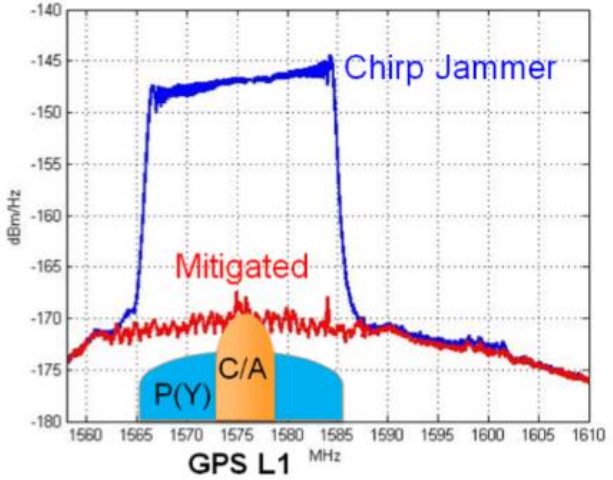
Assured GNSS
Attacks and Countermeasures

Stefan Söderholm

23 October 2023

Outline

Septentrio



Jamming

Tesla Model S and Model 3 vulnerable to GNSS spoofing attacks

June 28, 2019 - By GPS World Staff

Est. reading time: 5 minutes

Autopilot Navigation Steers Car off Road, Research from Regulus Cyber Shows

Tesla Model 3. (Photo: Tesla)

The Tesla Model S and Model 3 — electric cars built for speed and safety — are vulnerable to cyberattacks aimed at their navigation systems, according to recent

Spoofing

Test campaign

Septentrio

Assured PNT is key for our customers

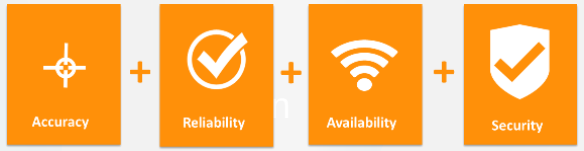
@ Interleuvenlaan Heverlee

Experts in Localization technology

APPLICATION KNOW HOW

RELIABLE & ACCURATE GPS/GNSS POSITIONING

YOUR OEM PARTNER



Autonomous Vehicles *Marine* *Construction & Mining* *UAV* *Reference Networks*

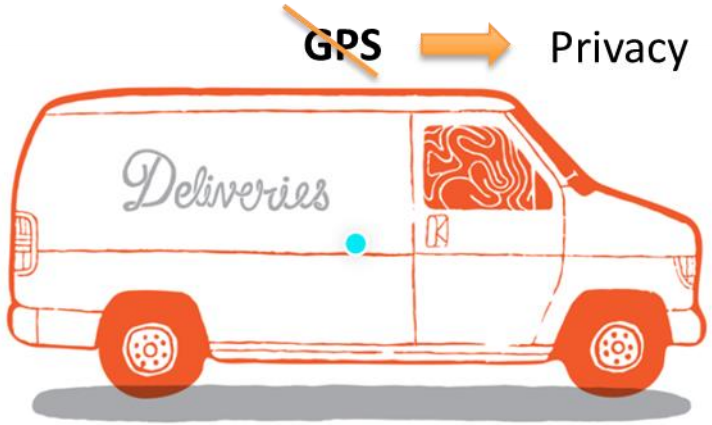
Modules **Boards** **Housed receivers** **Smart antenna** **Scientific Receivers**

septentrio

Jamming

Jamming

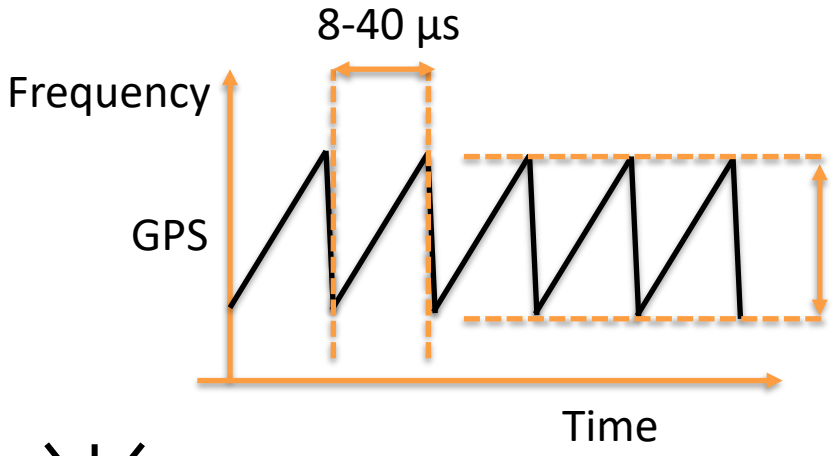
- Jamming, to jam = ”squeeze or pack tightly into a specified space”
- Jamming is always malicious and intentional
- The interfering signal does not contain any information
- Cause GNSS receivers to stop working or suffer in performance by adding an interfering signal to the GNSS frequency band that saturates the radio frontend.



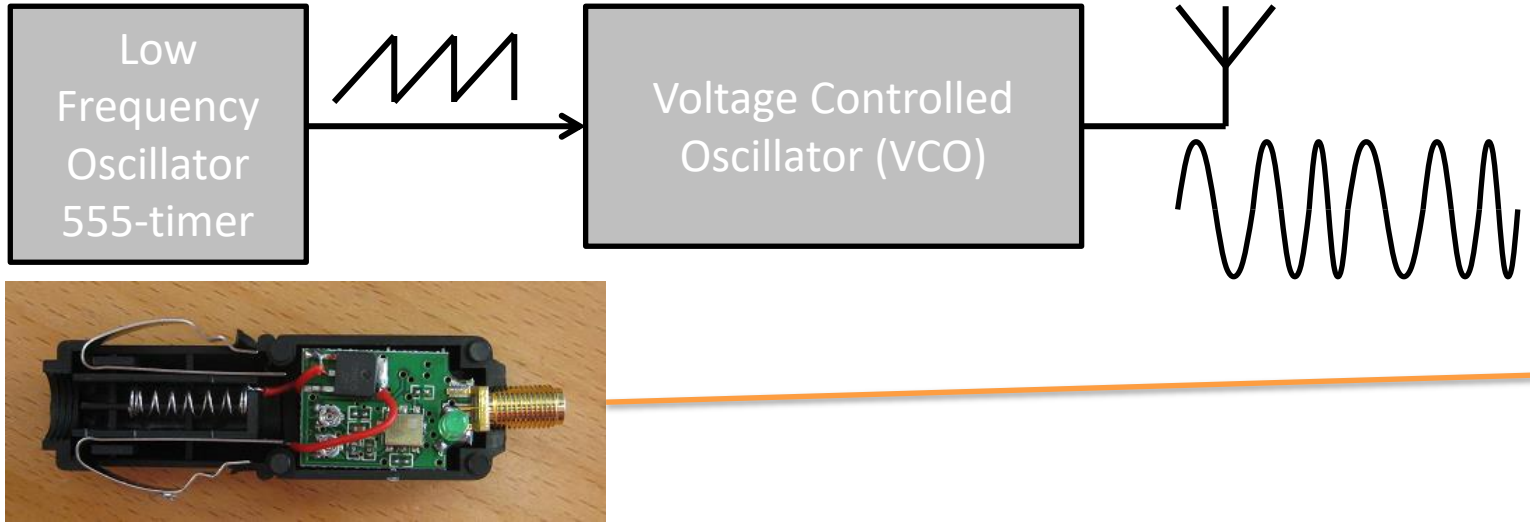
- Jammers is often referred to as PPD’s (Personal Privacy Devices)
- Especially in US it was considered OK to protect your own privacy by blocking any GPS receiver your employee might have installed in your car.

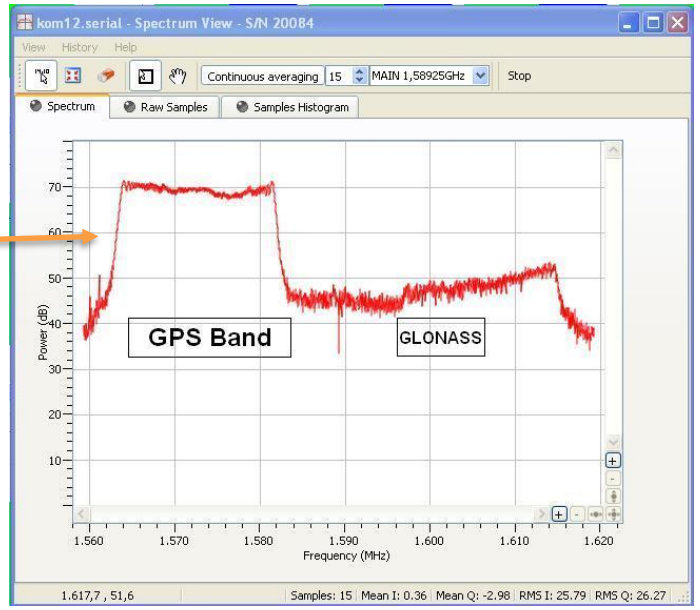
Chirp Jammers

- Sinewave with Changing Frequency
- Wipes out GPS band(s)



100 mW





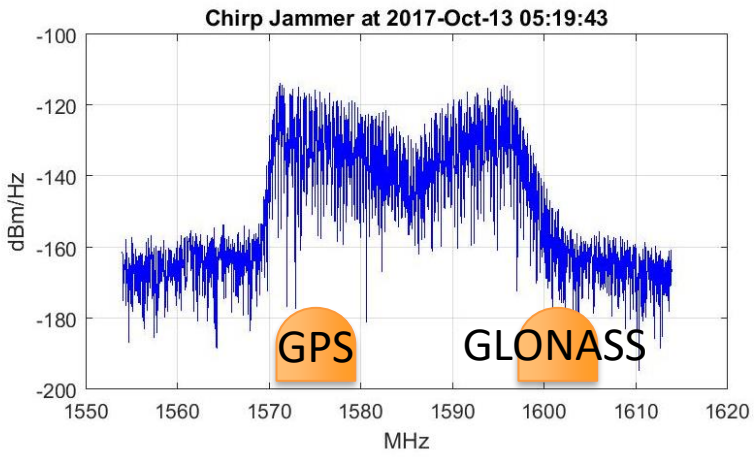
- 10 mW over ~20 MHz => 63 dBm/Hz

2.5 km

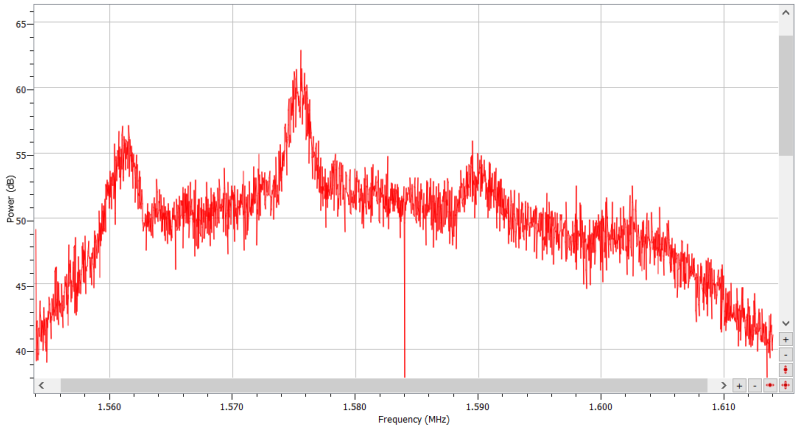
Noise Floor: -172 dBm/Hz

septentrio

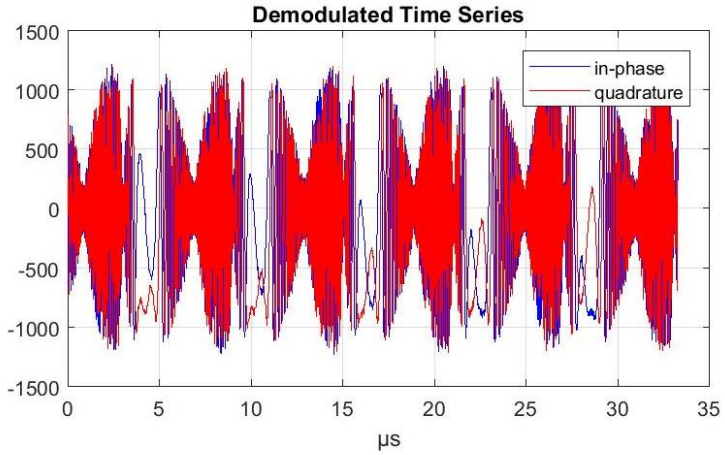
Jamming Mitigation: Concept



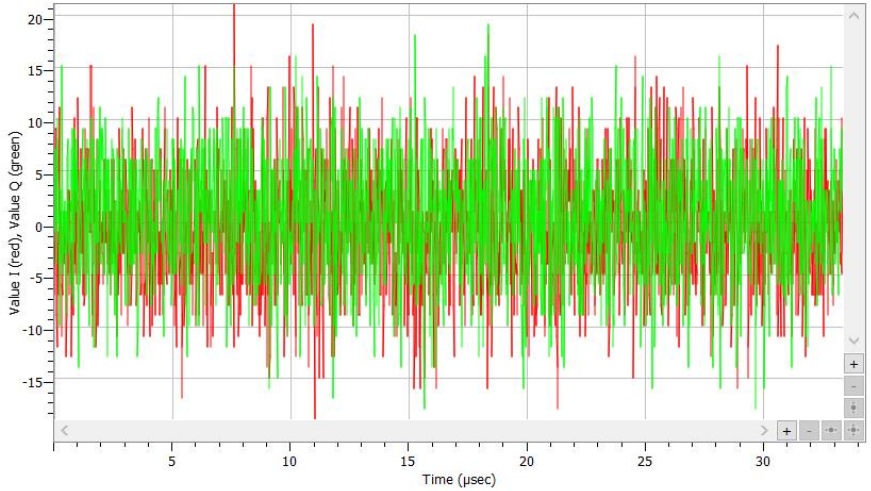
- General Concept:
  - GPS normally dominated by thermal noise
  - And GPS signals also look like noise



Normal GPS Spectrum



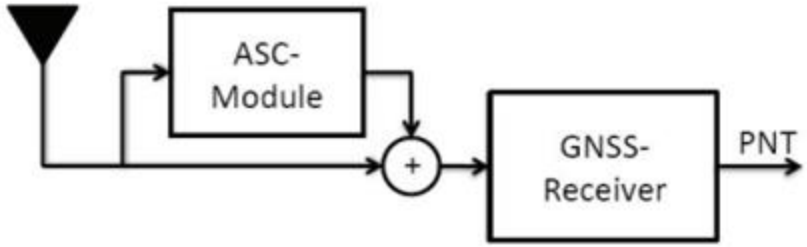
→ So, remove anything which doesn't look like noise



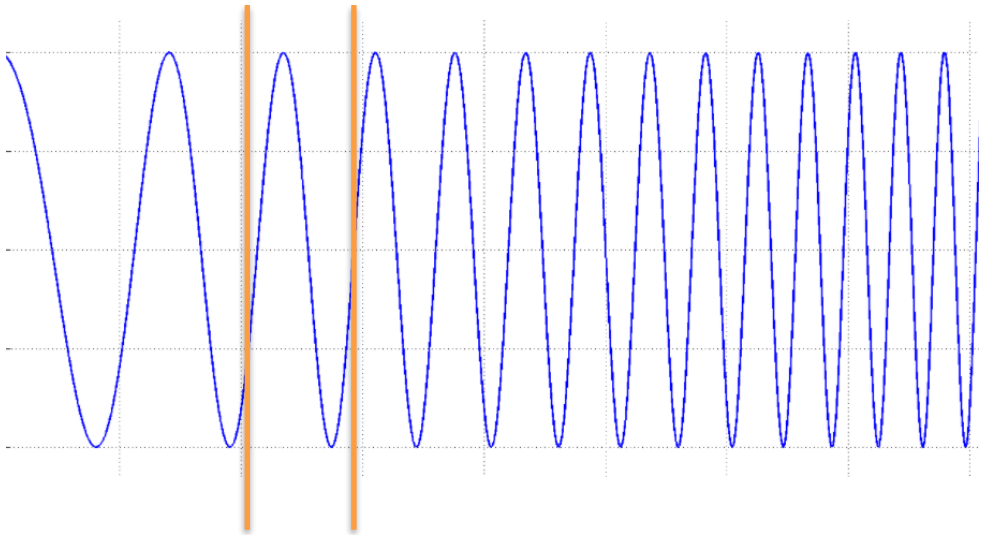
Mitigation Techniques : Chirp Jammers

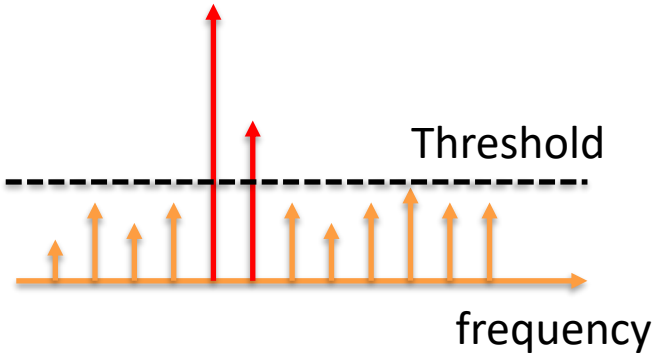
- Method 1: Mimick the signal, and subtract
  - Parameter estimation: frequency-range, chirp-rate, phase
  - Problem: can't deal well with reflections

Active Signal Cancellation



- Method 2: FFT – set peaks to zero - IFFT
  - = FDAF: Frequency Domain Adaptive Filter

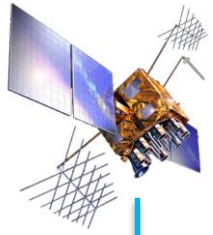


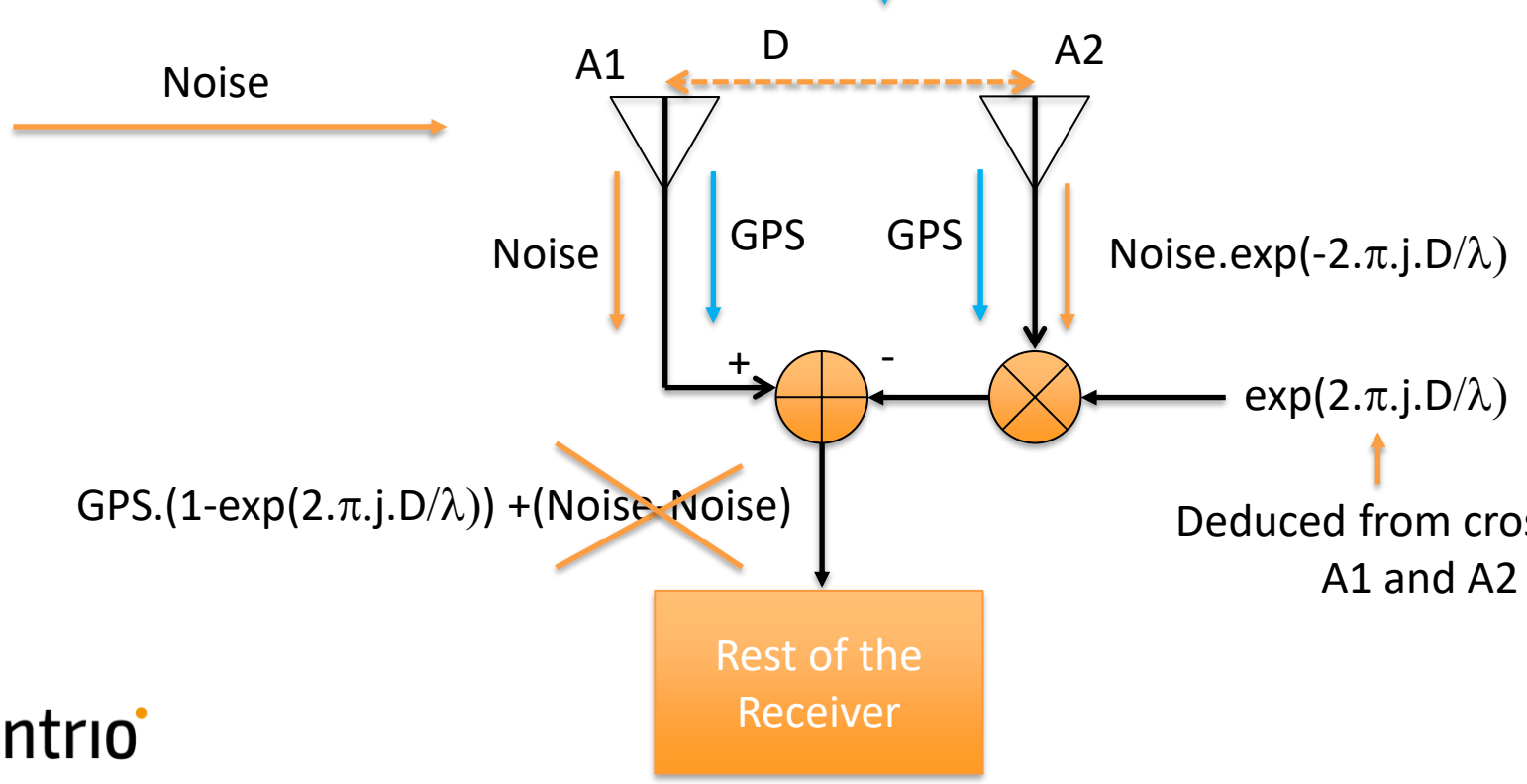


septentrio

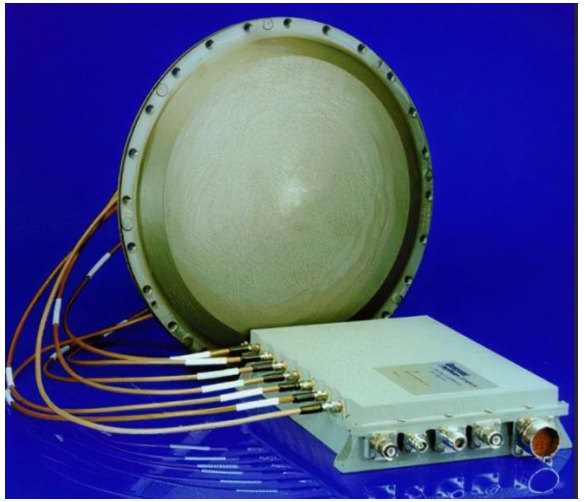
Military Grade Anti-Jamming: Beam Forming

- Random Noise at Main Lobes
  - Structure cannot be exploited
- Exploit Geometry
- Multiple Antenna Elements





- Typically uses 4 to 7 antenna elements
- CRPA: Controlled Radiation Pattern Antenna



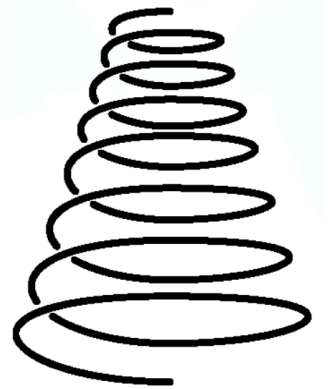
Deduced from cross-correlation A1 and A2 signal

septentrio

Spoofing

Spoofing

- Spoofing, to spoof = “imitate something, hoax or trick someone”
- Spoofing is always malicious and intentional.
- The interfering signal tries to generate and transmit false GNSS signals.
- Fool a receiver to think it is at different position than it really is.

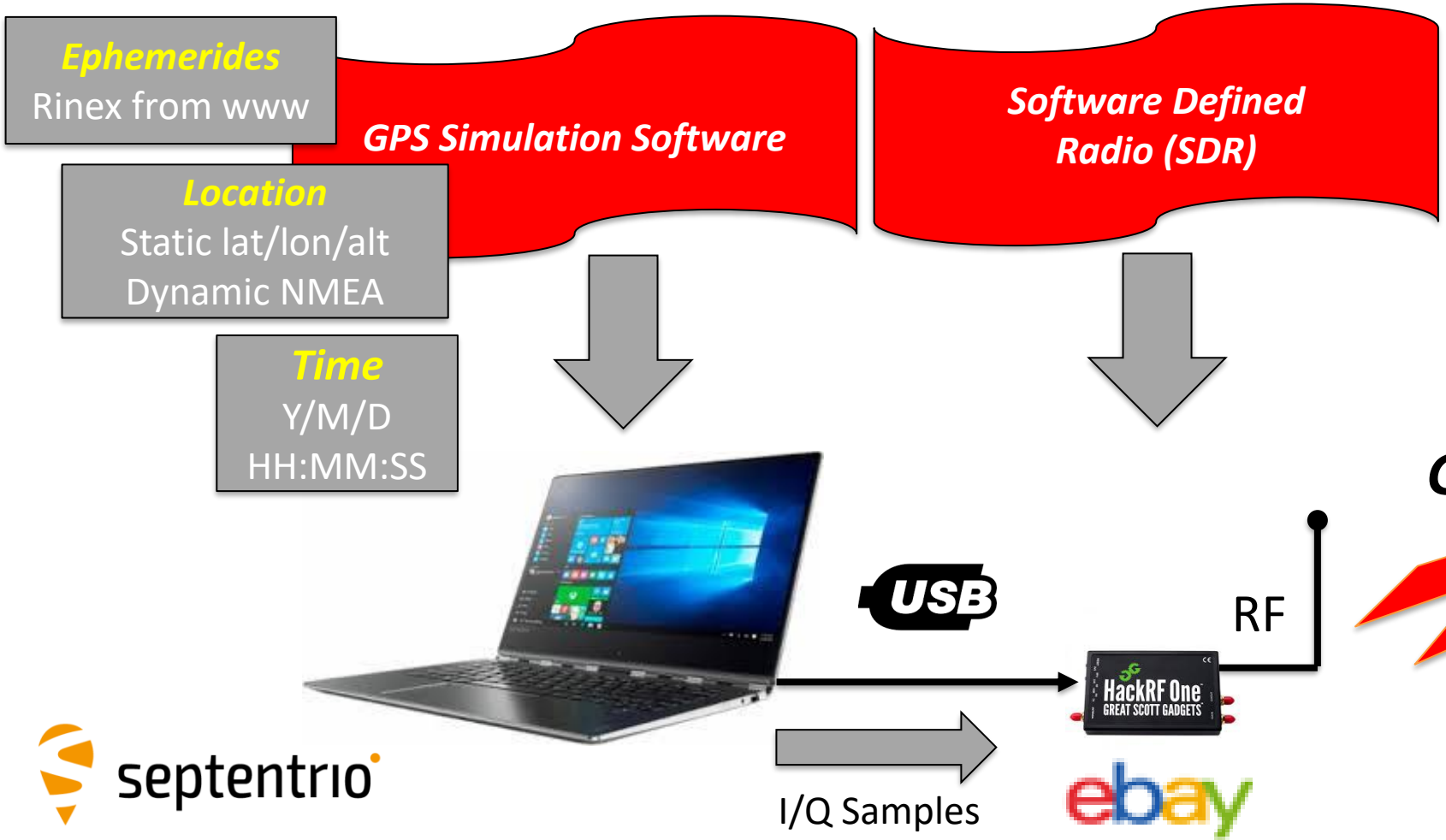


Pizza Time!

septentrio

Budget Spoofer

- A spoofer need to :
  - Generate true GNSS signals including data, modulation and timing.
  - Maintain time synchronization close to true GNSS time.
  - Adapt the signal power levels to match those of the true signals.



HackRF One 1-6GHz Open Source Software Defined Radio Platform…

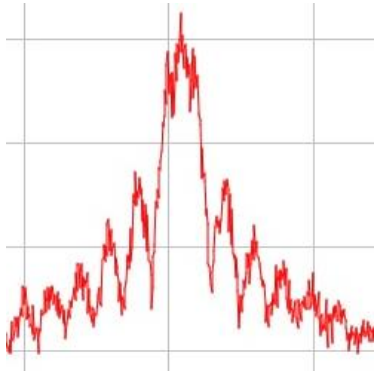
$139.81

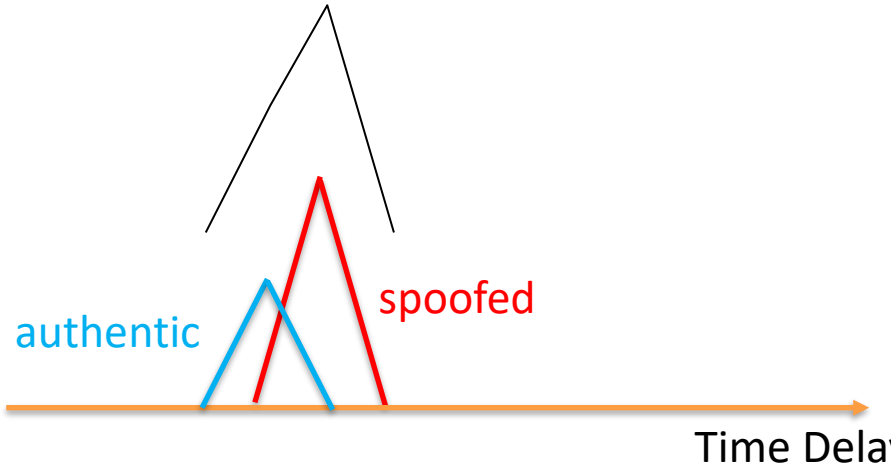
+$5.00 shipping

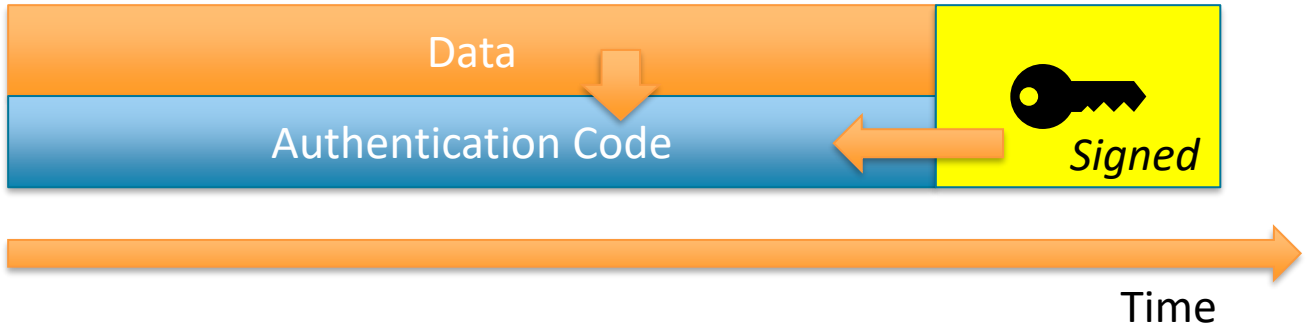
septentrio

Detection of Spoofing

- Detect excessive power
  - But can also come from high-gain antenna…
- Detect correlation profile deformation
  - But can also come from multipath…
- Detect divergence
  - But can also come from ionospheric scintillation…
- Detect wrong angle-of-arrival (2 antenna-receivers)
  - But can be reflection….
- Navigation data authentication



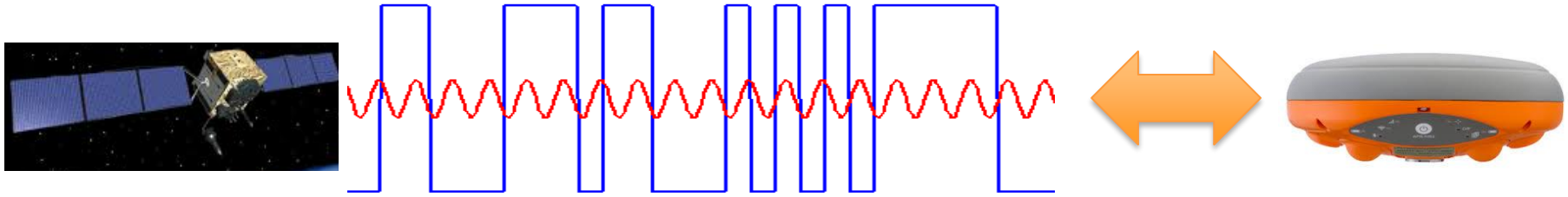




GALILEO OSNMA

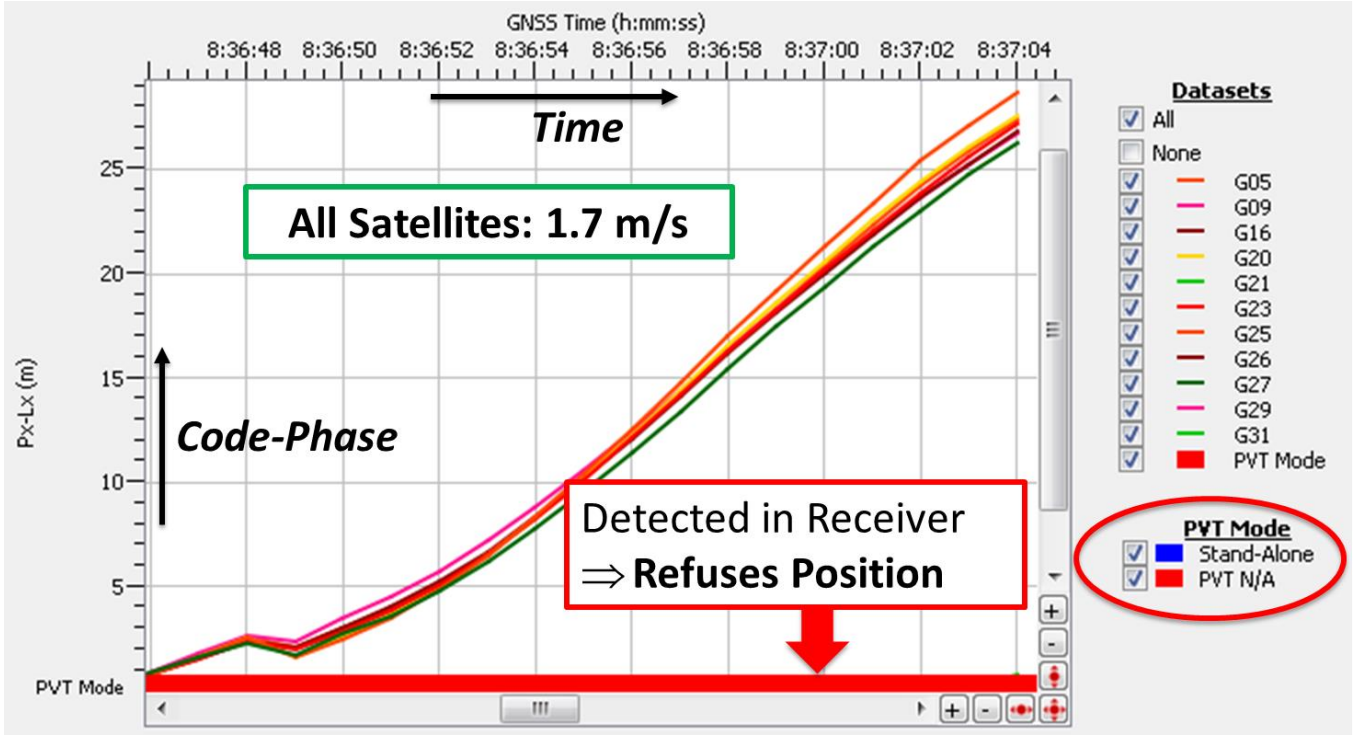
septentrio

Code-Carrier Divergence

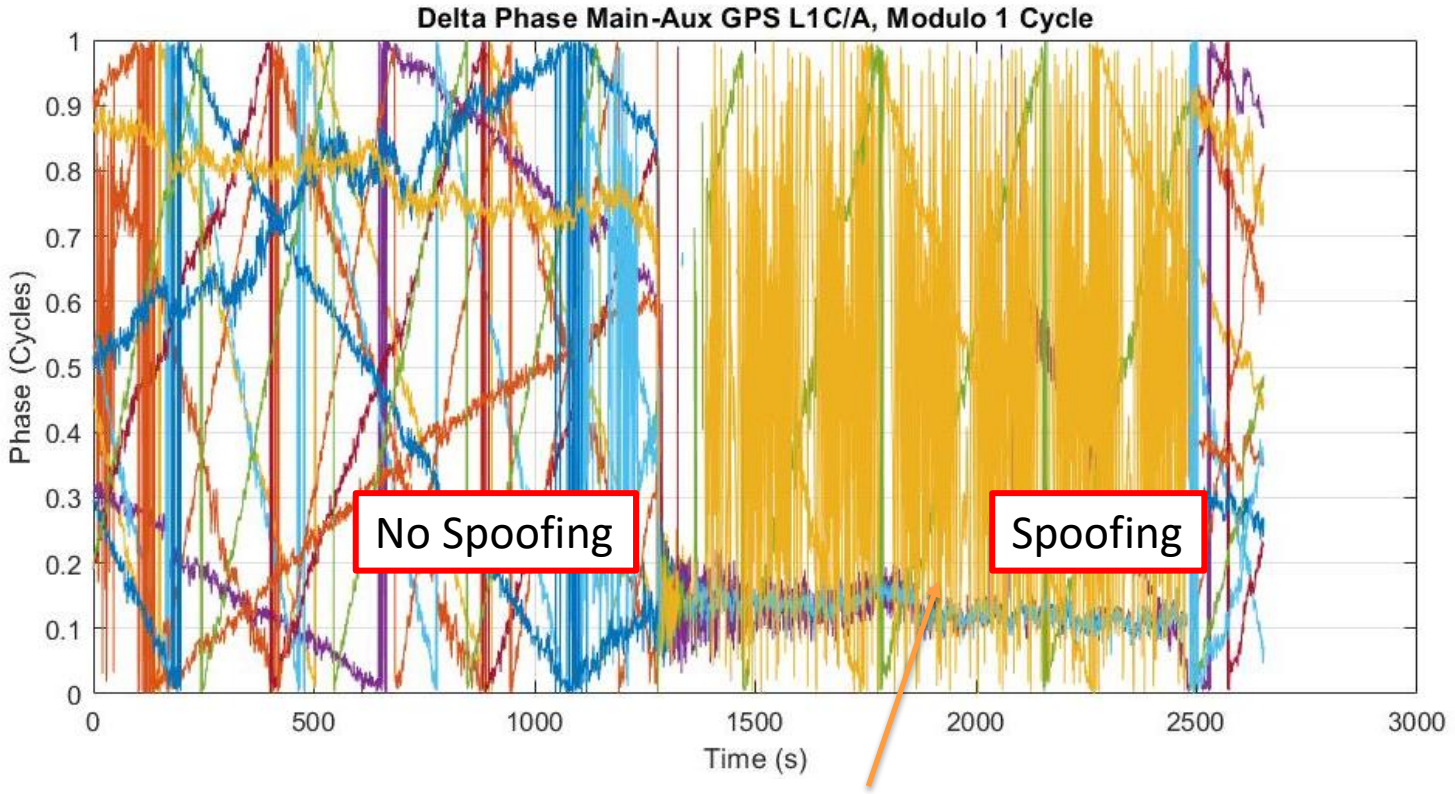


- Both Represent Range → Equal
- Only Slow Divergence Expected
  - Ionosphere, Phase Wind Up

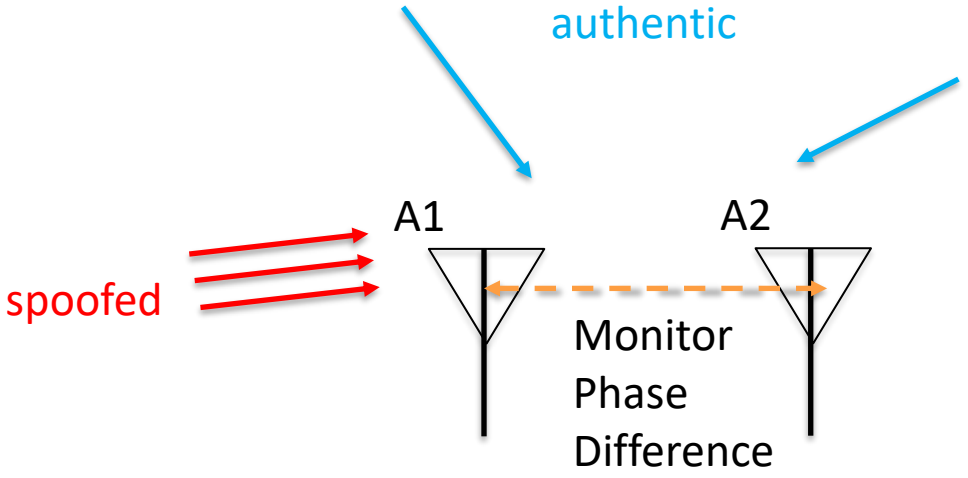
- Most SDR:s → Huge Code-carrier Divergence



Wrong Angle of arrival



Single Difference Phase

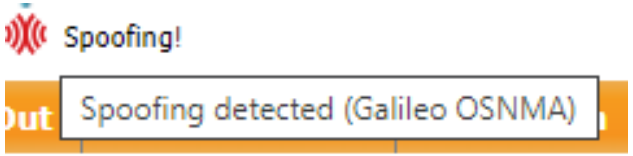


- A spoofer transmits all signals from the same location => Same angle of arrival
- Satellite signals arrive from different angles
- Spoofged measurement from two antennas will not match

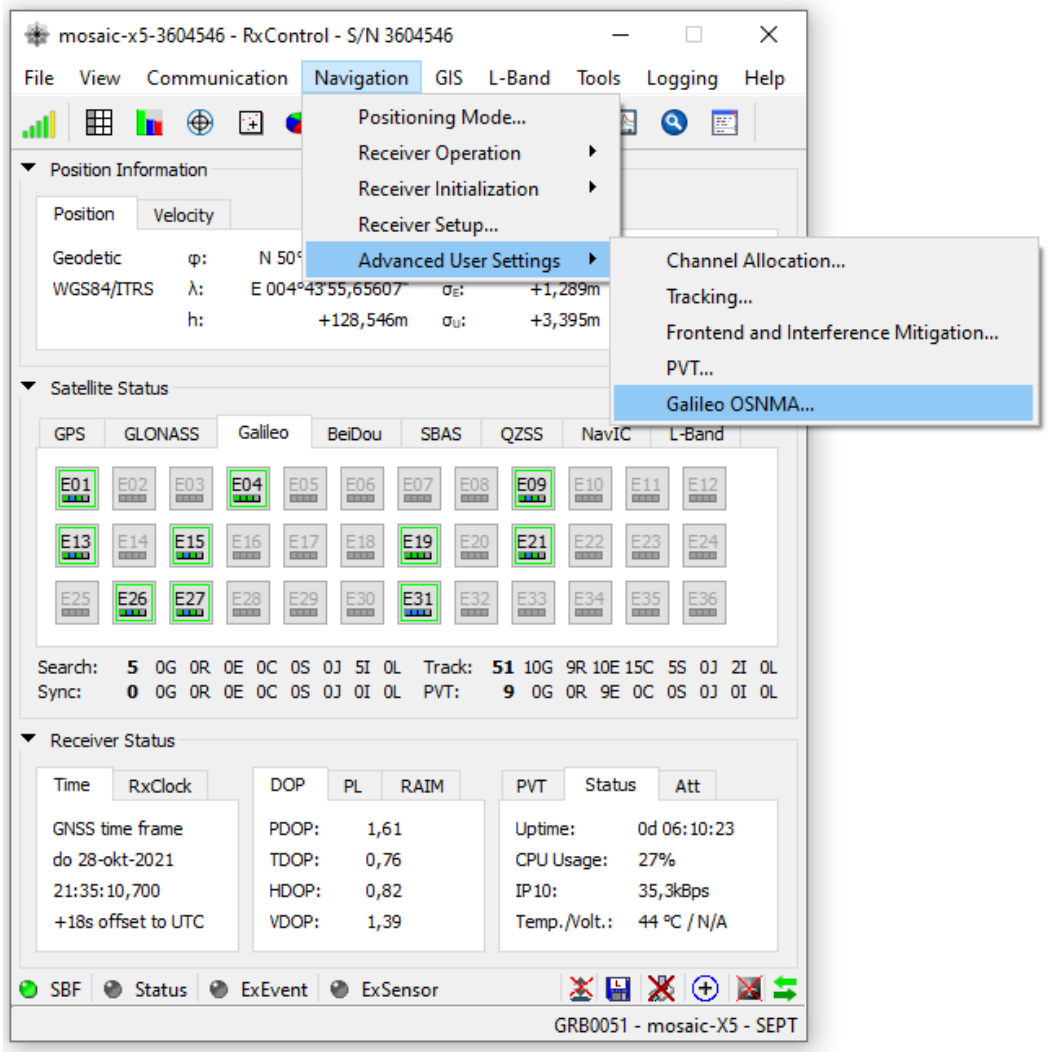
GALILEO Open Service Navigation Message Authentication

- First Cryptographic Service
- Now running on MOSAIC module

Accurate:
Authentication wrong → Spoofing!
Coherent Attack Protection



Latency: 30 seconds
NTP-Dependency



Test Campaign

The Norway Jamming/Spoofing test

- **Organizers:** Norwegian Governmental Organizations, coordination via Testnor

Statens vegvesen
Norwegian Public Roads Administration

Norwegian Communications Authority

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

Justervesenet

Norsk Romsenter
Norwegian Space Agency

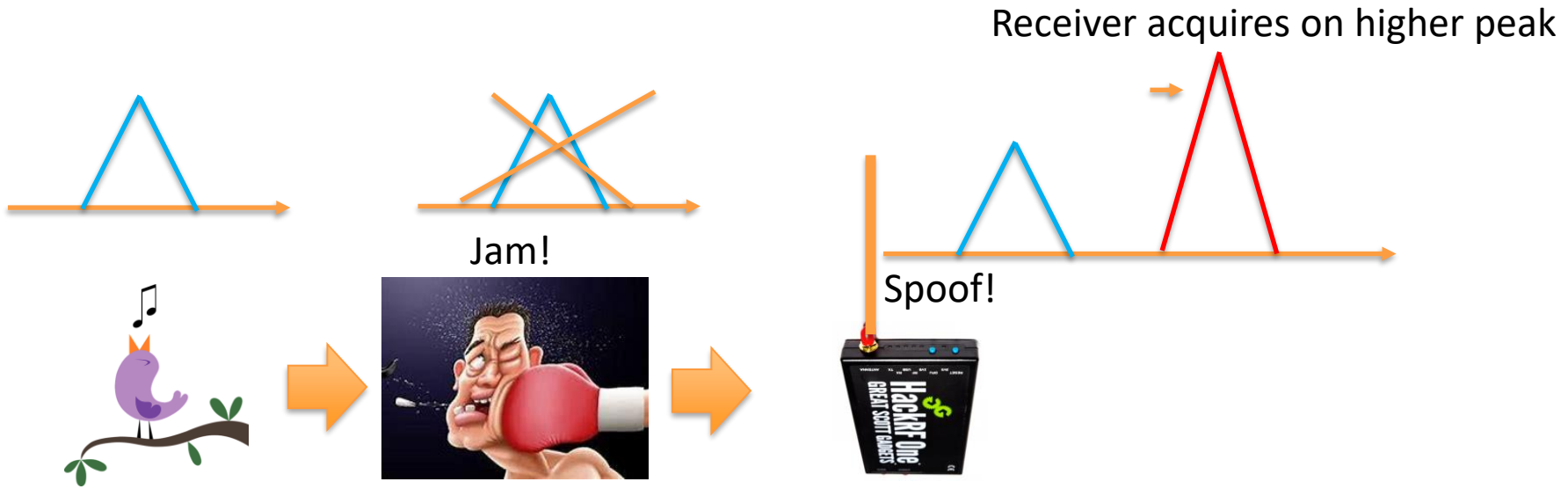
- **When:** September 18th till the 20th 2023

- **Where:** Andøya, Norway

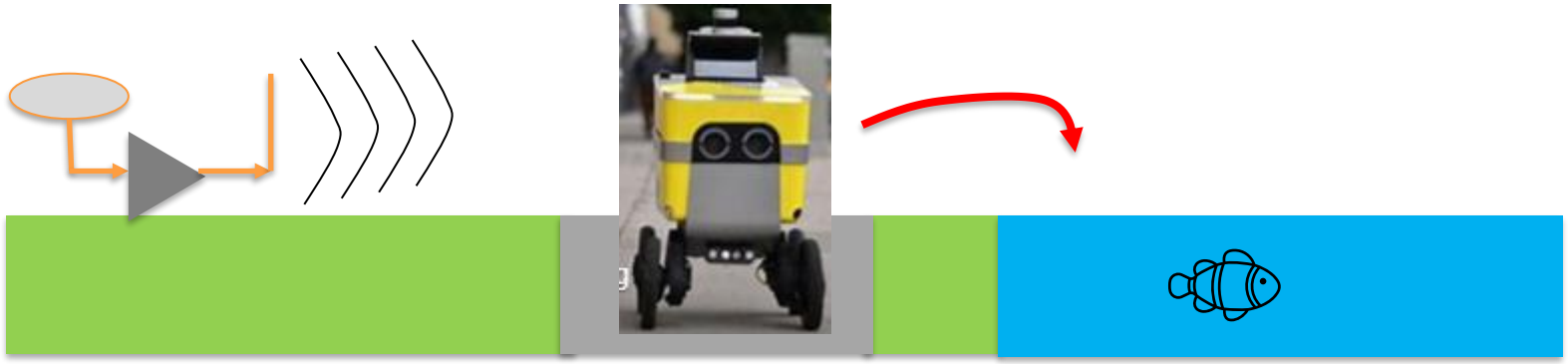
- **Who attended:** 300 participants from various industries

septentrio

Attack Type: Non-Coherent Attack

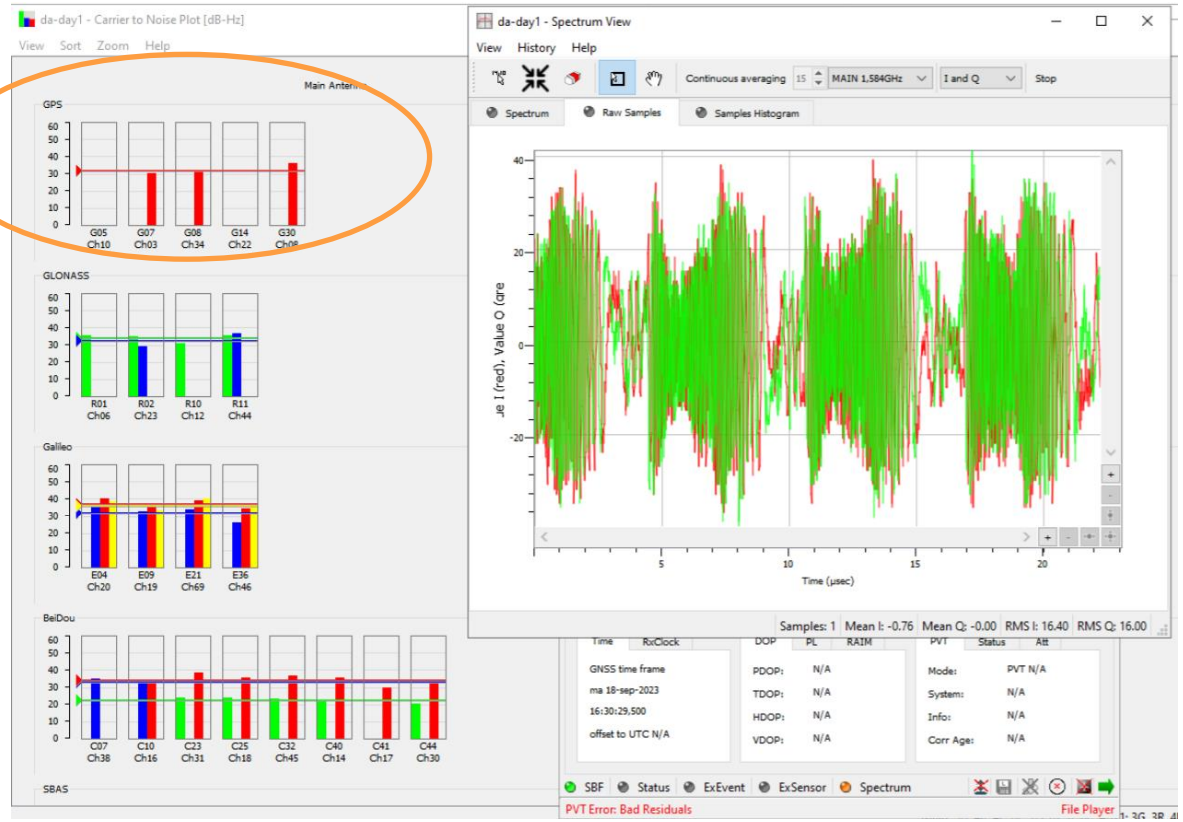


- Introduce jump of position or time
- Use jamming to obfuscate attack

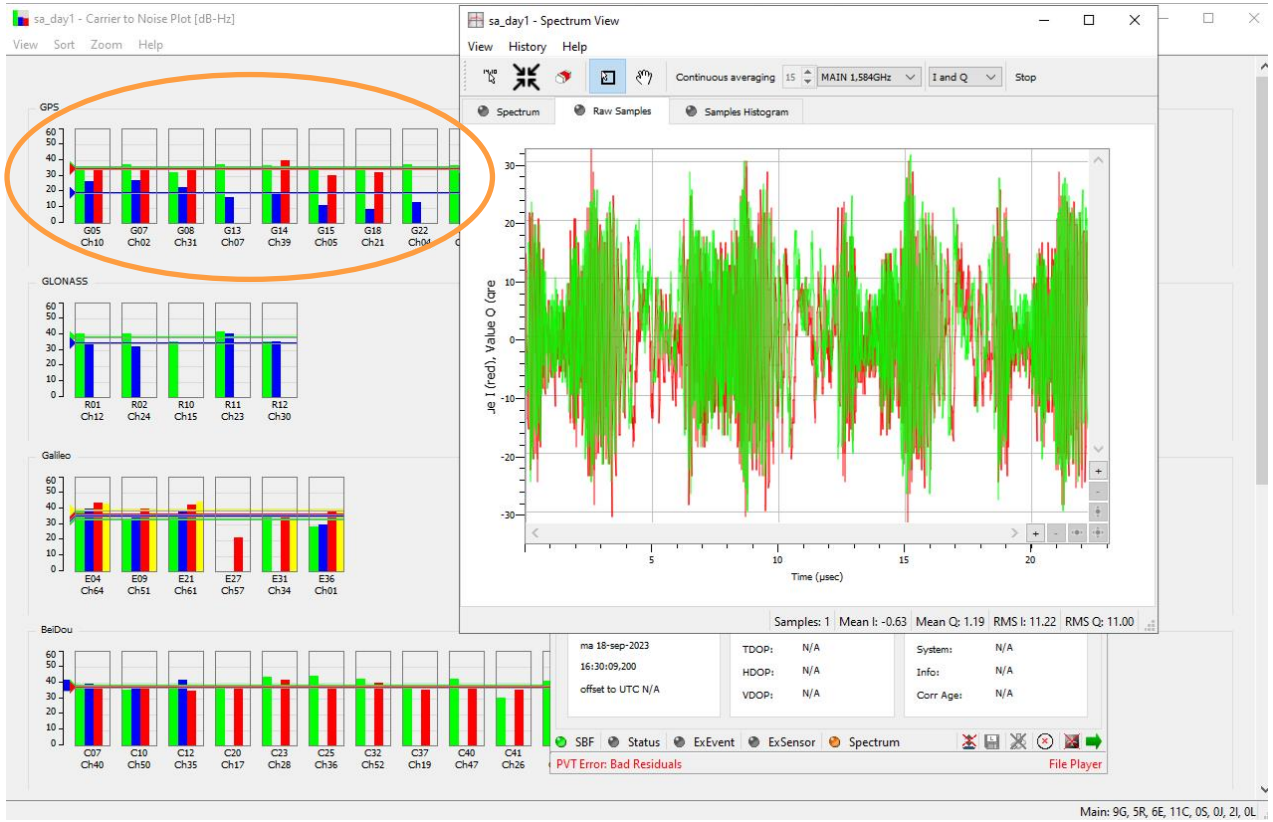


Chirp Jammer: WIMU in Action

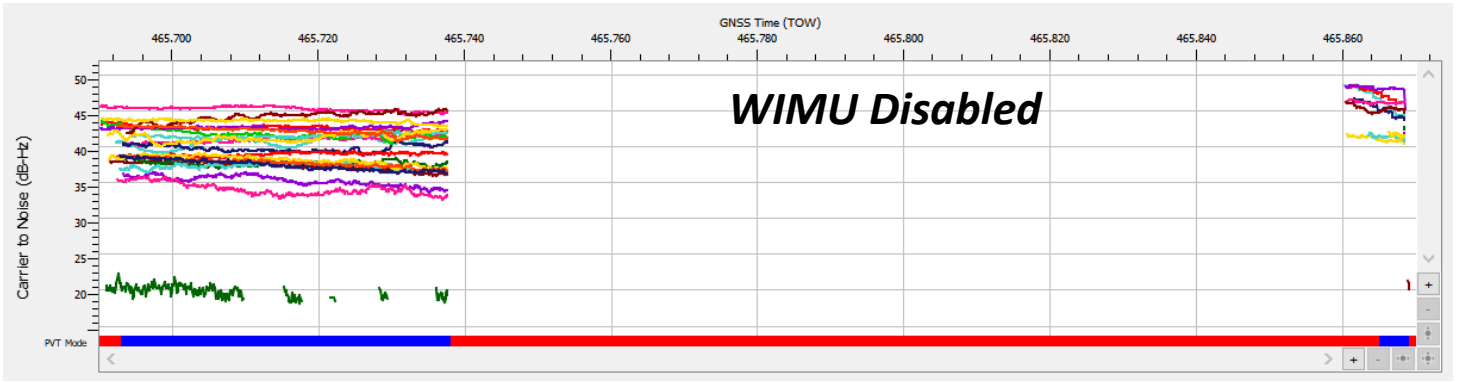
Receiver 1: WIMU Off → L1 mostly gone



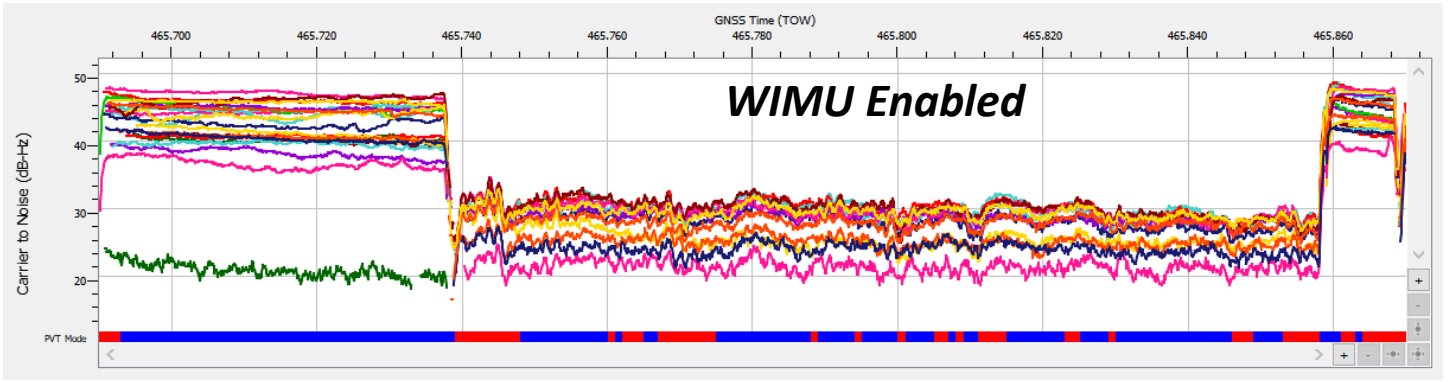
Receiver 2: WIMU On → L1 is back!



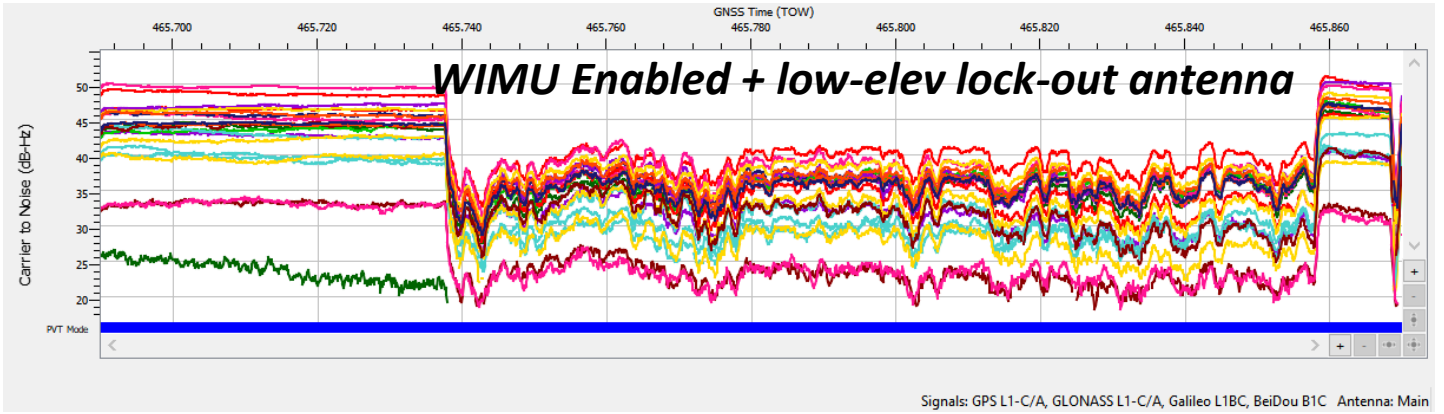
Response to Multi-frequency Chirp Jammer Attack



Receiver:
Mosaic-mini
Dual antenna config
Hi-Target antenna



Receiver:
Mosaic-mini
Single antenna config
Hi-Target antenna

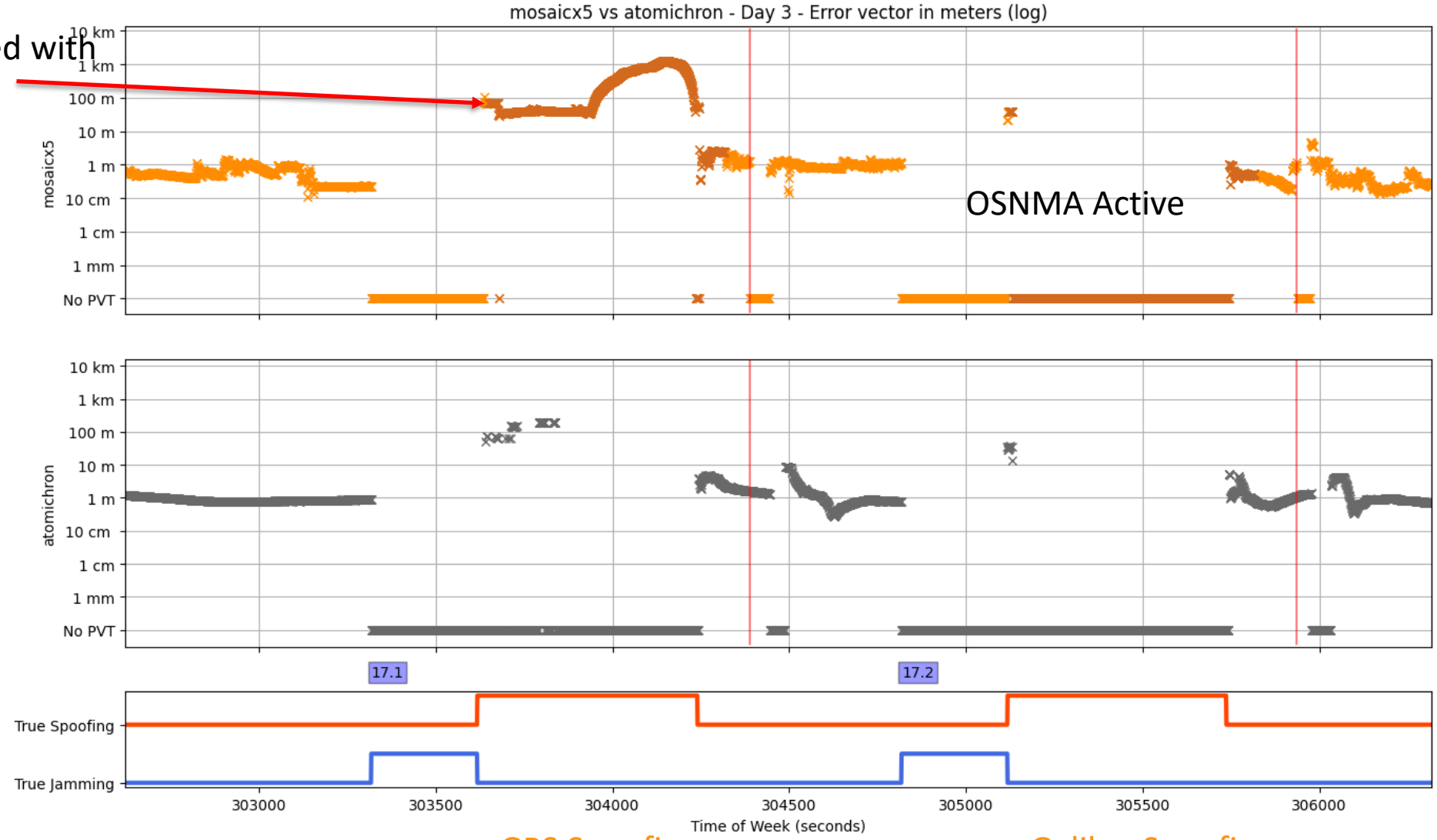


Receiver:
Mosaic-T
Single antenna config
AJ977XF antenna

septentrio

OSNMA and Atomichron

Position affected with only OSNMA



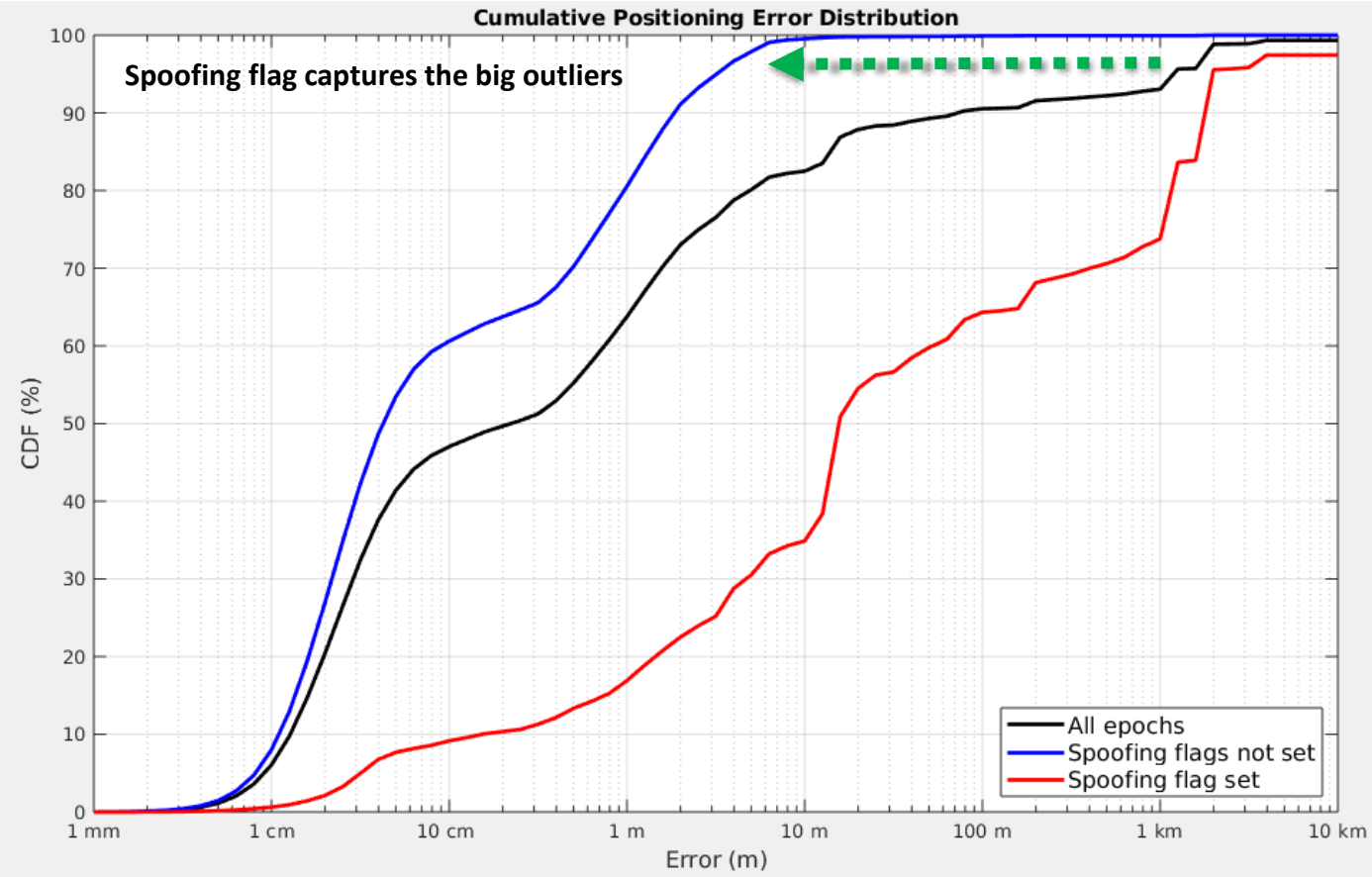
GPS Spoofing

Galileo Spoofing

Did we detect the spoofing?

Undetected spoofing epochs with an error > 10m

Receiver	Total (%)
Competitor 1	**67%**
Competitor 2	**45%**
Competitor 3	**26%**
Septentrio	**<1%**



Spoofing flags is set for all big outliers!

septentrio

septentrio

EMEA (HQ)

Greenhill Campus
Interleuvenlaan 15i,
3001 Leuven, **Belgium**

septentrio.com

Americas

Los Angeles, **USA**

sales@septentrio.com

Asia-Pacific

Melbourne, **Australia**
Shanghai, **China**
Yokohama, **Japan**