Interferentie en Spoofing Tegenmaatregelen in Septentrio Ontvangers

W. De Wilde, G. Cuypers & T. Willems

Haarlem, 31 Januari 2018

Outline

- Septentrio
- Interference and Jamming
  - Countermeasures
  - Experiment with Chirp Jammer
- Spoofing
  - Budget Spoofers
  - Countermeasures in Septentrio Receivers
  - Spoofing Robustness Test Results
- Conclusions

Septentrio

Septentrio

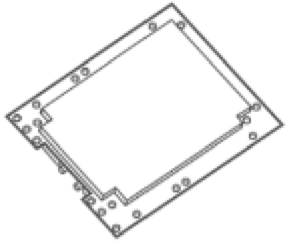
- Founded in 2000 as IMEC spin-off
- Septentrio NV (Leuven HQ), Septentrio Inc (Los Angeles) & Hong Kong
- International team of 100 people worldwide, 50 in GNSS R&D
- Focus on cm-dm accuracy
- Own hardware and software technology building blocks
- GNSS+inertial hybrid solutions
- Long term strategic partner of the European Space Agency

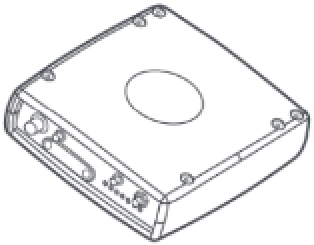
- **We offer high precision GNSS positioning and timing solutions for the most demanding applications**

Septentrio Products

AsteRx

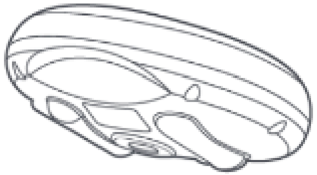
Rover Receivers and OEM boards for **automation and machine control**





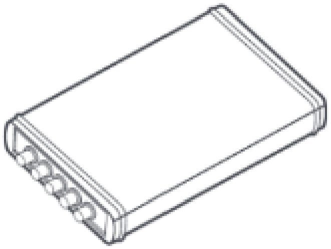
Altus

Smart antennas for **GIS and survey**



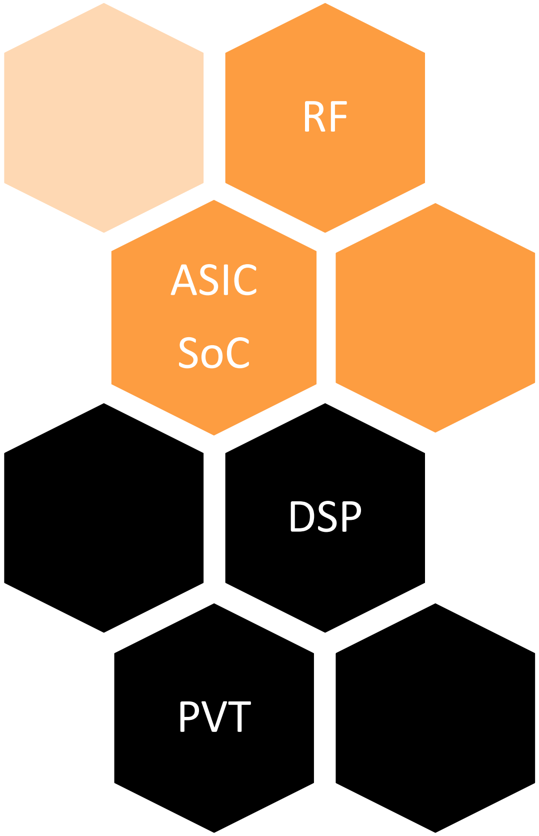
PolaRx

Reference receivers for **science and networks**



septentrio

Septentrio Core Technology



RF Front-end & Clock

- Multi-Frequency Multi-Constellation
- High interference immunity

System-on-chip (SoC) &

Application-specific integrated circuit (ASIC)

- All-in-view multi-frequency multi-constellation
- Fast acquisition
- Built-in interference mitigation (incl. chirp jammer mitigation)

Digital Signal Processing

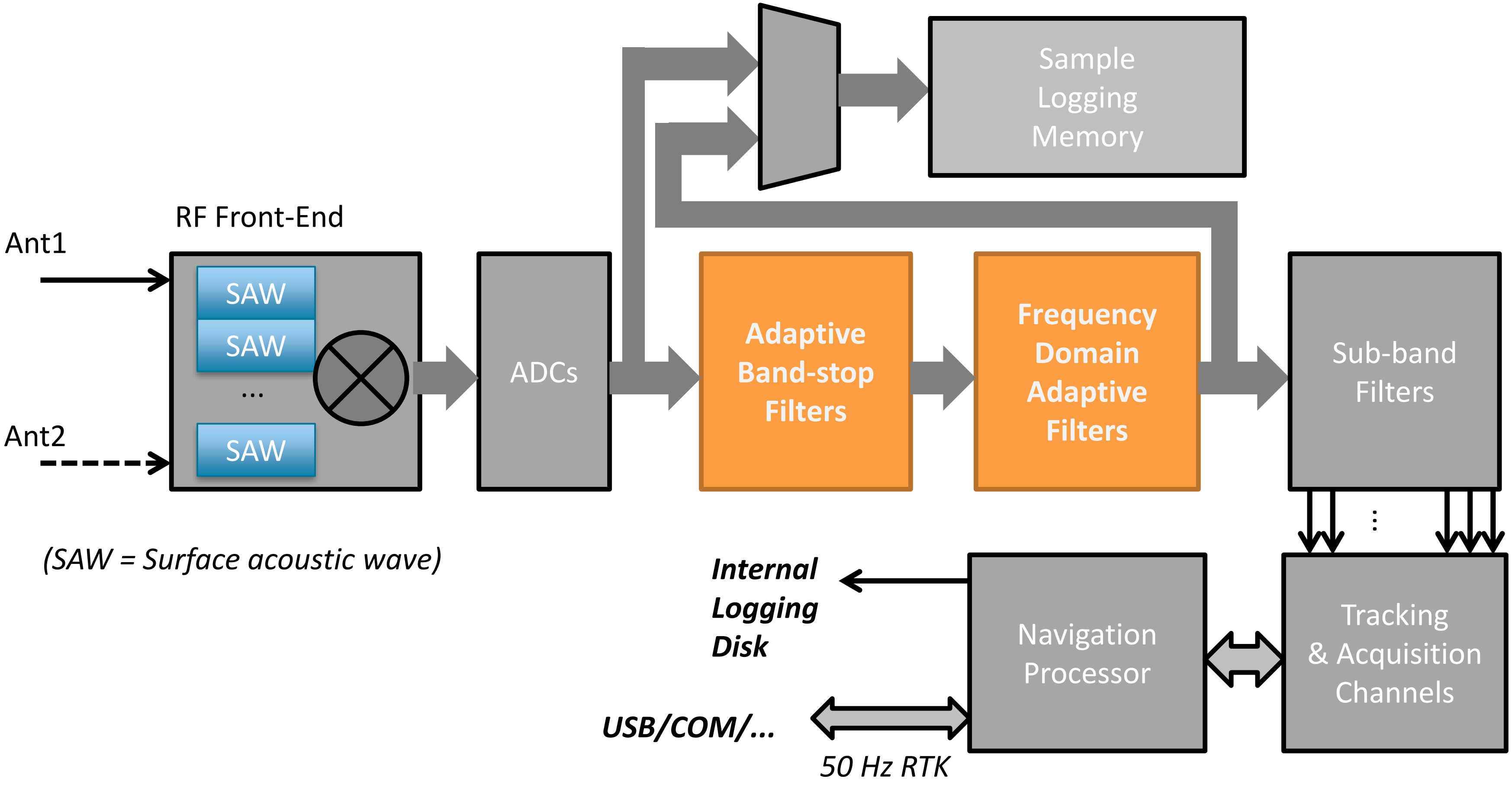
- All signals in space (GPS, Glonass, Galileo, Beidou, QZSS,...)
- Multipath mitigation (wide-band architecture, APME algorithm)
- Very low measurement noise
- Secure GNSS signals and Anti-Spoofing

Position, Velocity & Time **(PVT)**

- Scalable accuracy: sub-meter down to cm
- High availability in challenging environments
- High reliability

Interference & Jamming

Septentrio receivers provide passive and active interference mitigations



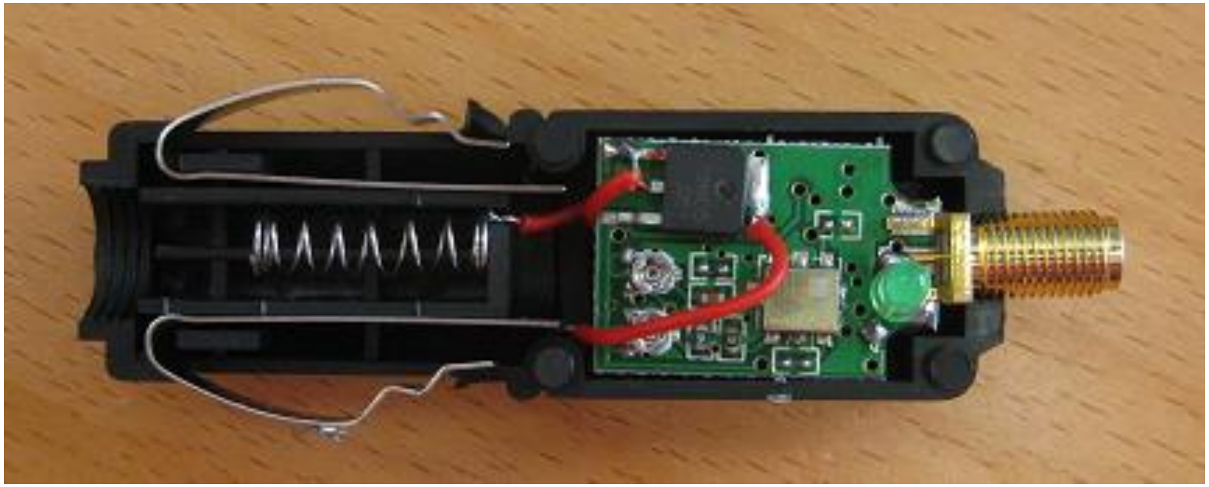
(SAW = Surface acoustic wave)

Interference Mitigation

- Standard feature
- **Narrow band interference mitigation**
  - Adaptive Notch Filters (fully automatic)
  - Multiple notch filters per band
- **Wide band interference mitigation**
  - Adaptive Frequency Domain Filters (fully automatic)
  - Effective for chirp jammers, radar,…
- **Monitoring and Control**
  - Spectrum monitoring
  - Adaptive filters status (manual control possible)
  - Via Graphical User Interface, Web Interface, binary messages
- **Frequency diversity**
  - Independent tracking of L1, L2(C), L5,…

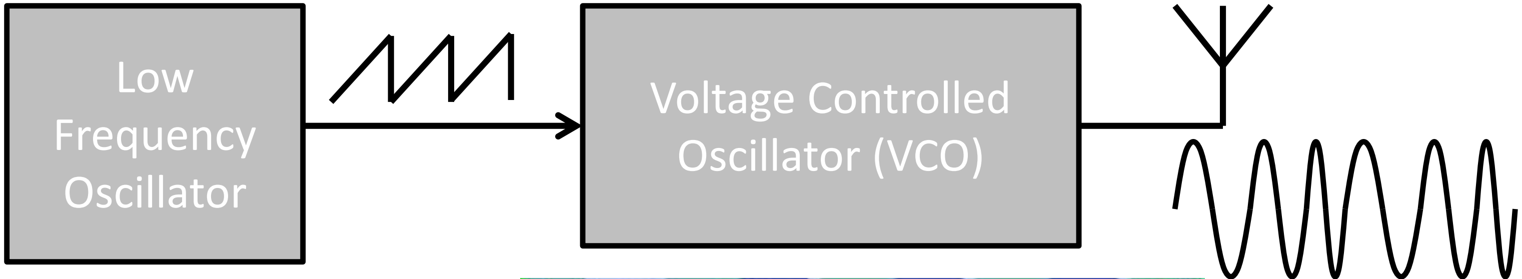
Jammers

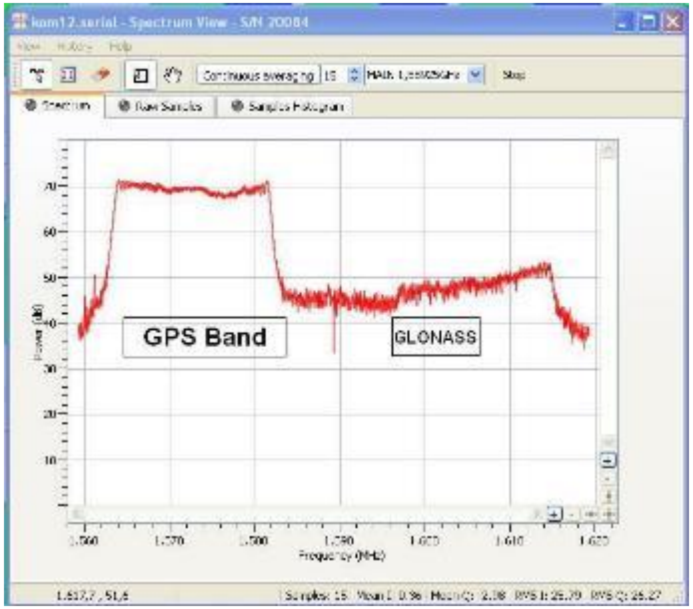
- Many flavours: 20€ - 300€
- Typical construction:
  - Powered from Cigarette Lighter (12V)
  - 10 mW Output Power
  - Chirp Signal in 1560-1600 MHz range
  - Cheap Analog Circuit



Chirp Signal

- Sinewave with Changing Frequency
- “Wipes out” GPS L1 band





kom12.serial - Spectrum View - S/N 20084

Continuous averaging 15 MAIN 1,5[illegible]GHz

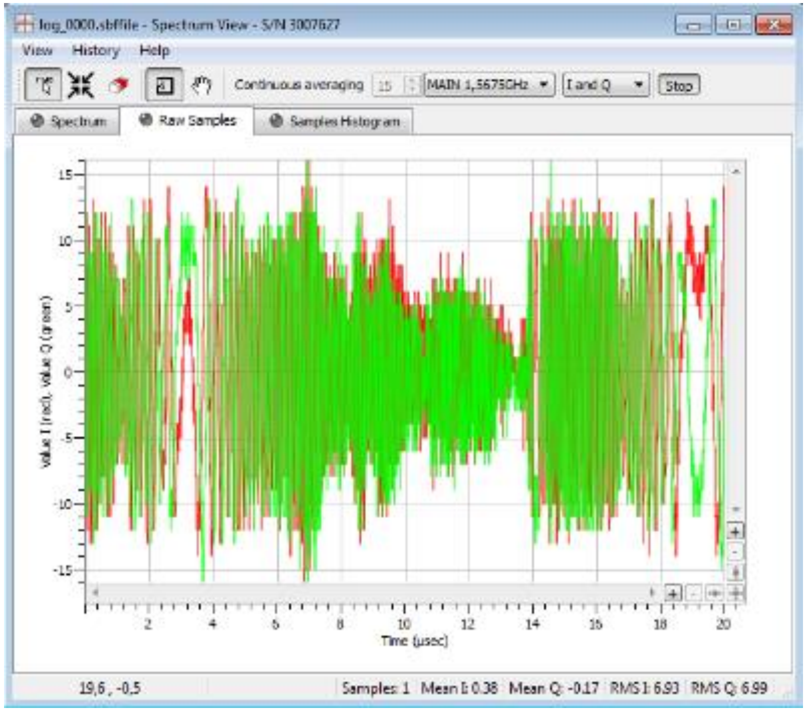
1.617,7 , 51,6

Samples: 15 Mean I: 0.96 Mean Q: 2.08 RMS I: 26.79 RMS Q: 26.27

Example Jammer: Problem Identification

Time & frequency domain plots in real time

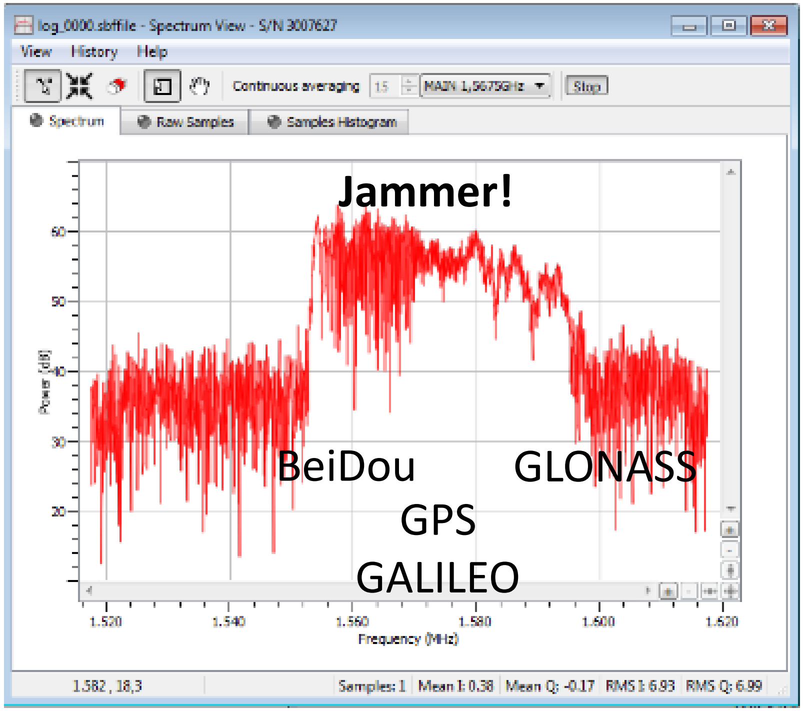
Time Domain Plot —FFT→ Frequency Domain Plot



Continuous averaging 15 | MAIN 1,5675GHz | I and Q

19,6 , -0,5 | Samples: 1 | Mean I: 0.38 | Mean Q: -0.17 | RMS I: 6.93 | RMS Q: 6.99

20 µs



Continuous averaging 15 | MAIN 1,5675GHz

1.582 , 18,3 | Samples: 1 | Mean I: 0.38 | Mean Q: -0.17 | RMS I: 6.93 | RMS Q: 6.99

Jammer!

BeiDou

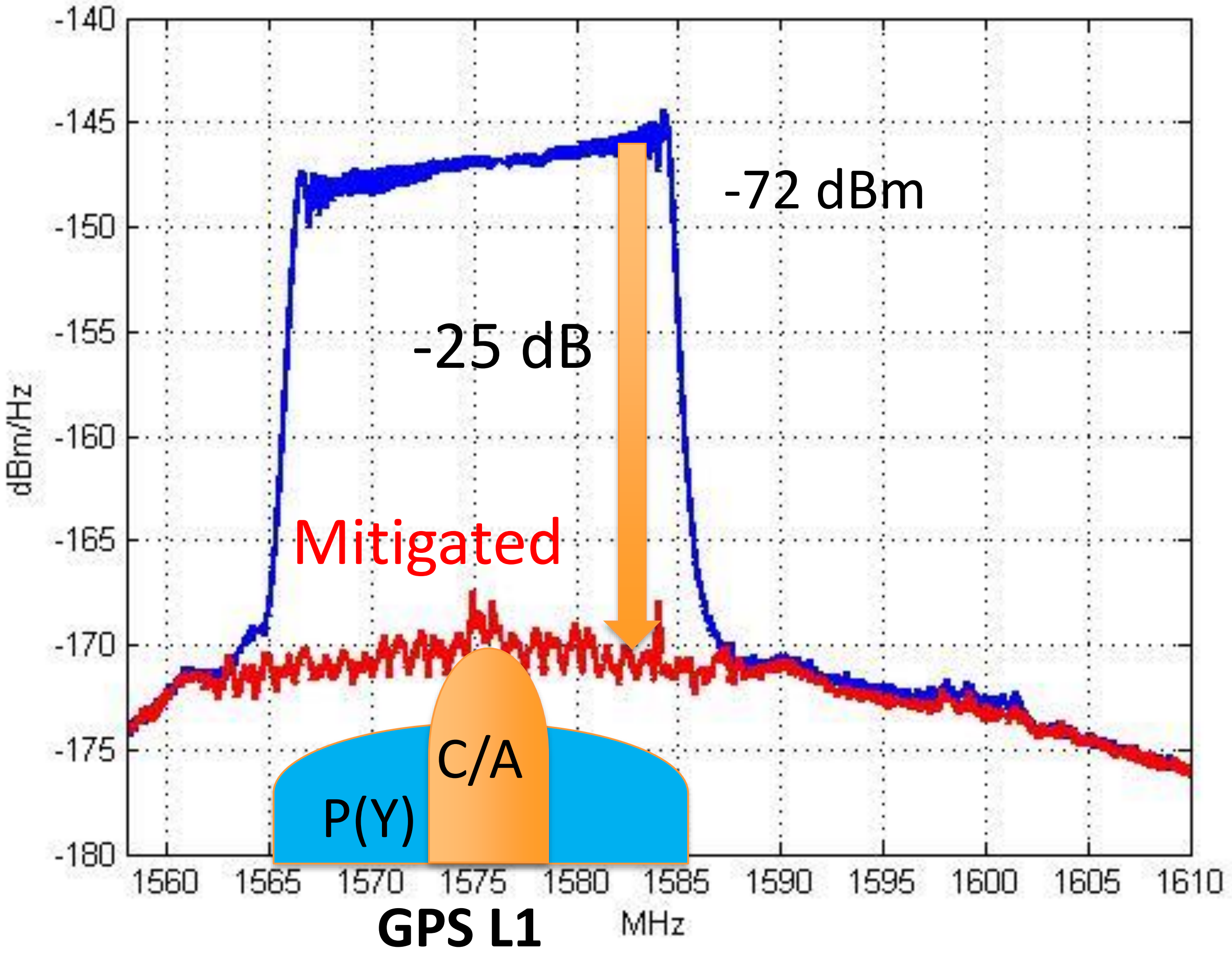
GLONASS

GPS

GALILEO

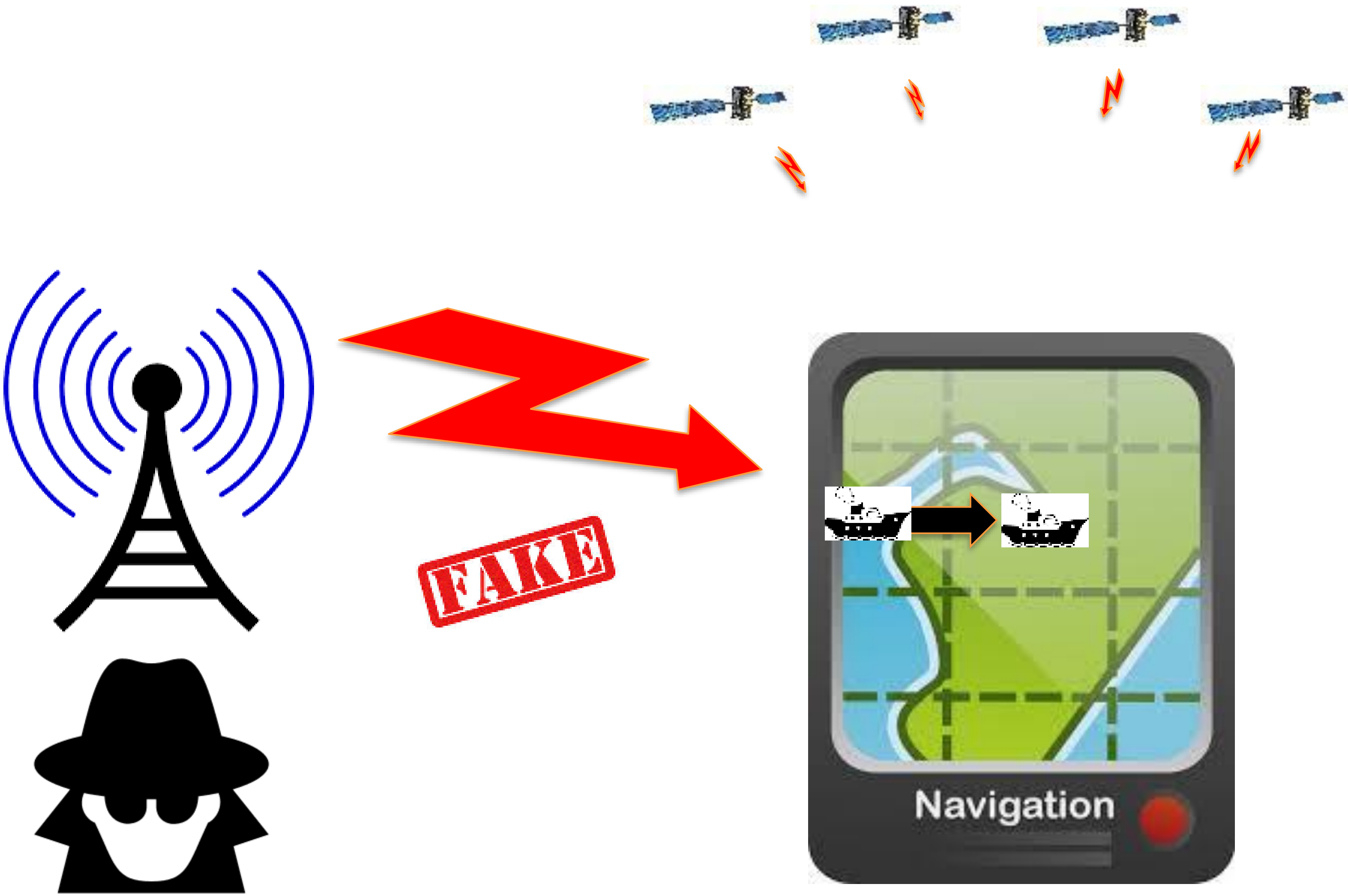
100 MHz

Chirp Jammer Mitigation



Spoofing

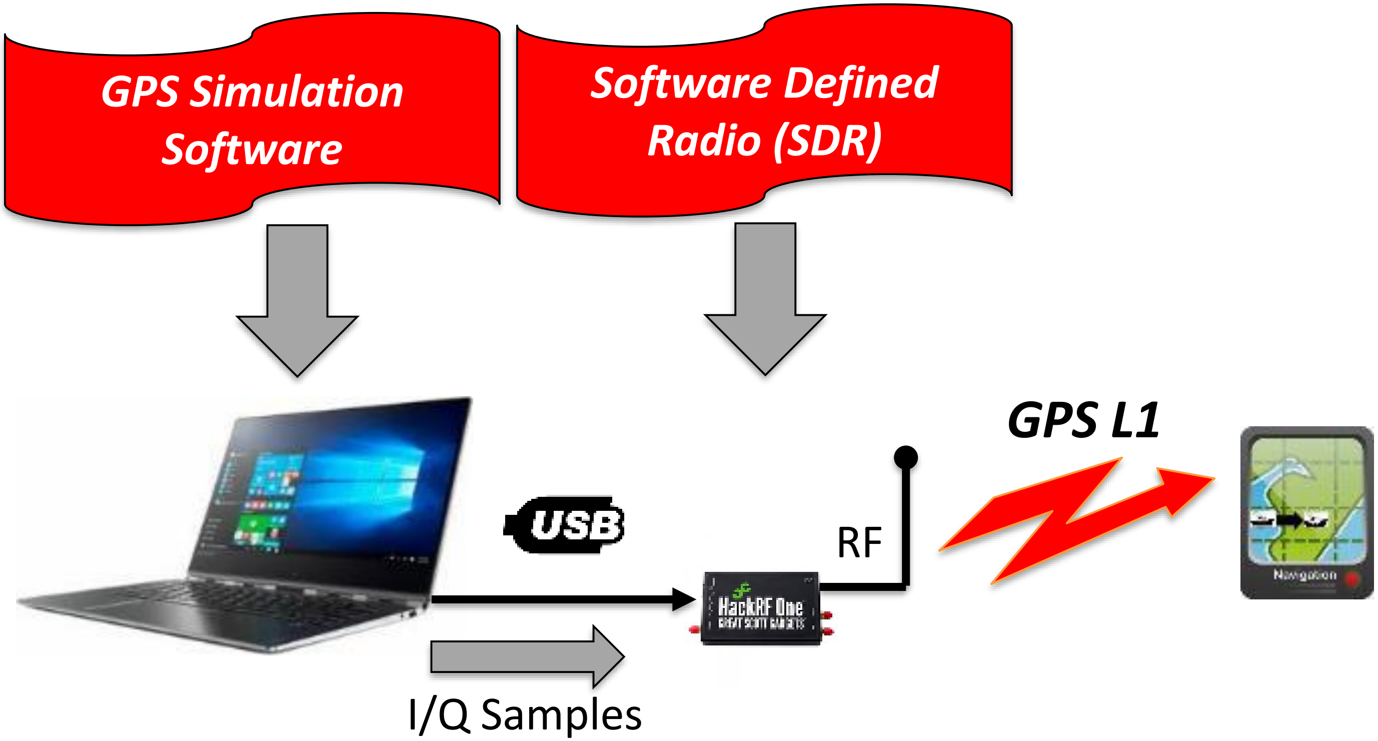
Spoofing Attack



septentrio

Spoofers: How feasible?

Budget Spoofer Ingredients



GPS Simulation Software

Software Defined Radio (SDR)

USB

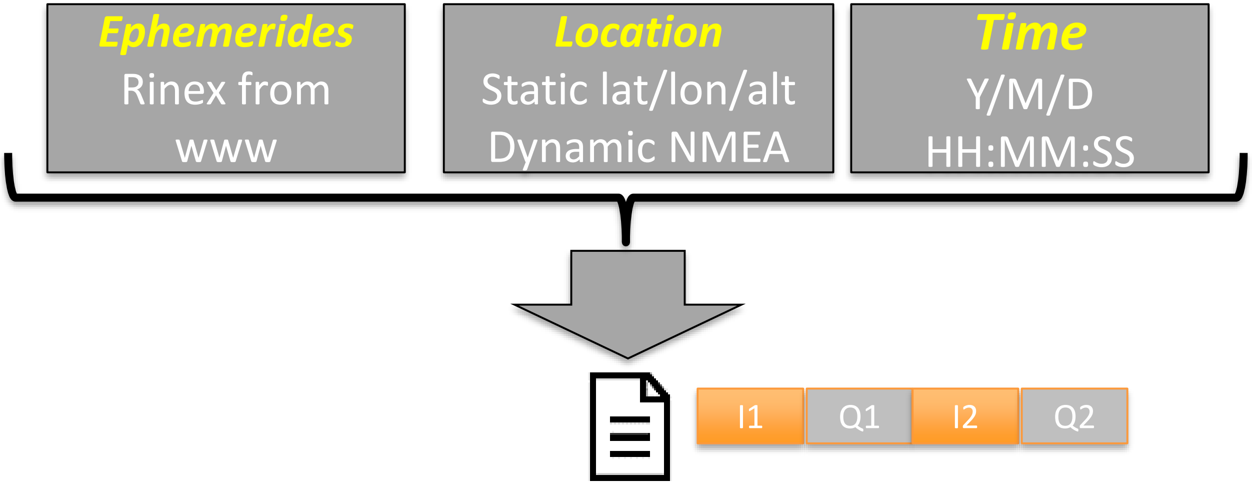
I/Q Samples

RF

GPS L1

Budget Spoofer Ingredients

- **GPS Simulation Software**
  - gps-sdr-sim
    - Open source (0€)
    - Easy to set up



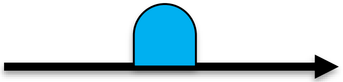
Ephemerides
Rinex from www

Location
Static lat/lon/alt
Dynamic NMEA

Time
Y/M/D
HH:MM:SS

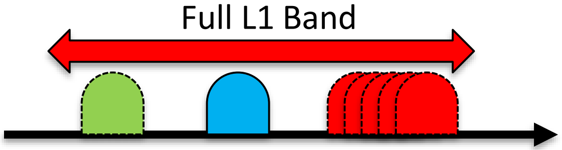
Budget Spoofer Ingredients

- **Software Defined Radio (SDR)**
  - HackRF One (2015)
    - Up to 20 MHz BW

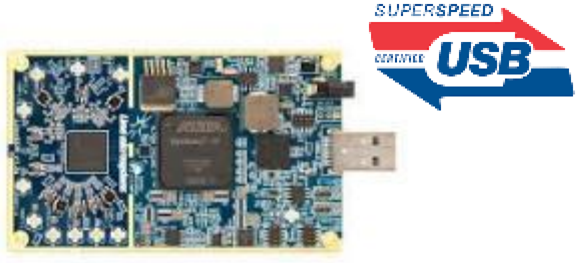


    - ca. 300€
    - Output up to 1 mW
    - **Overpowers receivers in ca. 1 km radius**

  - LimeSDR (2017)
    - Up to 60 MHz BW



    - ca. 250 €



Budget Spoofer Limitations

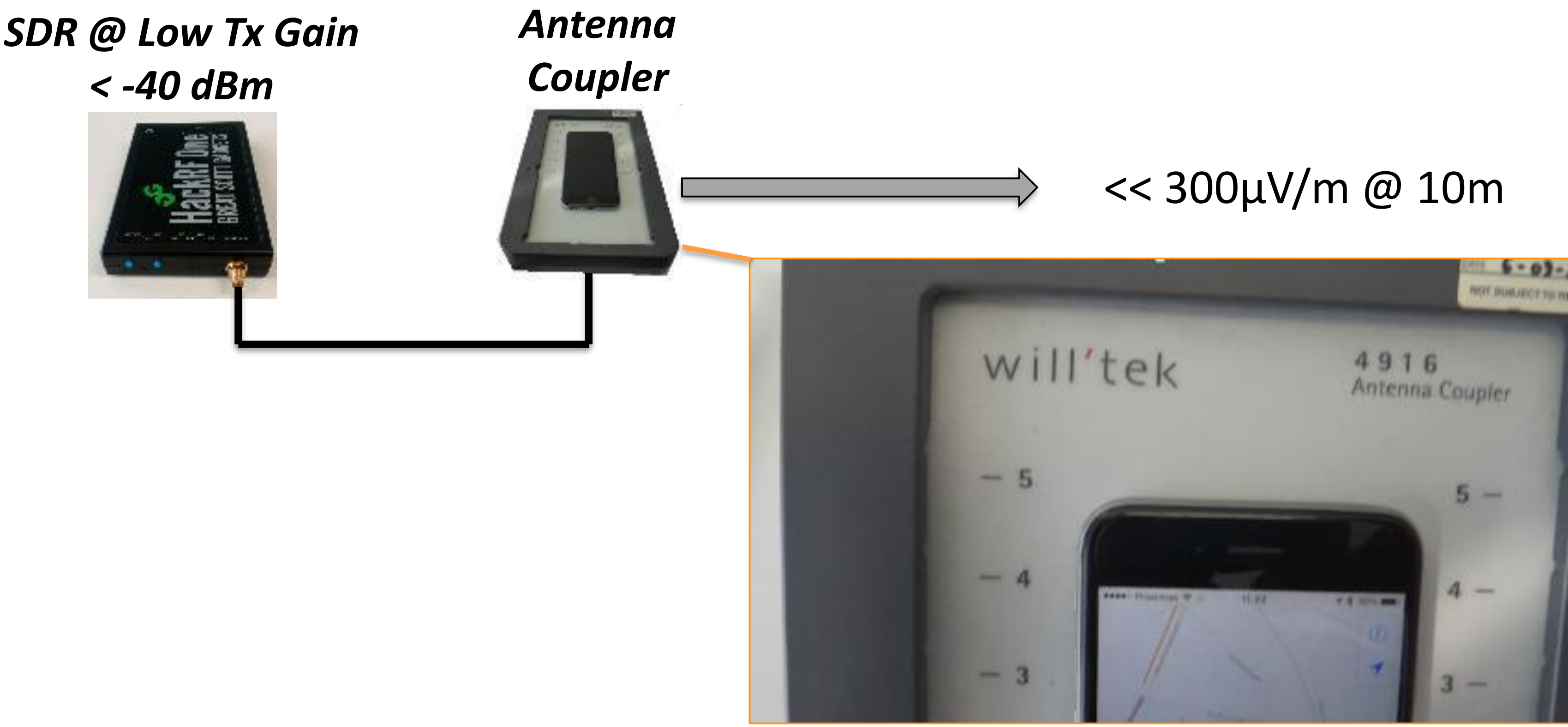
- **Software: GPS L1 C/A Only**
- **Start Time Uncertainty**
  - +/- 100 ms
- **Precomputed File**
  - Anticipate on time
  - No on-the-fly changes
- **However:**
  - Many spoofing projects active online
  - Real time version of gps-sdr-sim ...
- **Significant threat !**

Geek Required

Pokémon GO

Budget Spoofer Testing with iPhone 6

- Radiating Test using Antenna Coupler
- Low transmit power to avoid any harmful interference



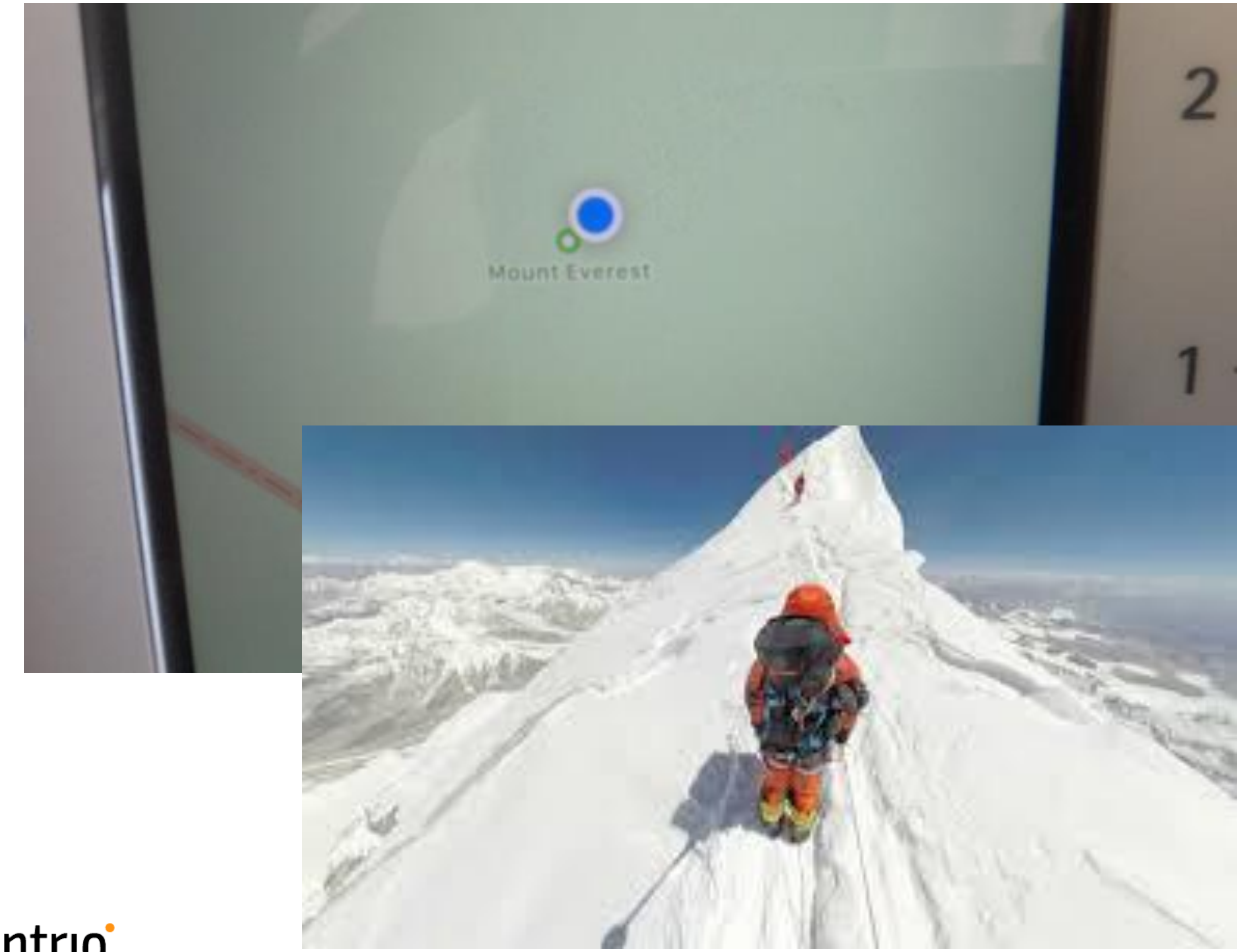
SDR @ Low Tx Gain < -40 dBm

Antenna Coupler

<< 300µV/m @ 10m

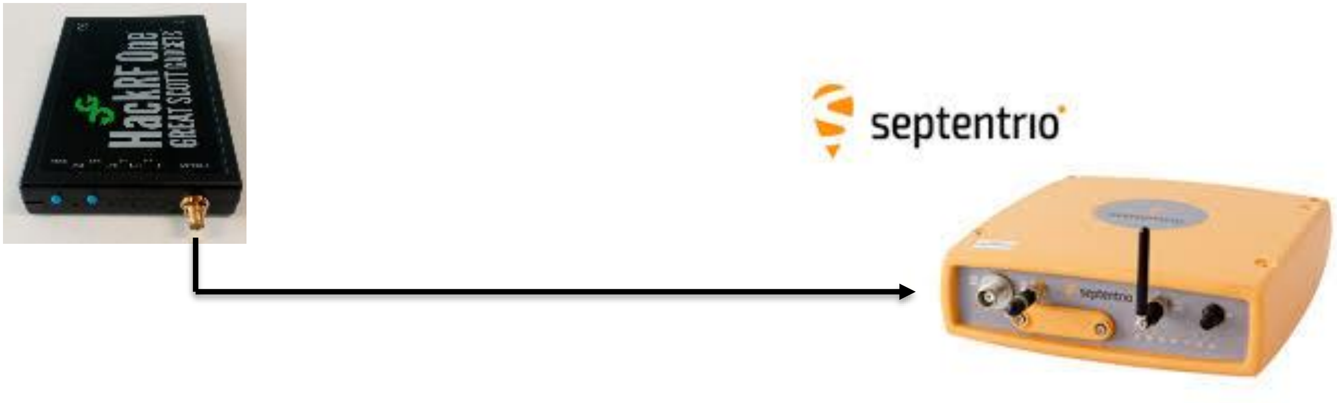
Budget Spoofer Testing with iPhone 6

- iPhone 6 very easily spoofed, even with Picowatts



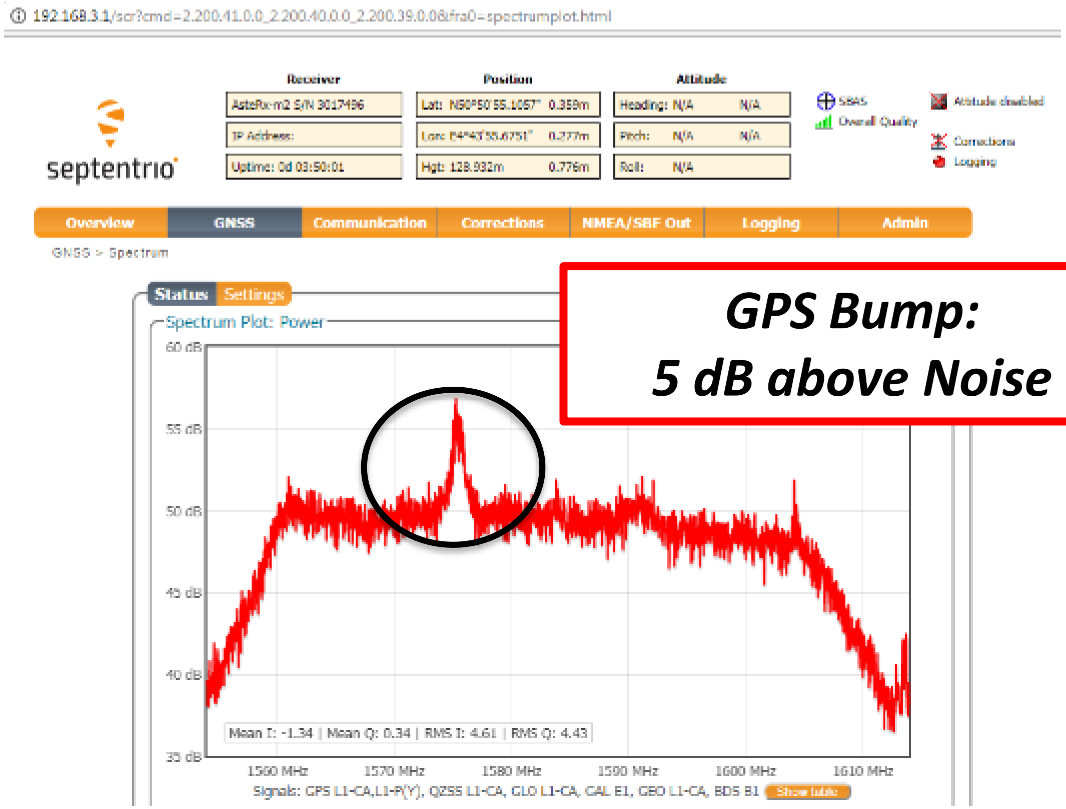
Spoofing Robustness of Septentrio Receivers

- Spectrum monitoring
  - Interference mitigation
- C/No monitoring
- Code-minus-Carrier Phase monitoring
- Receiver Autonomous Integrity Monitoring (RAIM)
- Redundancy (multi-band) + additional sensors (e.g. inertial)



Spectrum Monitoring

- Normal Spectrum, No Spoofing:



192.168.3.1/scr?cmd=2.200.41.0.0_2.200.40.0.0_2.200.39.0.0&fra0=spectrumplot.html

Receiver	Position		Attitude	
AsteRx-m2 S/N 3017496	Lat: N50°50'55.1057"	0.359m	Heading: N/A	N/A
IP Address:	Lon: E4°43'55.6751"	0.277m	Pitch: N/A	N/A
Uptime: 0d 03:50:01	Hgt: 128.932m	0.776m	Roll: N/A	

GNSS > Spectrum

Spectrum Plot: Power

Mean I: -1.34 | Mean Q: 0.34 | RMS I: 4.61 | RMS Q: 4.43

Signals: GPS L1-CA,L1-P(Y), QZSS L1-CA, GLO L1-CA, GAL E1, GEO L1-CA, BDS B1

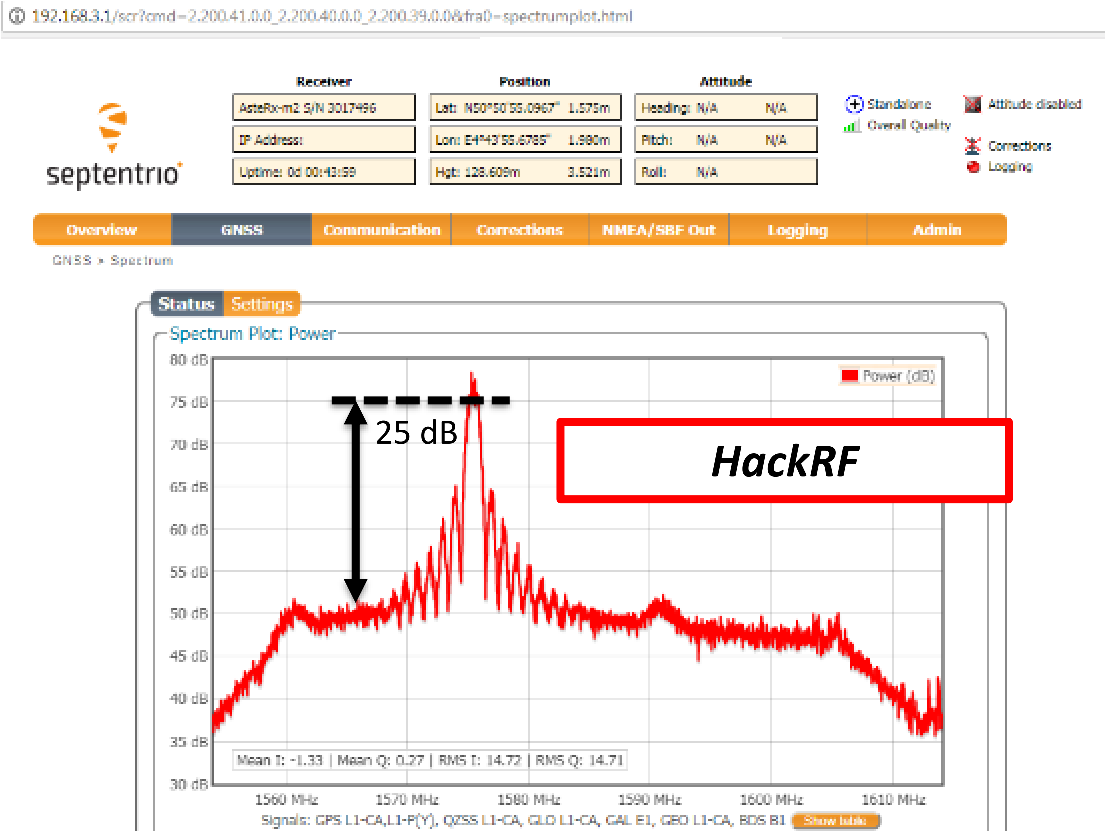
GPS Bump:
5 dB above Noise

AsteRx-m^2

Spectrum Monitoring

- Typical Spectrum during Spoofing Attack

  Detected by receiver as wide-band interference



192.168.3.1/scr?cmd=2.200.41.0.0_2.200.40.0.0_2.200.39.0.0&fra0=spectrumplot.html

Receiver	Position	Attitude
AsteRx-m2 S/N 3017456	Lat: N50°50'55.0967" 1.575m	Heading: N/A N/A
IP Address:	Lon: E4°43'55.6785" 1.980m	Pitch: N/A N/A
Uptime: 0d 00:43:59	Hgt: 128.609m 3.521m	Roll: N/A

Mean I: -1.33 | Mean Q: 0.27 | RMS I: 14.72 | RMS Q: 14.71

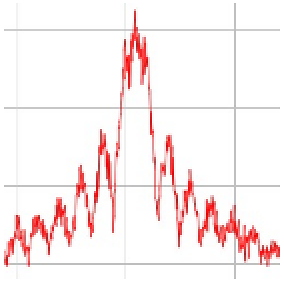
Signals: GPS L1-CA,L1-P(Y), QZSS L1-CA, GLO L1-CA, GAL E1, GEO L1-CA, BDS B1

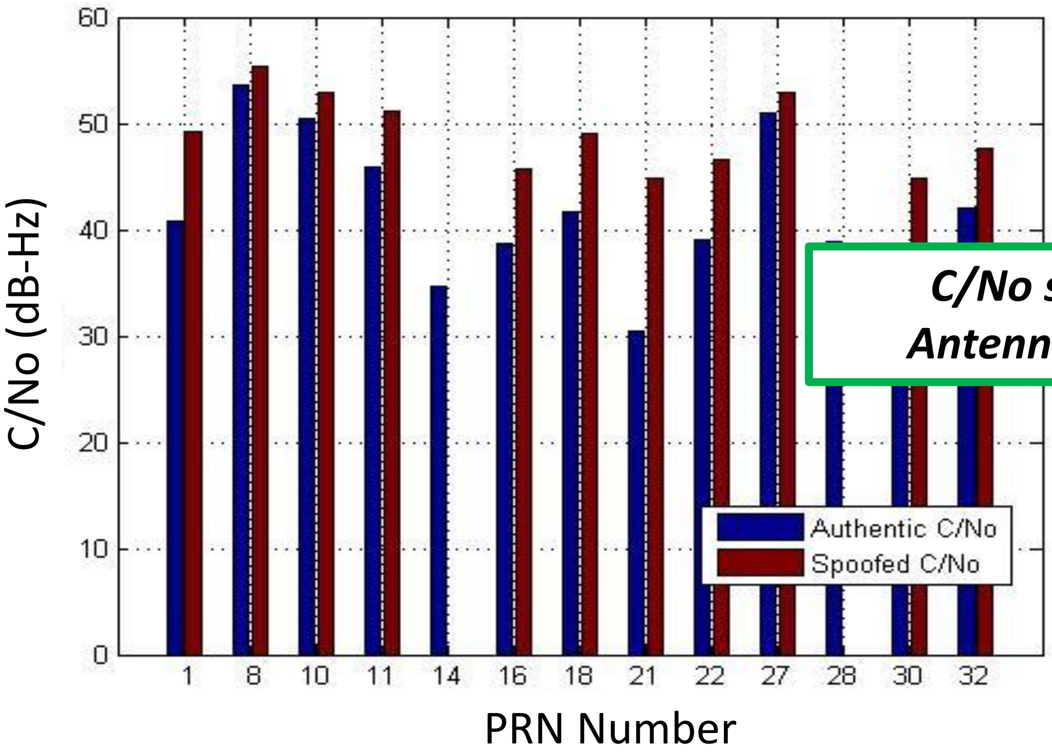
HackRF

Message Indicates Wide-band Interference @ 1575 MHz

C/No Monitoring

- C/No Close to Reality (!)

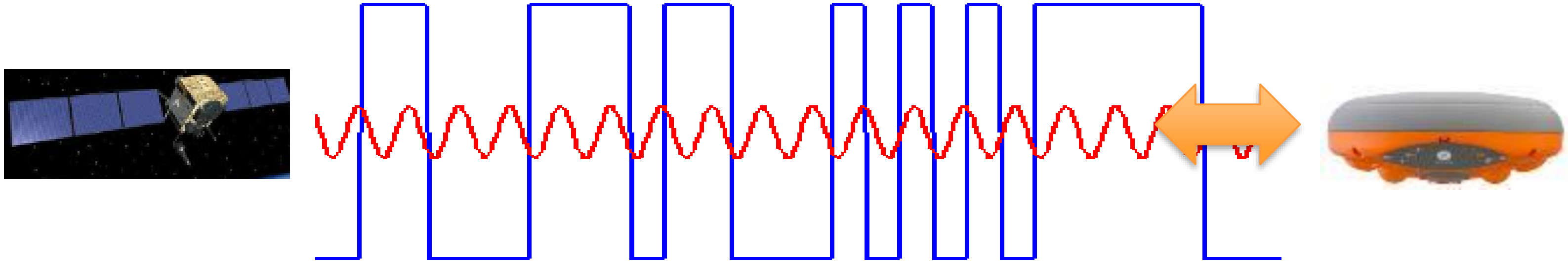




C/No set by Cross-Talk Antenna Gain Emulation

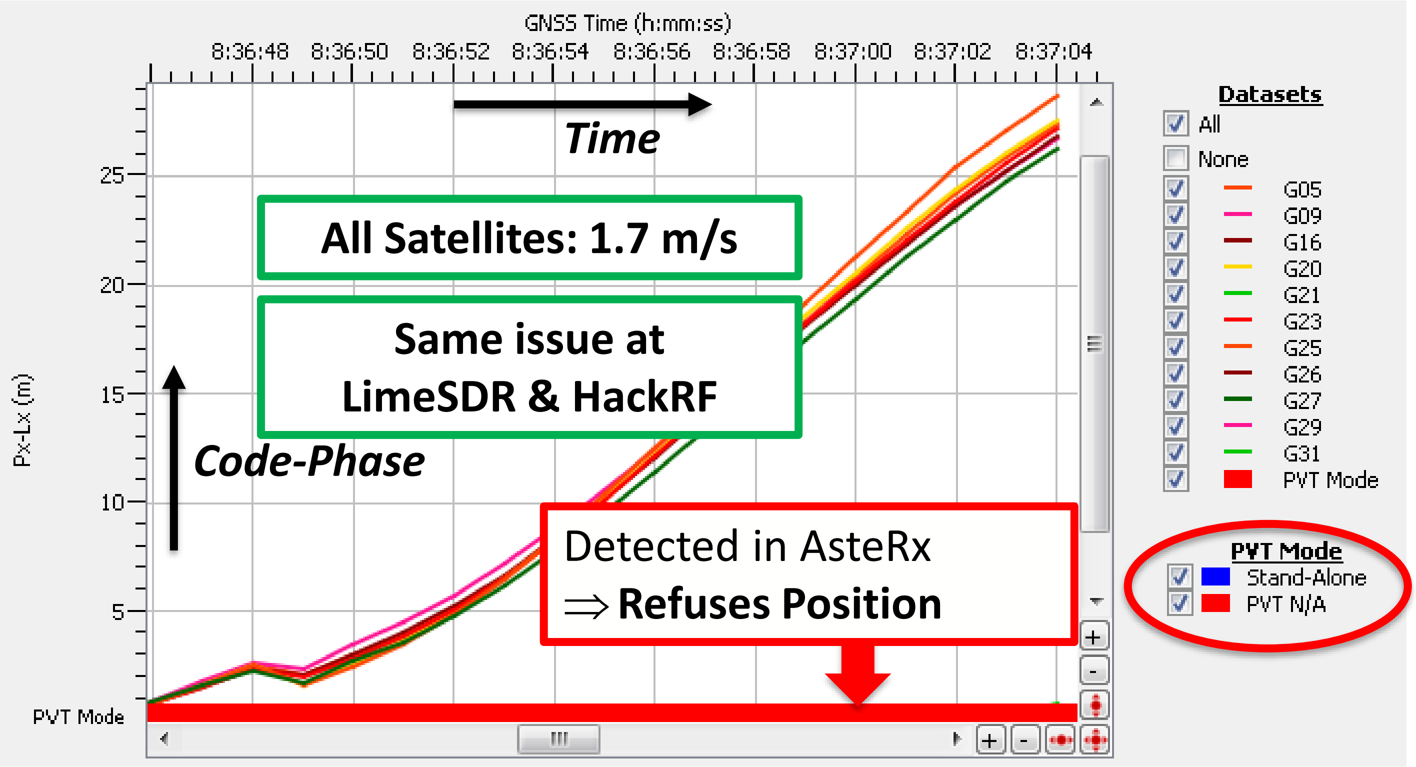
Range Quality Monitoring

- Code-minus-Carrier Phase monitoring
  - Same Physical Range
  - Should only change slowly (cm/s)
    - Ionosphere, Phase Wind Up



Range Quality Monitoring

- Receiver directly connected to SDR (only GPS L1 C/A signals)
- Huge Code-Carrier Divergence detected
- Receiver not spoofed



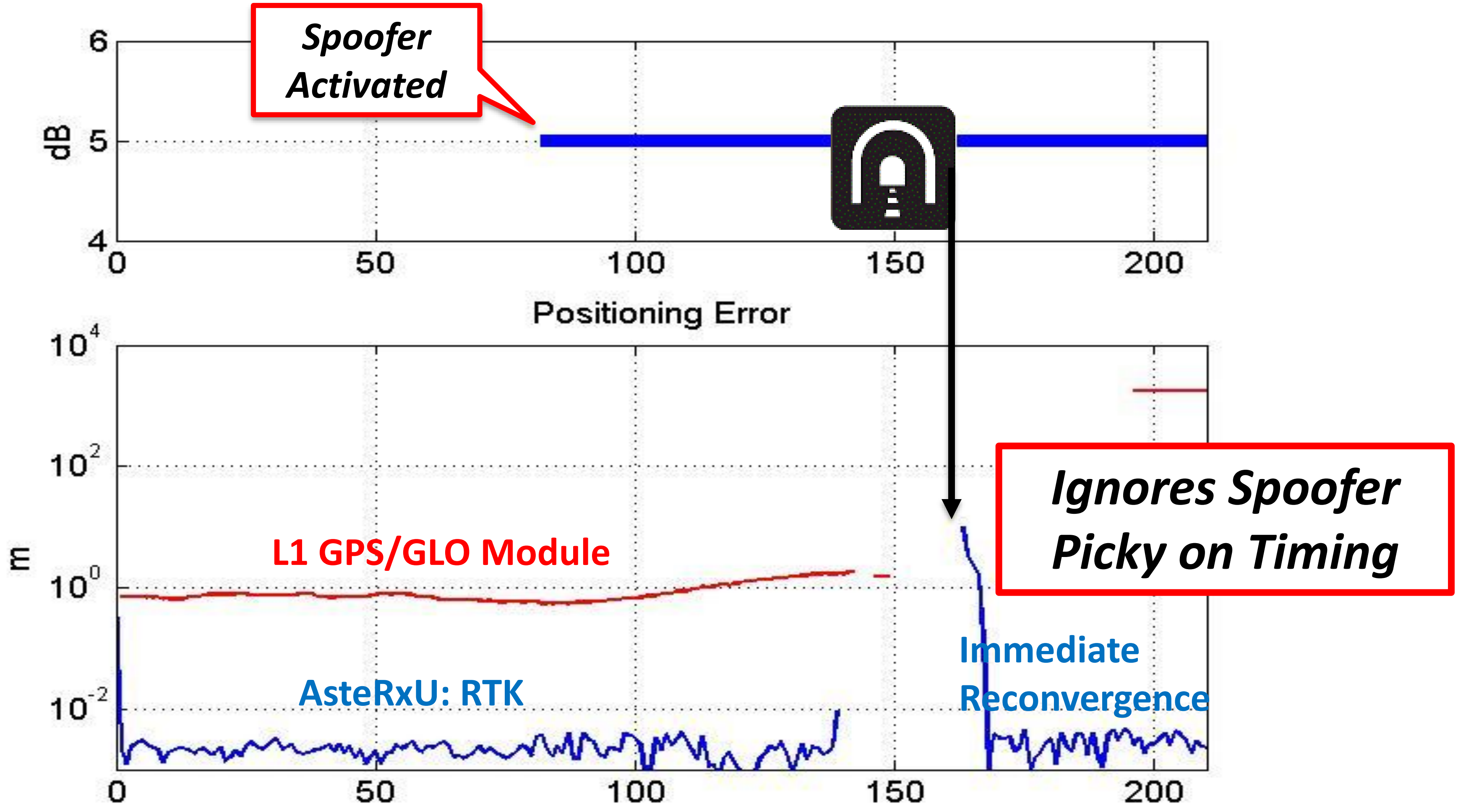
All Satellites: 1.7 m/s

Same issue at LimeSDR & HackRF

Detected in AsteRx

⇒ **Refuses Position**

AsteRx-U Receiver in “Tunnel Test”



Spoofer Activated

L1 GPS/GLO Module

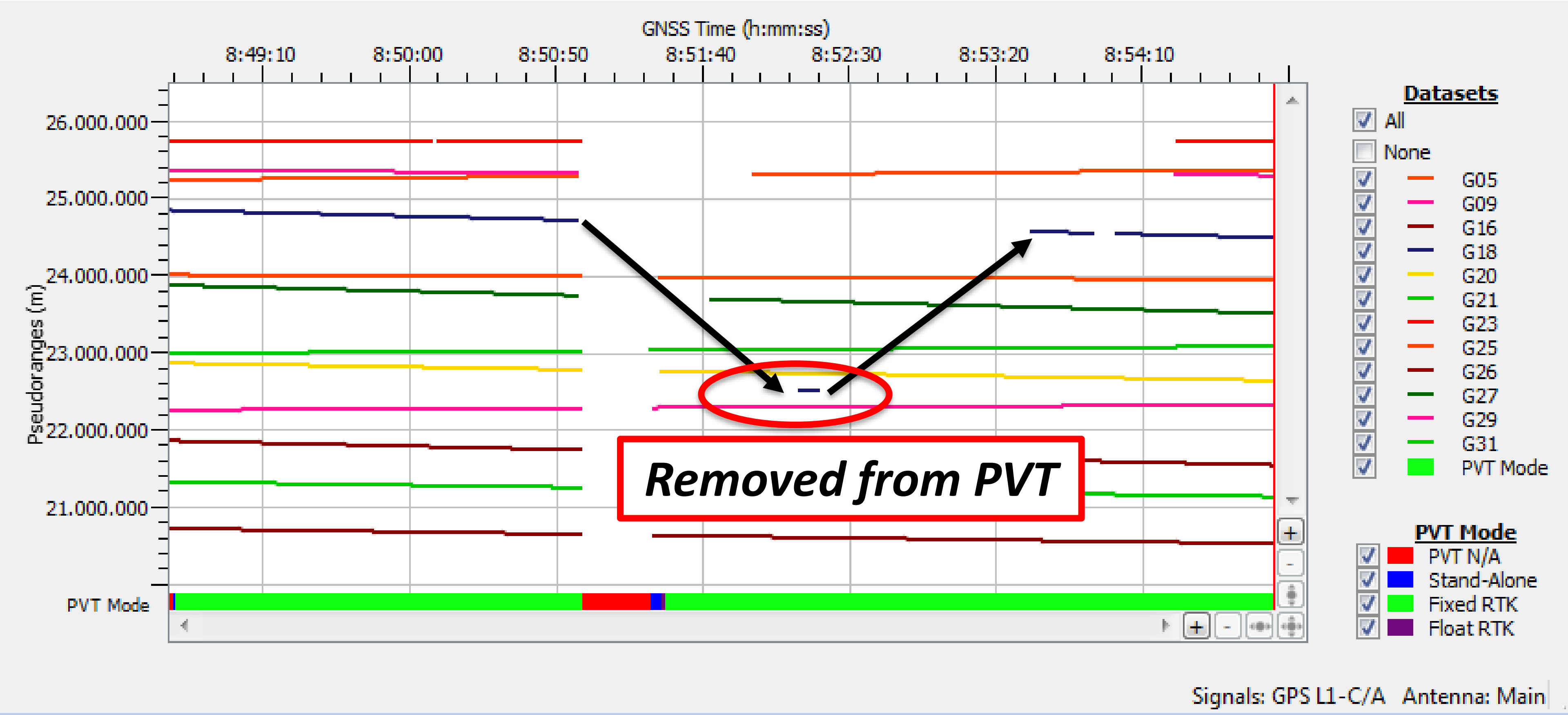
AsteRxU: RTK

Ignores Spoofer
Picky on Timing

Immediate Reconvergence

Receiver Autonomous Integrity Monitoring

- Receiver rejects ranges that don't make sense

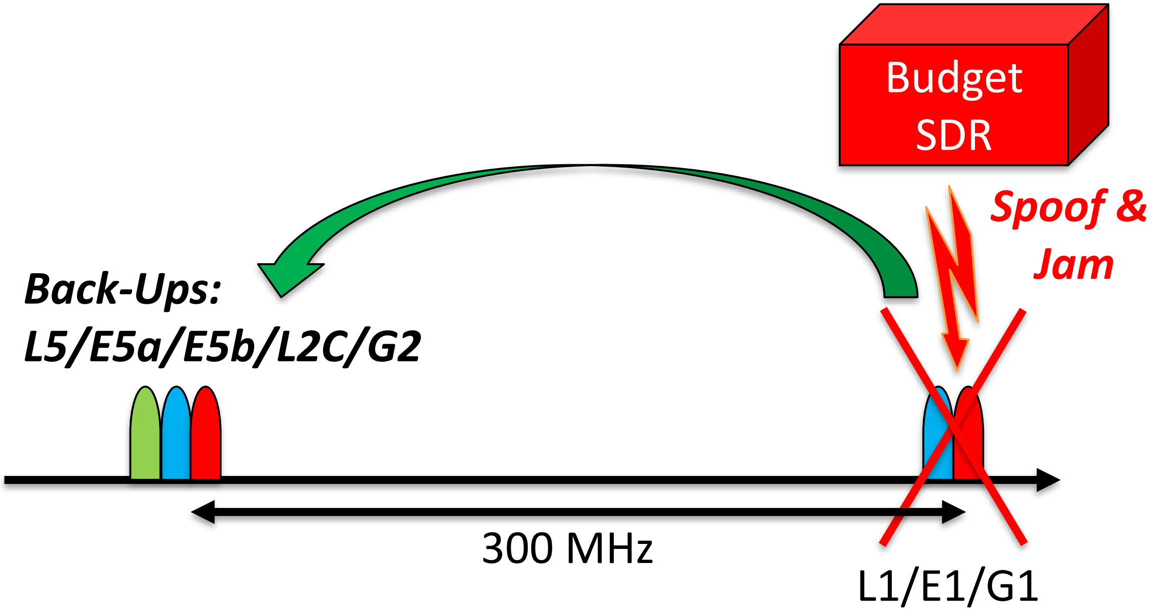


Removed from PVT

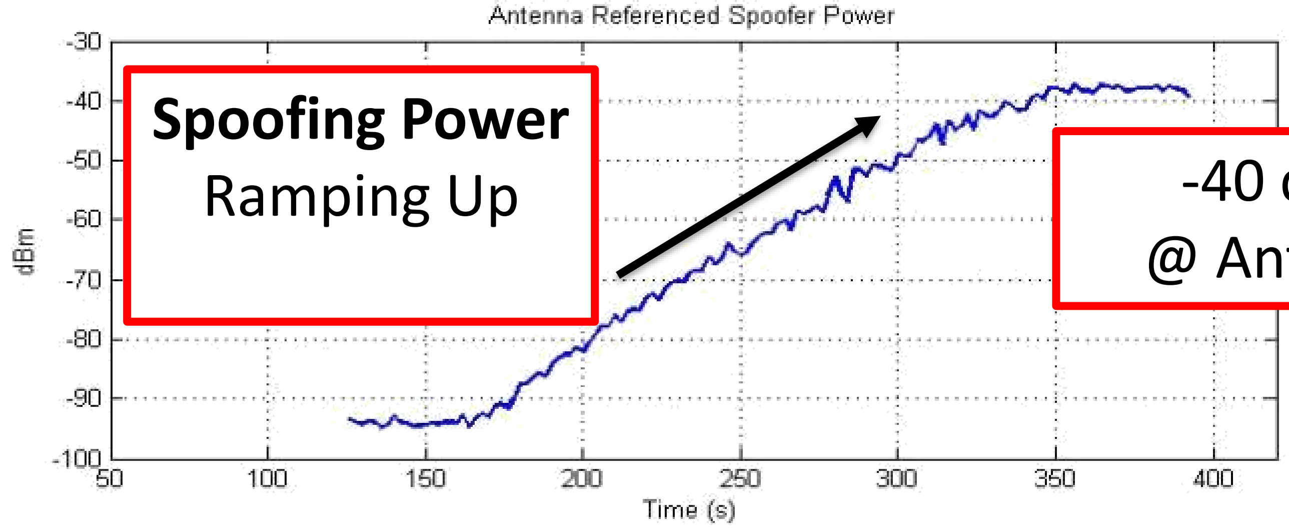
septentrio

Redundancy: GNSS and non-GNSS

- Receivers fully exploit **Frequency Diversity**
  - + Good RF Filtering
  - + Independent tracking of different signals
- Other sensors (non-GNSS) also help, e.g. INS hybridisation



AsteRx Survives Extreme Spoofing Power



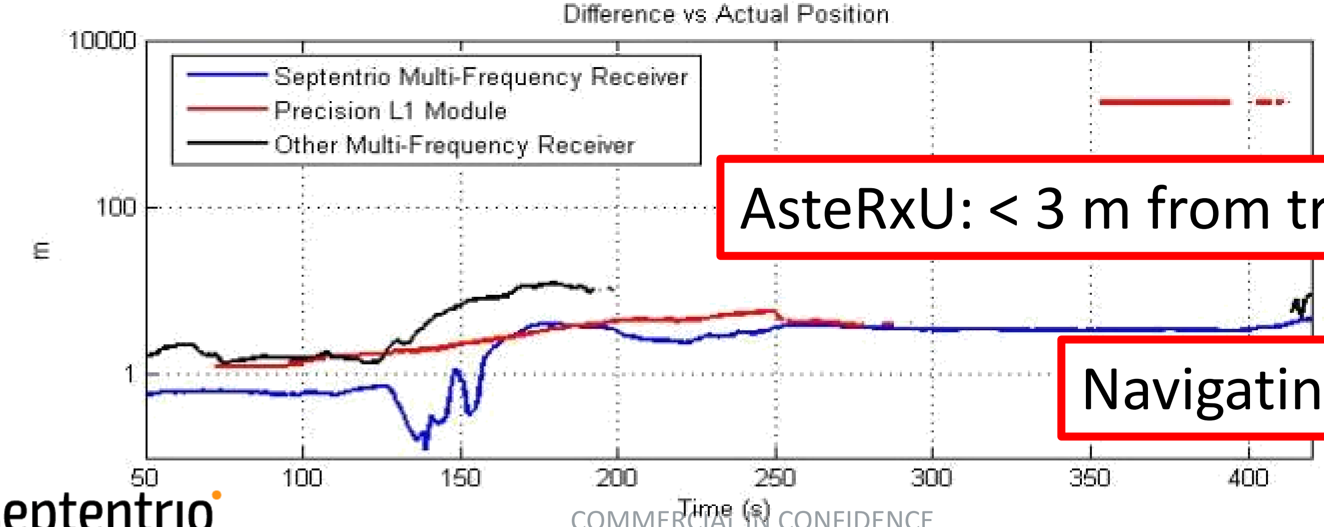
Antenna Referenced Spoofer Power

Spoofing Power

Ramping Up

-40 dBm

@ Antenna



Difference vs Actual Position

AsteRxU: < 3 m from track

Navigating on L2/L5

Conclusions

- **Generic Interference**

✓ Adaptive Notch Filters

✓ Adaptive Frequency Domain Filters

- **Jammers** (from € 20) are a significant threat

✓ Smart adaptive filtering

- **Spoofers** (from €300 !) are a significant threat

✓ Detection of signal anomalies in terms of spectrum, code-minus-carrier phase, C/No, etc.

✓ Reject anomalous signals/measurements

✓ Receiver Autonomous Integrity Monitoring (RAIM)

✓ Exploit redundancy (multi-band, other sensors)

Tom Willems – tom.willems@septentrio.com

septentrio

Europe

Greenhill Campus
Interleuvenlaan 15i,
3001 Leuven
Belgium

+32 16 30 08 00

Americas

23848 Hawthorne Blvd.
Suite 200,
Torrance, CA 90505
USA

+1 888 655-9998

Asia/Pacific

Level 901
The Lee Gardens 33,
Hysan Avenue, Causeway Bay
Hong Kong

+852 3959 8680

@septentrio
www.septentrio.com