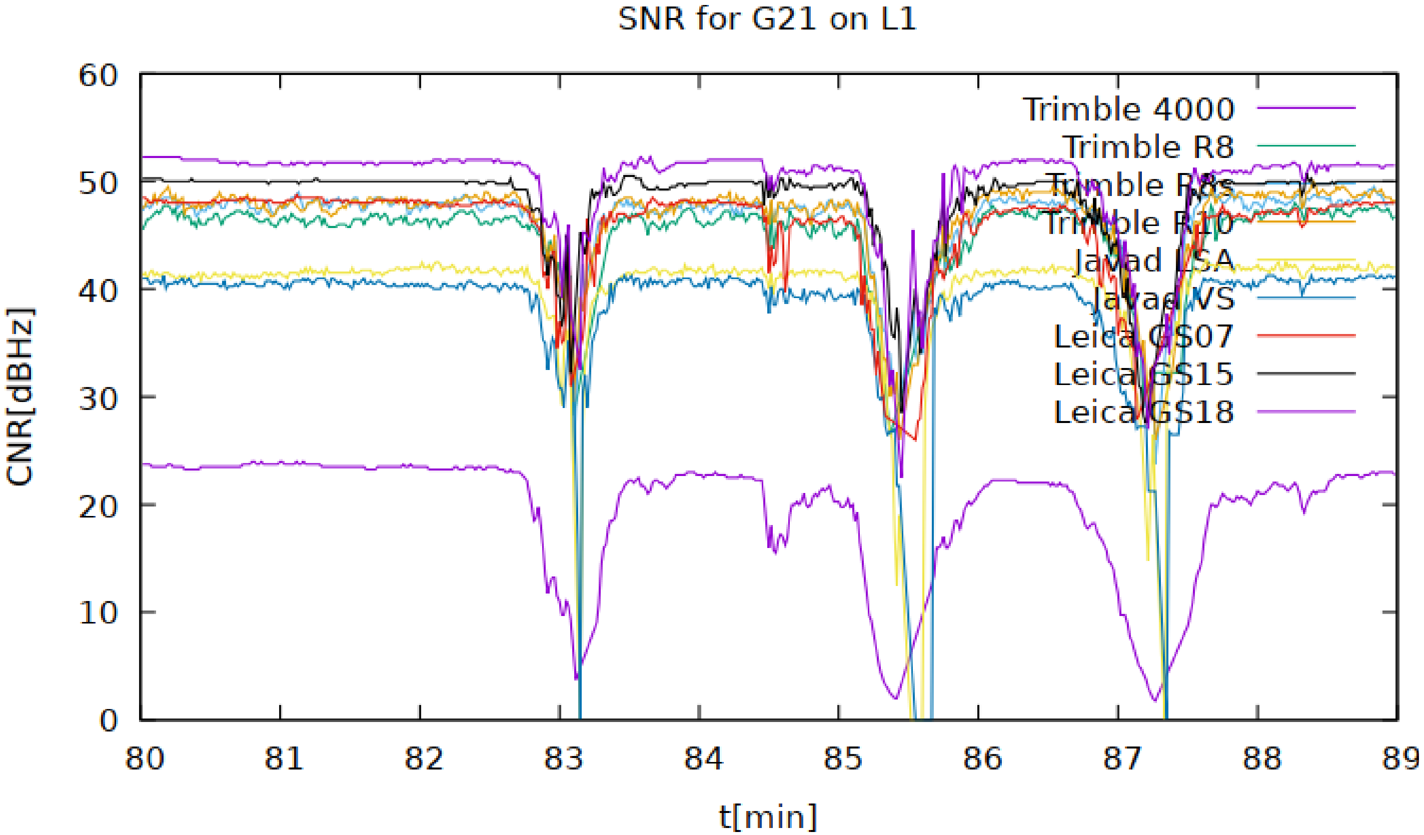


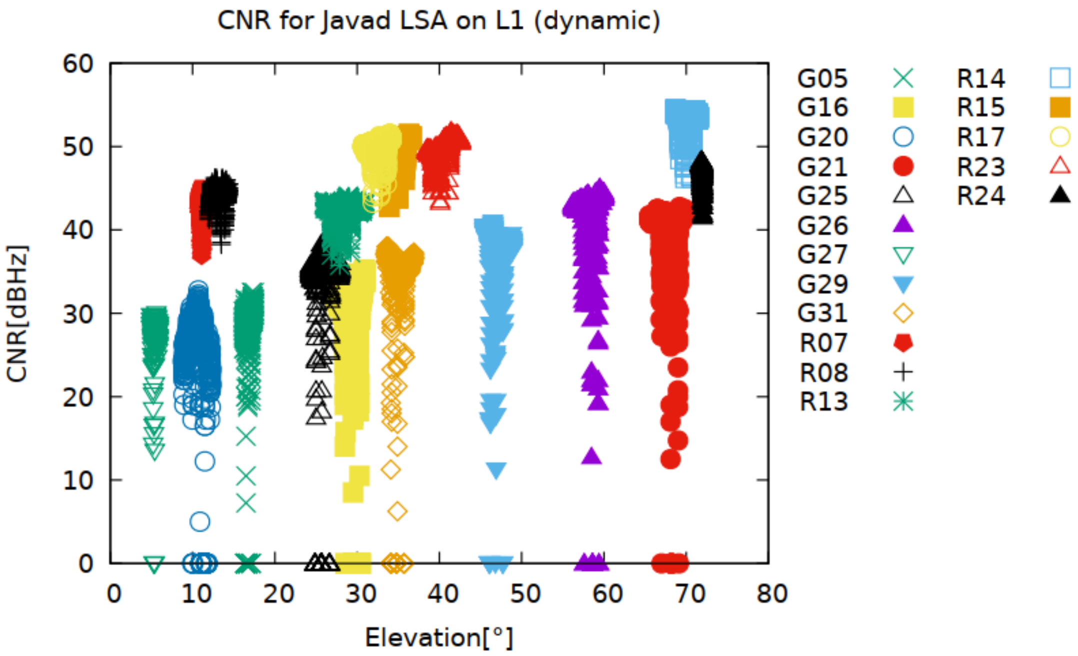


Receiver E



Jamming effect on C/N0



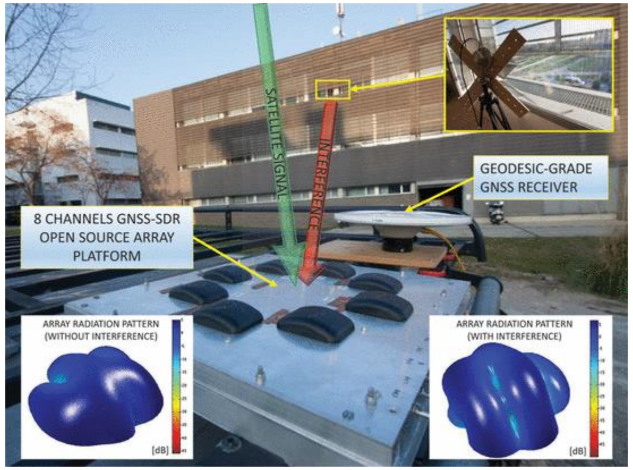


The estimated C/N₀ can reveal the presence of interfering signals.
It is highly recommended to verify if C/N0 measurements are affected by correlated changes.

Defenses against Jamming

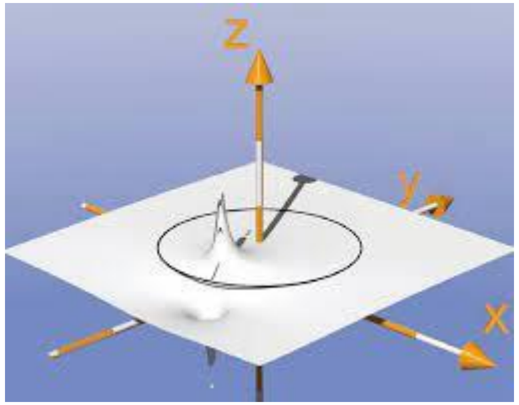
Detection and Mitigation

- antenna defenses


SATELLITE SIGNAL
INTERFERENCE
GEODESIC-GRADE GNSS RECEIVER
8 CHANNELS GNSS-SDR OPEN SOURCE ARRAY PLATFORM
ARRAY RADIATION PATTERN (WITHOUT INTERFERENCE)
[dB]
ARRAY RADIATION PATTERN (WITH INTERFERENCE)
[dB]

J. Arribas, P. Closas, C. Fernández-Prades, "Interference Mitigation in GNSS Receivers by Array Signal Processing: A Software Radio Approach

- signal processing defenses (adaptive notch filters)
  ***minimization** of the **energy** of the signal at the output of the filter*



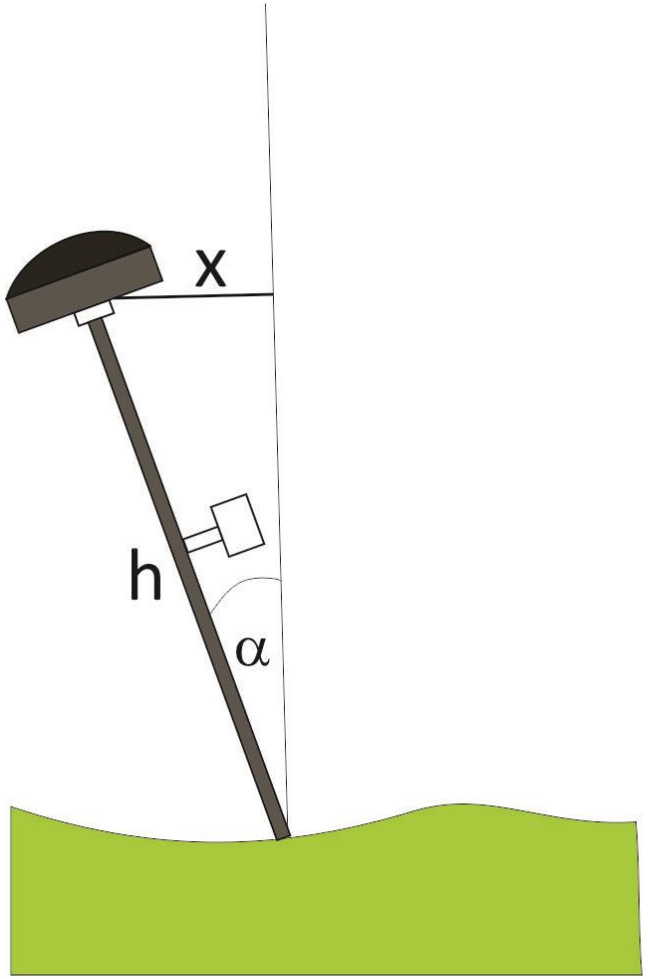
Adaption block which tracks the jamming instantaneous frequency.

Jamming Mitigation Solutions

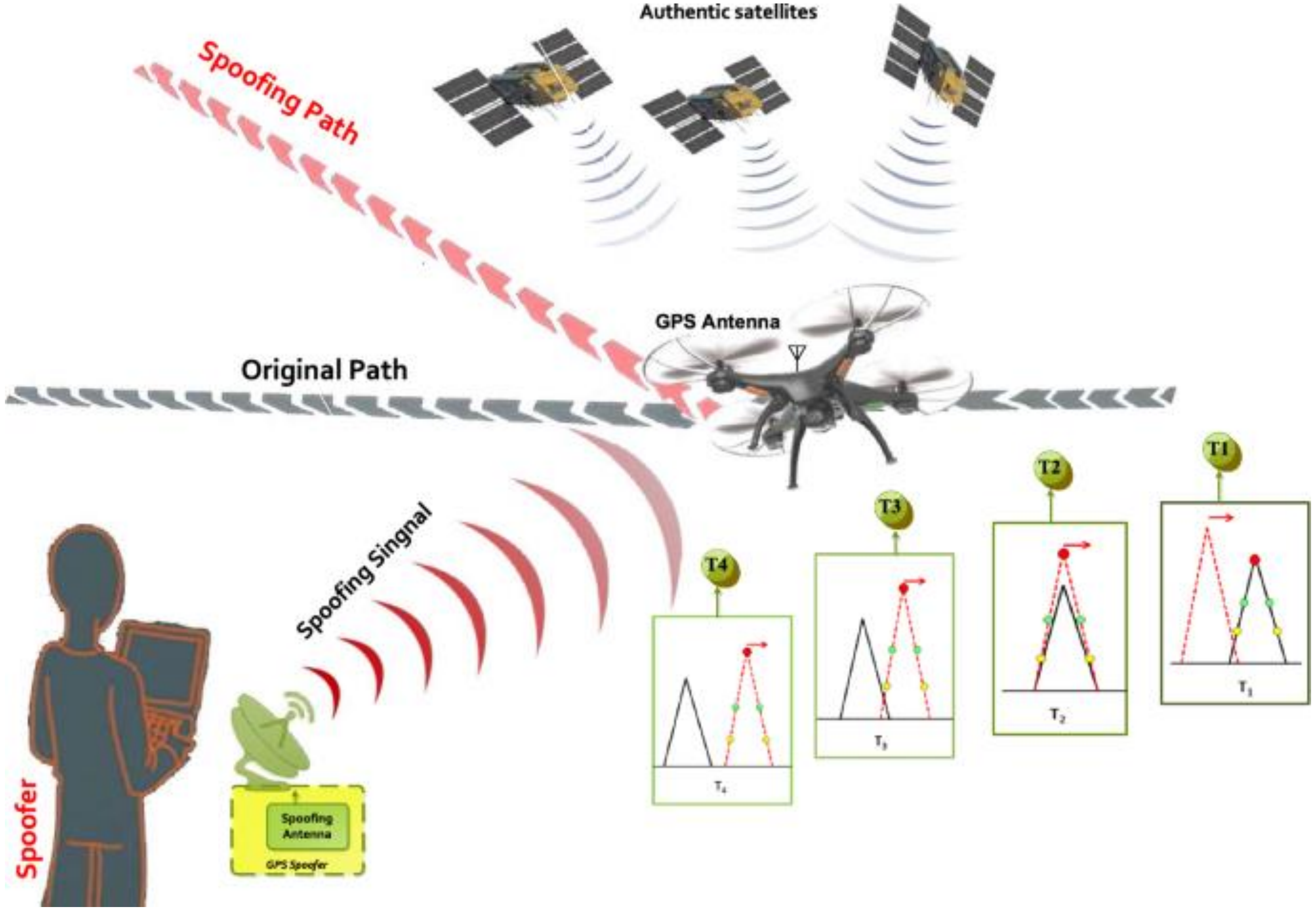
An efficient way of GNSS jamming mitigation based on polarization exists:

- Physical Rotation of the antenna in synchronized way to the jammer‘s location

  →not appliable for static receivers
- Digital Rotation of the antenna in time-domain.



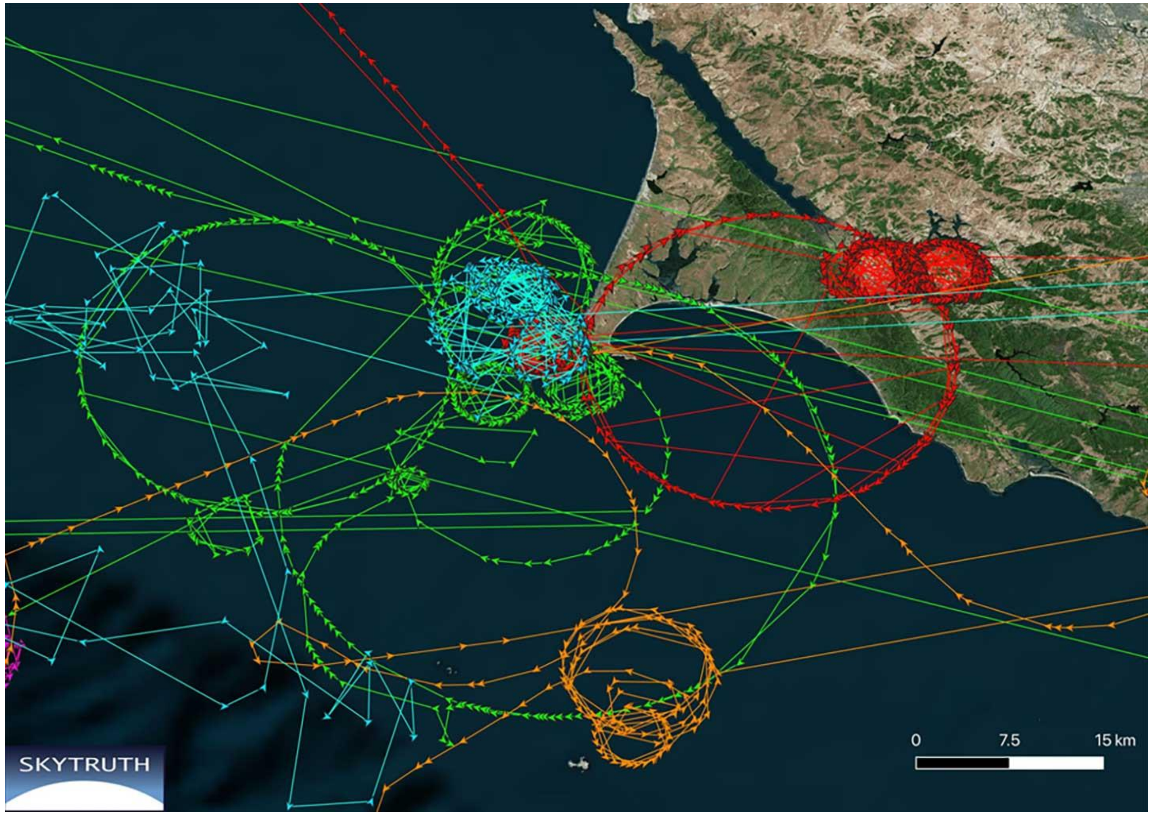
GNSS Spoofing

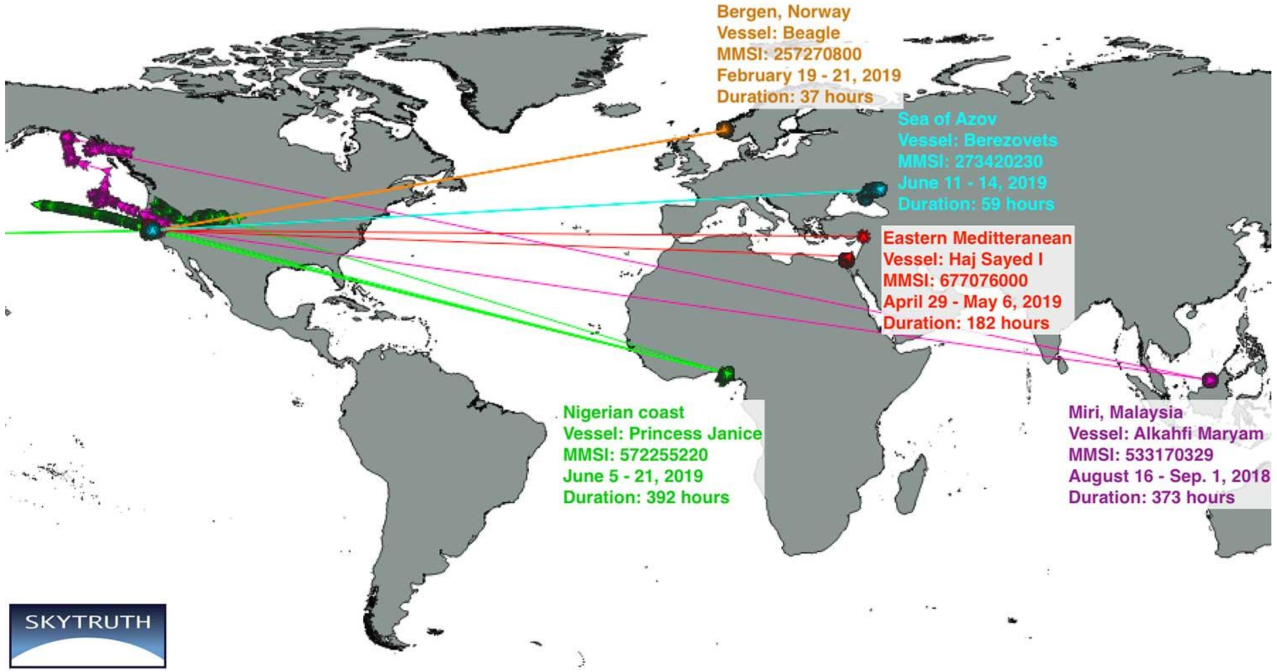


Source: Shafiee, E & Mosavi, M. & Moazedi, Maryam & Shafiee, Ebrahim. (2021). A Modified Imperialist Competitive Algorithm for Spoofing Attack Detection in Single-Frequency GPS Receivers. Wireless Personal Communications. 119. 10.1007/s11277-021-08244-2.

GNSS Spoofing Accidents: Maritime

In the most recent observations, the actual locations of the ships were thousands of miles away. In most cases, literally halfway across the globe.





Bergen, Norway
Vessel: Beagle
MMSI: 257270800
February 19 - 21, 2019
Duration: 37 hours

Sea of Azov
Vessel: Berezovets
MMSI: 273420230
June 11 - 14, 2019
Duration: 59 hours

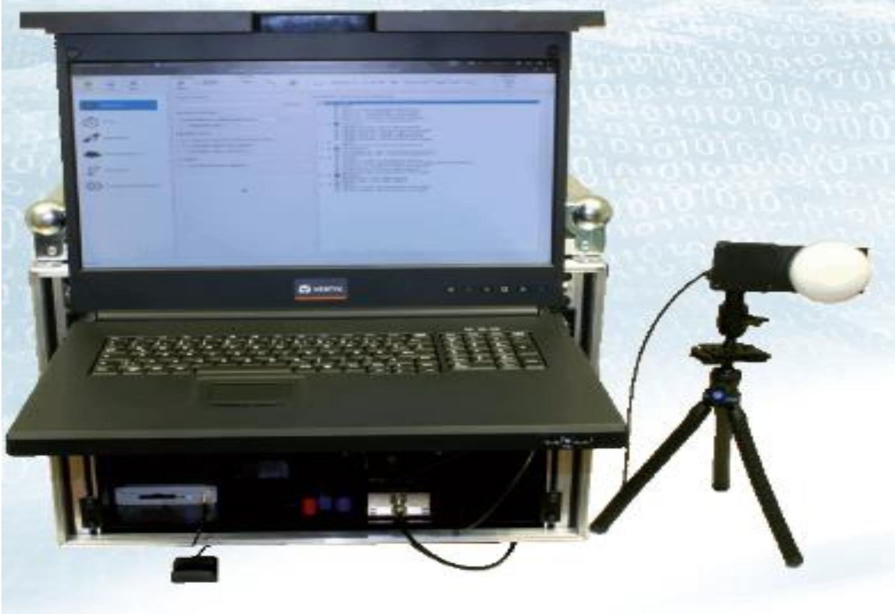
Eastern Meditteranean
Vessel: Haj Sayed I
MMSI: 677076000
April 29 - May 6, 2019
Duration: 182 hours

Nigerian coast
Vessel: Princess Janice
MMSI: 572255220
June 5 - 21, 2019
Duration: 392 hours

Miri, Malaysia
Vessel: Alkahfi Maryam
MMSI: 533170329
August 16 - Sep. 1, 2018
Duration: 373 hours

Source: https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/

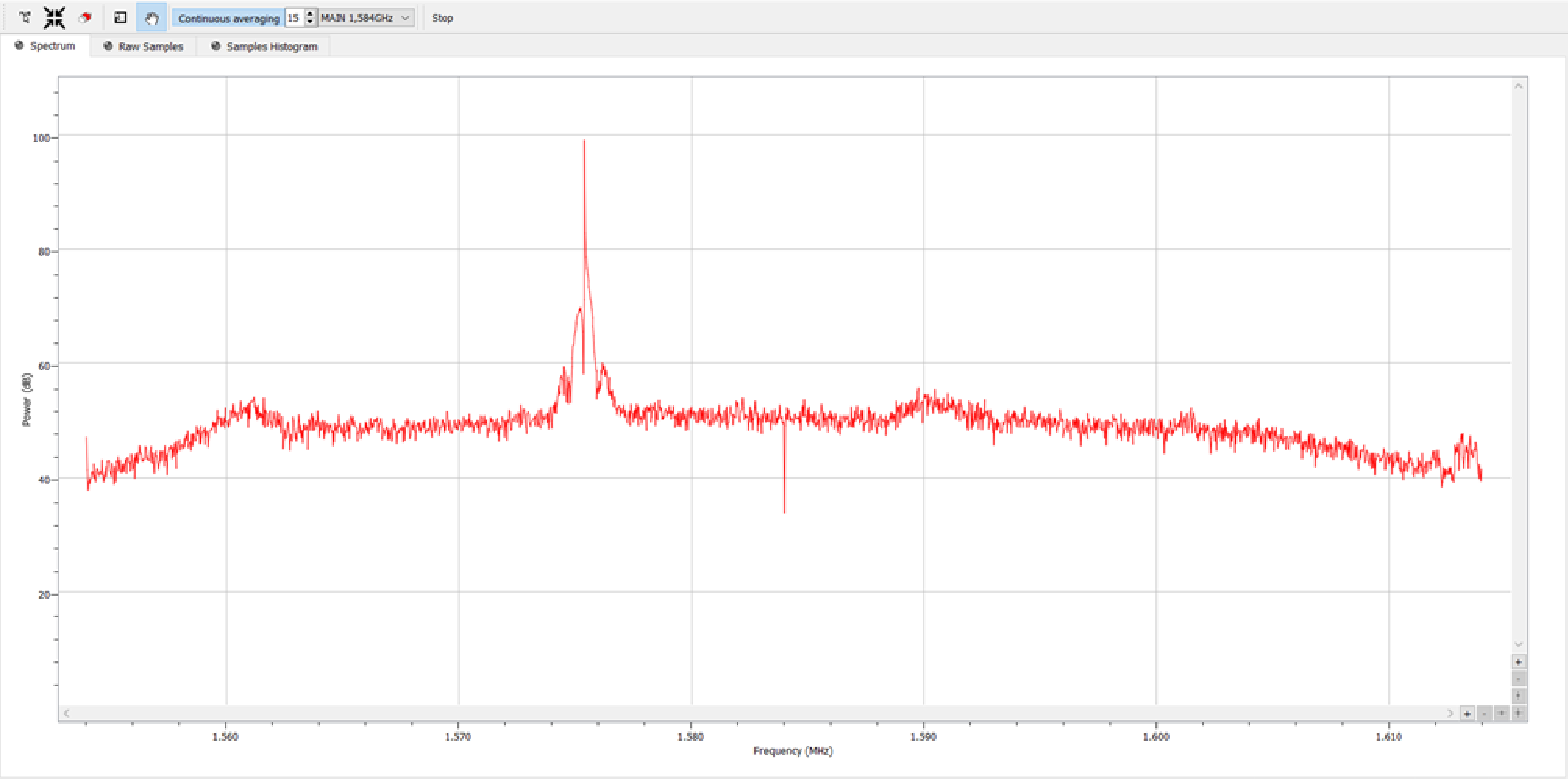
Spoofing equipment



Source: https://www.ohb-digital.at

First sign to look out whether you are spoofed…

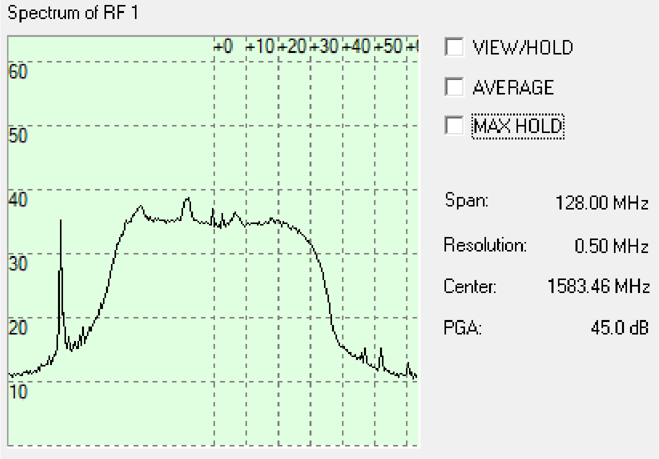
The spoofed signals are visible in the radio-frequency spectrum.



The low power of GPS signals means that they are barely discernible from the thermal noise background.

To spoof a receiver, **the SDR signals are transmitted with a much higher power** making them clearly visible above the background.

2nd sign to look out whether you are spoofed…



Spectrum of RF 1

□ VIEW/HOLD

□ AVERAGE

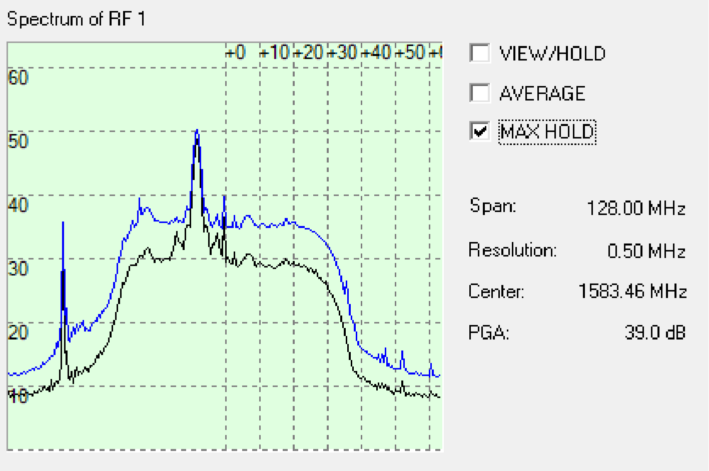
□ MAX HOLD

Span: 128.00 MHz

Resolution: 0.50 MHz

Center: 1583.46 MHz

PGA: 45.0 dB



Spectrum of RF 1

□ VIEW/HOLD

□ AVERAGE

☑ MAX HOLD

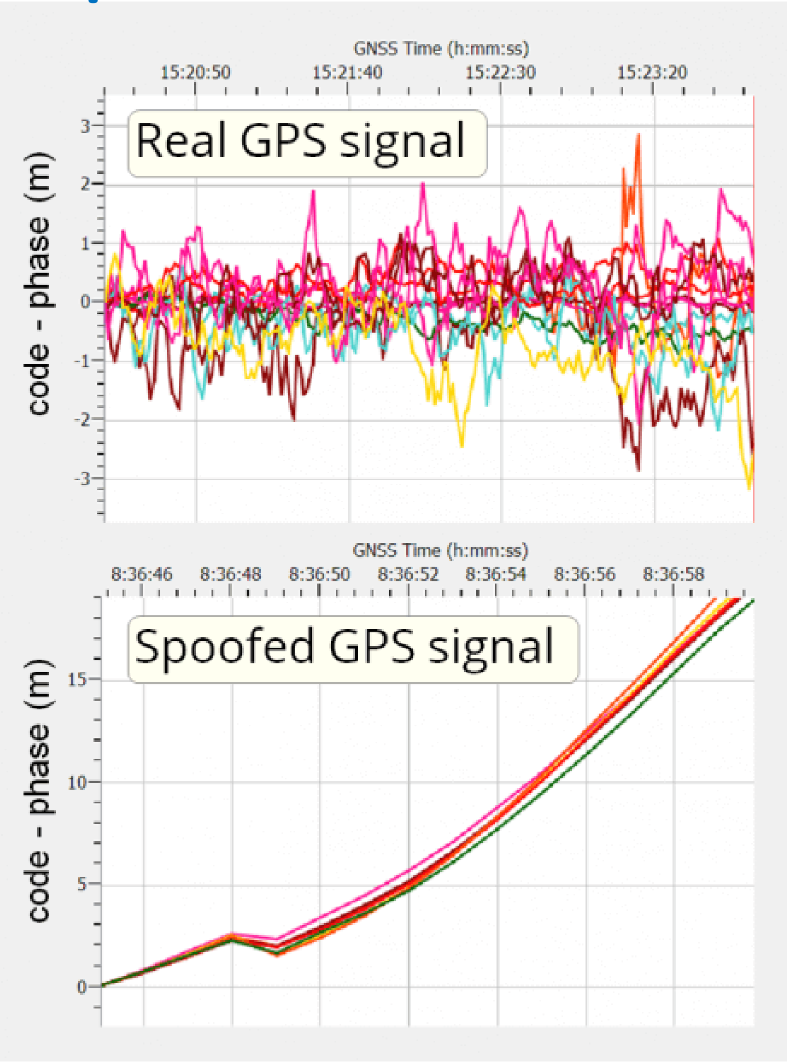
Span: 128.00 MHz

Resolution: 0.50 MHz

Center: 1583.46 MHz

PGA: 39.0 dB

Spectrum uBlox F9P before and during spoofing



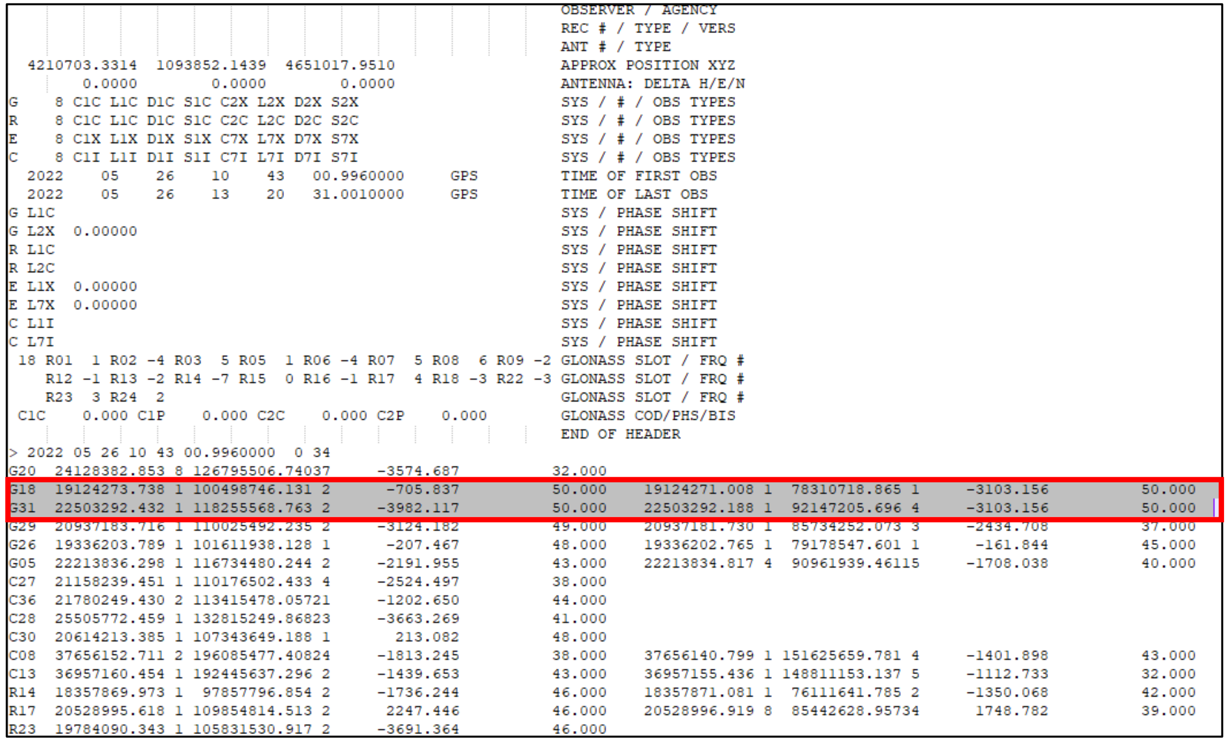
Divergent code minus carrier behaviour

Source:
https://www.septentrio.com/en/learn-more/insights/spoofing-your-gps-attack-proof

3rd sign to look out whether you are spoofed…

Confused RINEX data

- Incomplete and/or inaccurate NAV and OBS files



```
                                                            OBSERVER / AGENCY
                                                            REC # / TYPE / VERS
                                                            ANT # / TYPE
  4210703.3314  1093852.1439  4651017.9510                  APPROX POSITION XYZ
        0.0000        0.0000        0.0000                  ANTENNA: DELTA H/E/N
G    8 C1C L1C D1C S1C C2X L2X D2X S2X                      SYS / # / OBS TYPES
R    8 C1C L1C D1C S1C C2C L2C D2C S2C                      SYS / # / OBS TYPES
E    8 C1X L1X D1X S1X C7X L7X D7X S7X                      SYS / # / OBS TYPES
C    8 C1I L1I D1I S1I C7I L7I D7I S7I                      SYS / # / OBS TYPES
  2022    05    26    10    43   00.9960000     GPS         TIME OF FIRST OBS
  2022    05    26    13    20   31.0010000     GPS         TIME OF LAST OBS
G L1C                                                       SYS / PHASE SHIFT
G L2X  0.00000                                              SYS / PHASE SHIFT
R L1C                                                       SYS / PHASE SHIFT
R L2C                                                       SYS / PHASE SHIFT
E L1X  0.00000                                              SYS / PHASE SHIFT
E L7X  0.00000                                              SYS / PHASE SHIFT
C L1I                                                       SYS / PHASE SHIFT
C L7I                                                       SYS / PHASE SHIFT
 18 R01  1 R02 -4 R03  5 R05  1 R06 -4 R07  5 R08  6 R09 -2 GLONASS SLOT / FRQ #
    R12 -1 R13 -2 R14 -7 R15  0 R16 -1 R17  4 R18 -3 R22 -3 GLONASS SLOT / FRQ #
    R23  3 R24  2                                           GLONASS SLOT / FRQ #
 C1C    0.000 C1P    0.000 C2C    0.000 C2P    0.000        GLONASS COD/PHS/BIS
                                                            END OF HEADER
> 2022 05 26 10 43 00.9960000  0 34
G20  24128382.853 8 126795506.74037       -3574.687          32.000
G18  19124273.738 1 100498746.131 2        -705.837          50.000    19124271.008 1  78310718.865 1       -3103.156          50.000
G31  22503292.432 1 118255568.763 2       -3982.117          50.000    22503292.188 1  92147205.696 4       -3103.156          50.000
G29  20937183.716 1 110025492.235 2       -3124.182          49.000    20937181.730 1  85734252.073 3       -2434.708          37.000
G26  19336203.789 1 101611938.128 1        -207.467          48.000    19336202.765 1  79178547.601 1        -161.844          45.000
G05  22213836.298 1 116734480.244 2       -2191.955          43.000    22213834.817 4  90961939.46115       -1708.038          40.000
C27  21158239.451 1 110176502.433 4       -2524.497          38.000
C36  21780249.430 2 113415478.05721       -1202.650          44.000
C28  25505772.459 1 132815249.86823       -3663.269          41.000
C30  20614213.385 1 107343649.188 1         213.082          48.000
C08  37656152.711 2 196085477.40824       -1813.245          38.000    37656140.799 1 151625659.781 4       -1401.898          43.000
C13  36957160.454 1 192445637.296 2       -1439.653          43.000    36957155.436 1 148811153.137 5       -1112.733          32.000
R14  18357869.973 1  97857796.854 2       -1736.244          46.000    18357871.081 1  76111641.785 2       -1350.068          42.000
R17  20528995.618 1 109854814.513 2        2247.446          46.000    20528996.919 8  85442628.95734        1748.782          39.000
R23  19784090.343 1 105831530.917 2       -3691.364          46.000
```

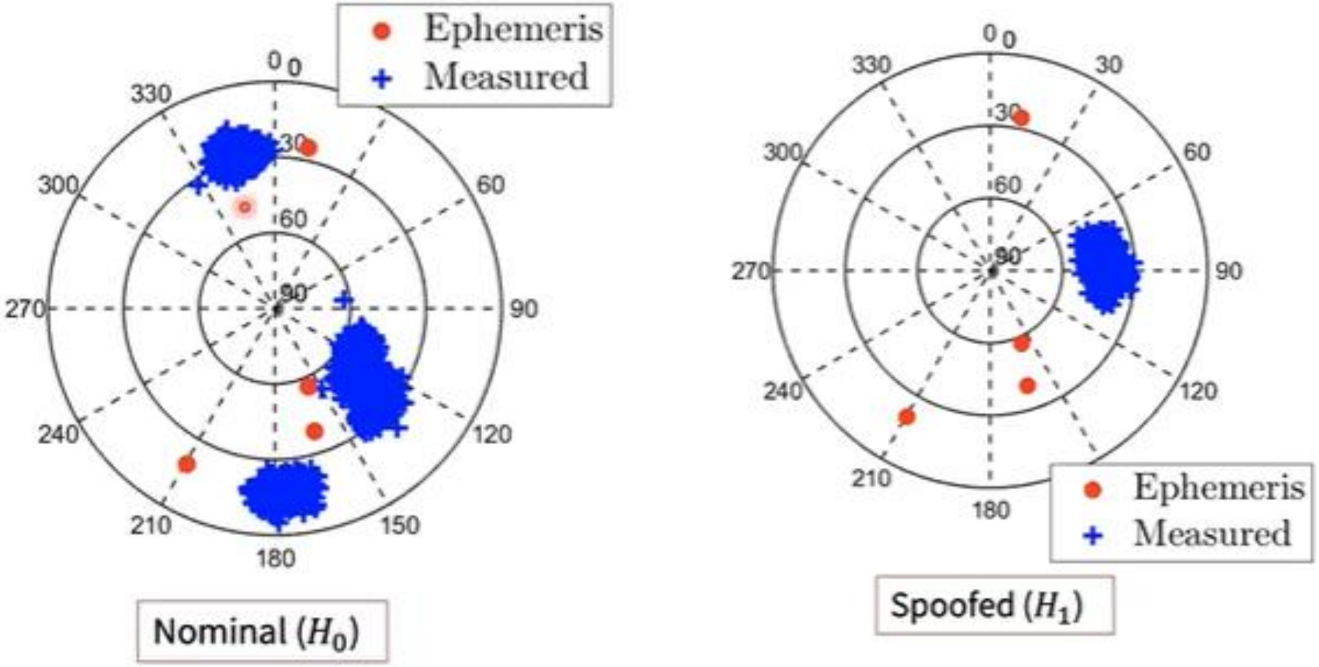
SIGNS FOR SPOOFED SIGNALS IN RINEX „OBS“

1. Very high SNR value (50.0)
2. The same Doppler data (impossible for two satellites).
3. Added satellite data for satellite not in view.

GNSS spoofing detection through spatial processing

SPOOFED NAVIGATION MESSAGE

- An algorithmic framework for signal-geometry-based approaches of GNSS spoofing detection exist.
- Algorithms are based on formulation of a simple vs. simple hypothesis test independent of nuisance parameters that results in significantly reduced missed detection probability compared to prior approaches.
- It is highly tractable such that it can be computed online by the receiver.

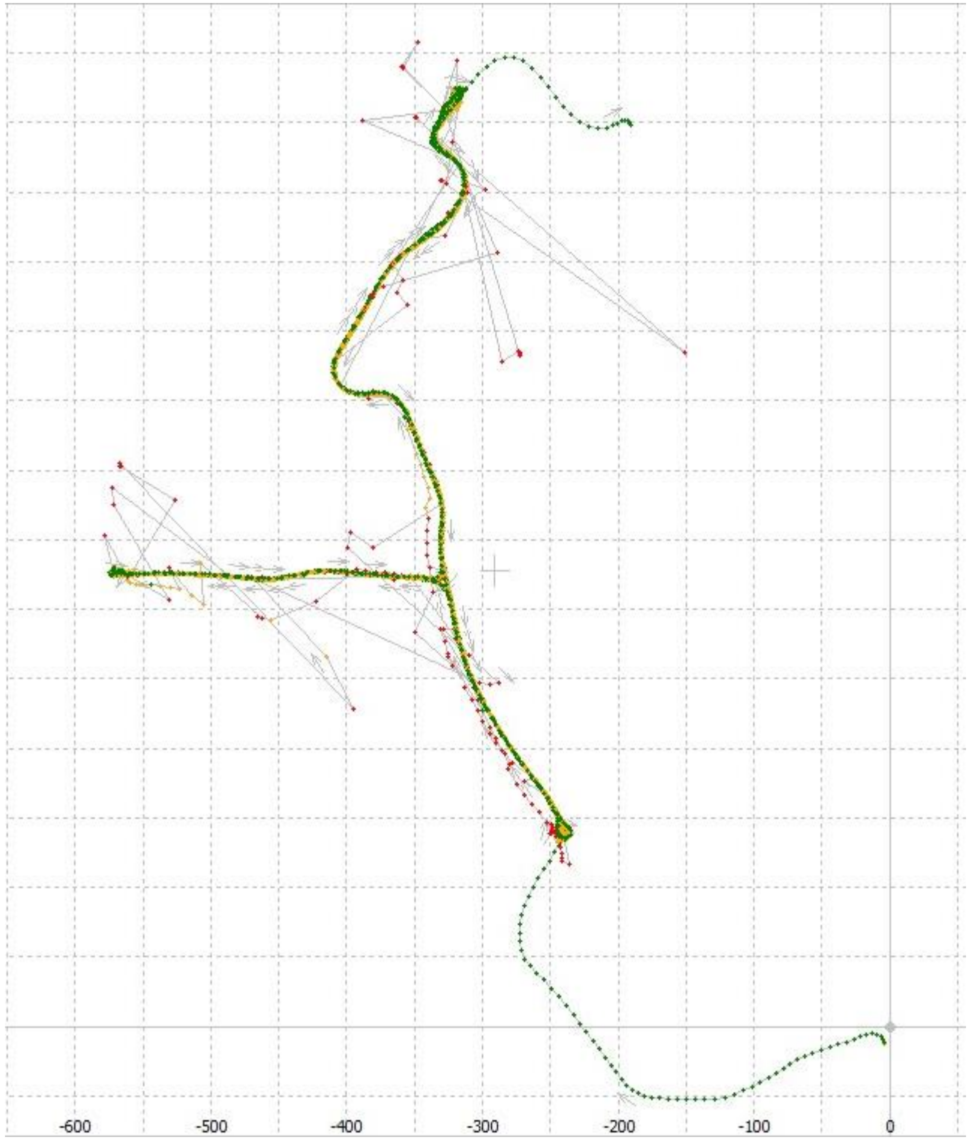


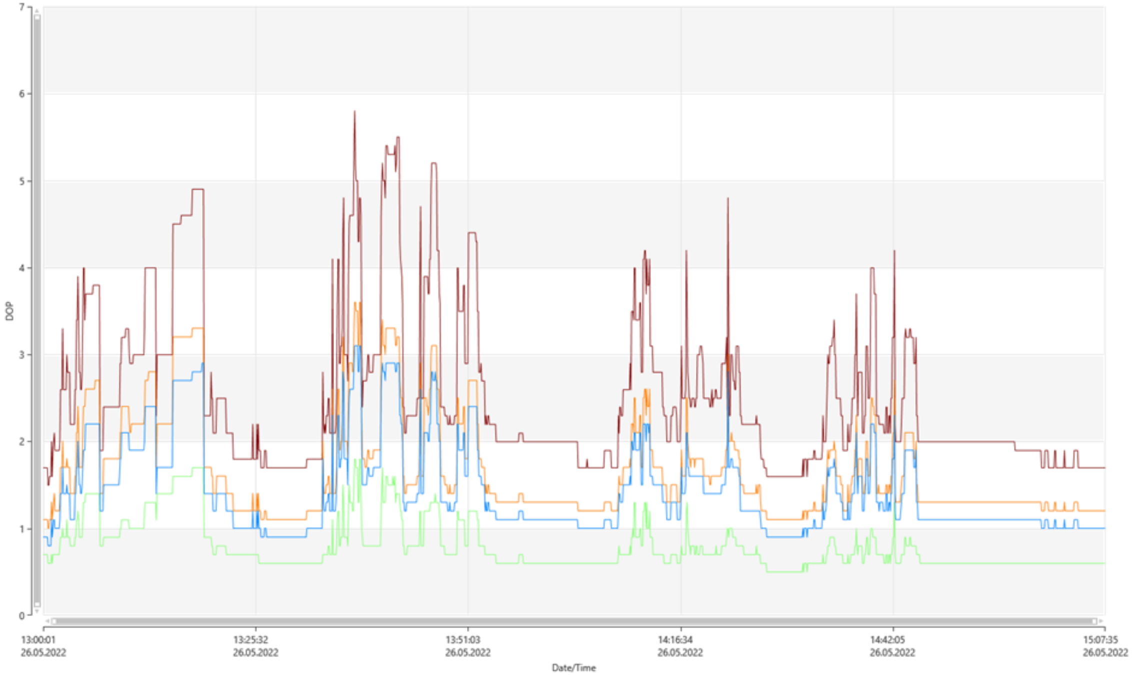
Nominal (H_0)

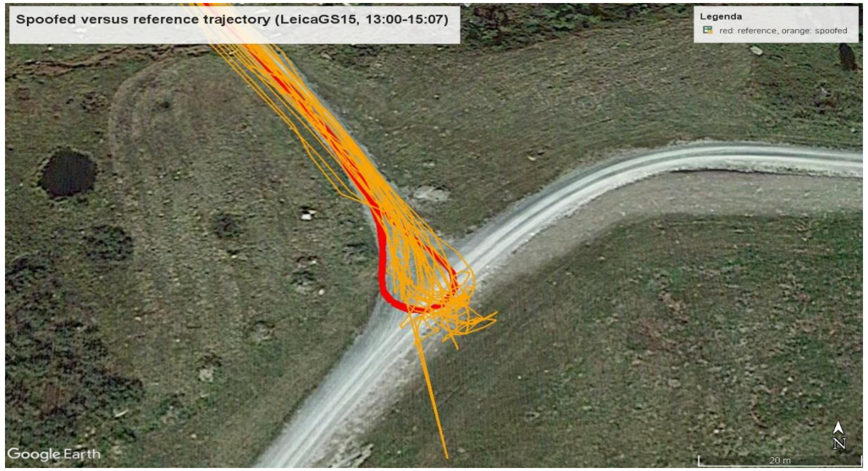
Spoofed (H_1)

Hypothesis testing.

Leica GS15 Performance during Spoofing



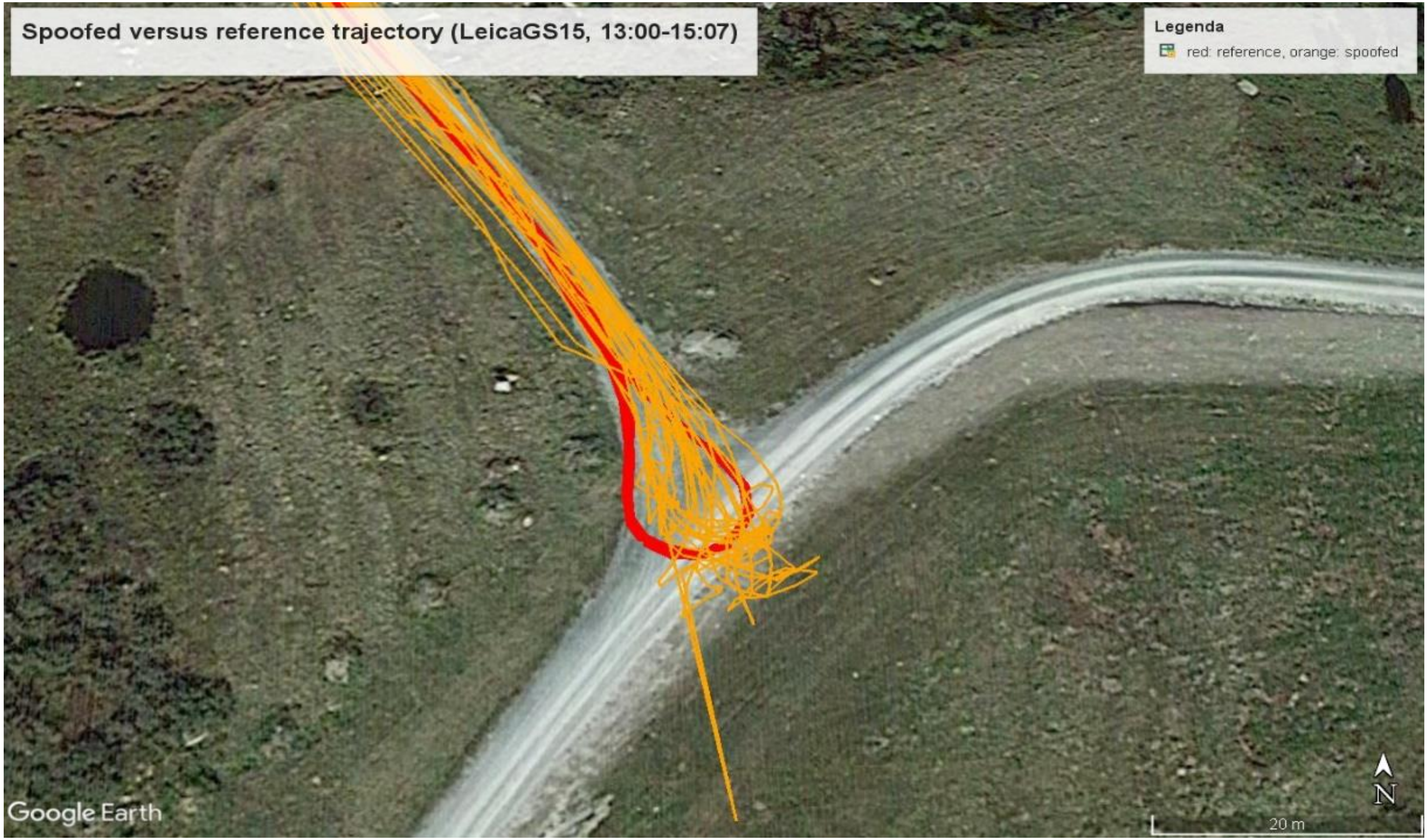




Spoofed versus reference trajectory (LeicaGS15, 13:00-15:07)

Legenda

red: reference, orange: spoofed



Spoofed versus reference trajectory (LeicaGS15, 13:00-15:07)

Legenda

red: reference, orange: spoofed

Conclusions

- It is required to cGNSS jamming and spoofing present **a new threat to critical infrastructure**.
- GNSS jamming causes a loss of GNSS lock for the receiver and the inability to regain the lock.
- Attack costs are low (from 10-300 EUR).
- Check the accuracy and quality of GNSS signals in real-time.
- It is advisable to strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.
- CORS networks could play a crucial role – system should detect wide-range jamming or spoofing or can be used for attacker localization.

Thank you for your attention!

From the CAT STEVENS & MR. BIG – Wild World:
“… take good care
I hope you make a lot of nice friends out there.
But just remember there’s a lot of bad and beware,
beware.”

University
of Ljubljana
Faculty
of Civil and Geodetic
Engineering

Contact

University of Ljubljana
Faculty of Civil and Geodetic Engineering
Jamova cesta 2, SI-1000 Ljubljana, Slovenia

Polona Pavlovčič Prešeren: polona.pavlovcic-preseren@fgg.uni-lj.si