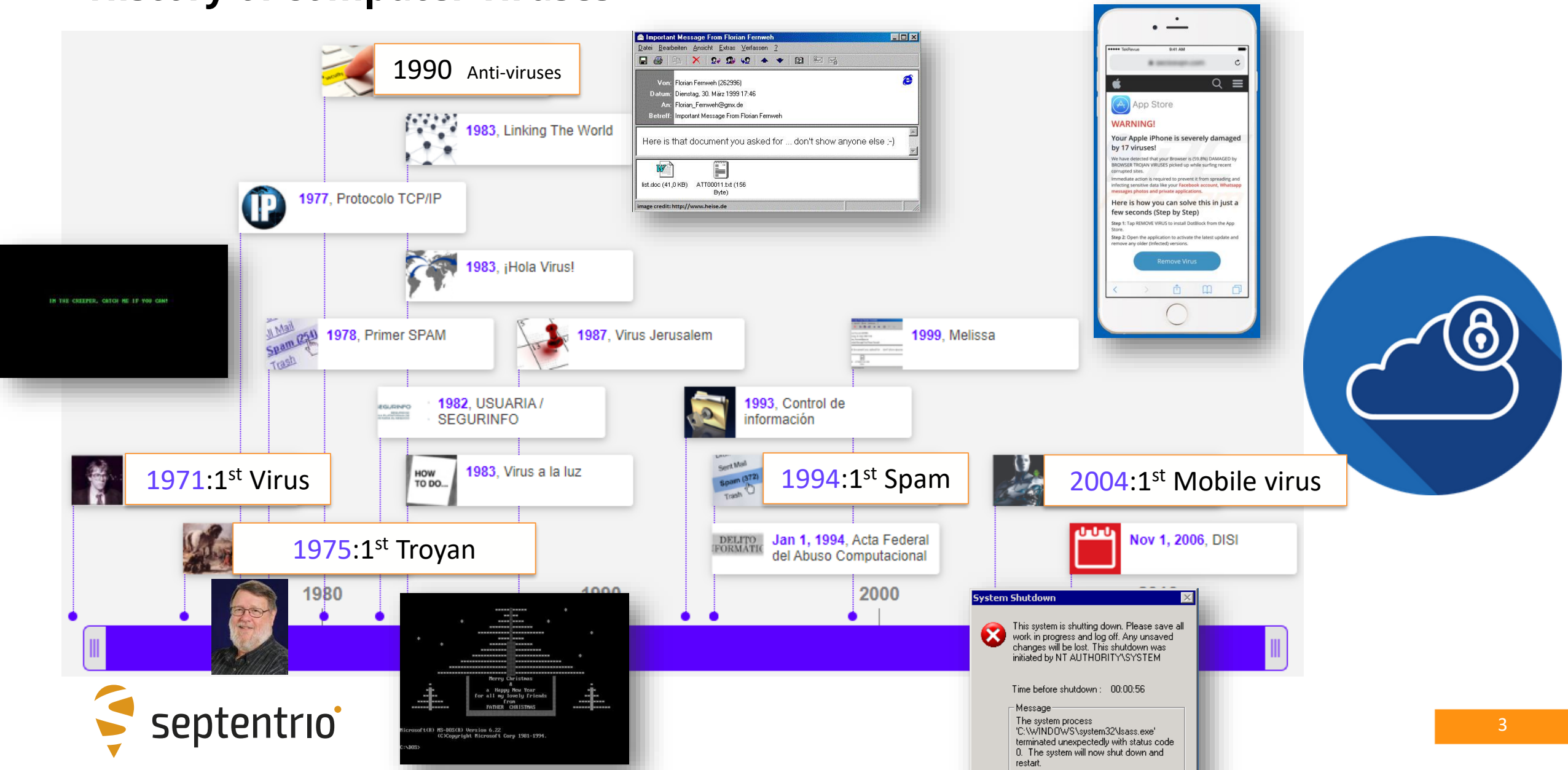
Practical experience with and countermeasures for GNSS jamming and spoofing

Gustavo Lopez

18 December 2019

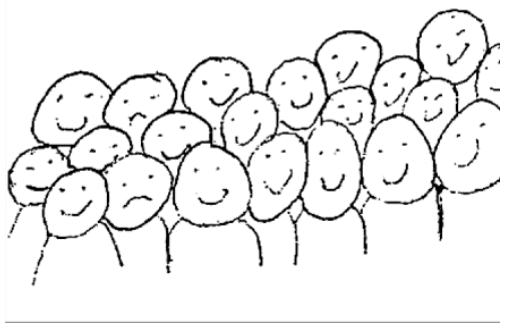
1983

History of computer viruses

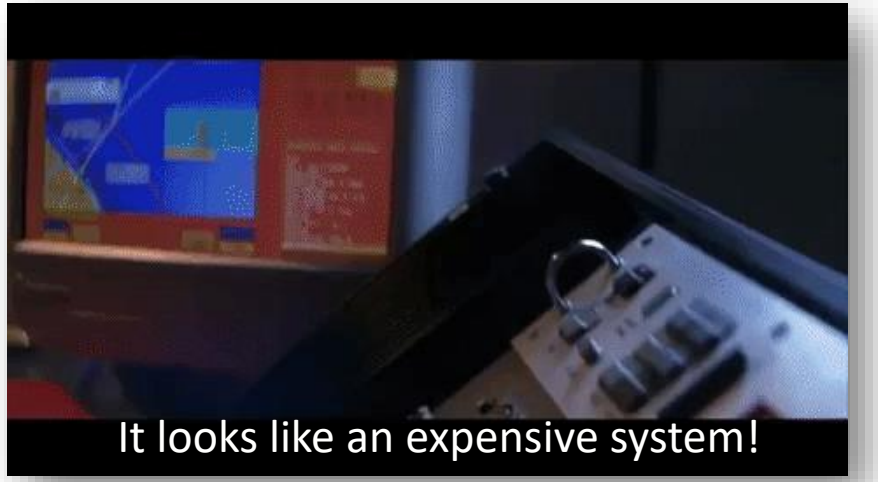


septentrio

People do know about computer viruses



What about GPS jamming/spoofing?



septentrio

Who is Septentrio?

APPLICATION KNOW HOW

- Machine control & guidance
- Reference stations
- Scientific applications
- Survey, Mapping and GIS
- UAS & Robotics

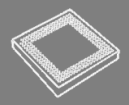
RELIABLE & ACCURATE POSITIONING

- Reliable positioning
- Advanced anti-jamming & anti-spoofing technology
- Robust and secure FW

YOUR OEM PARTNER

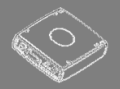
- Our mission is to make our customers successful

septentrio



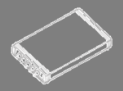
Modules

Boards



Housed receivers

Smart antenna

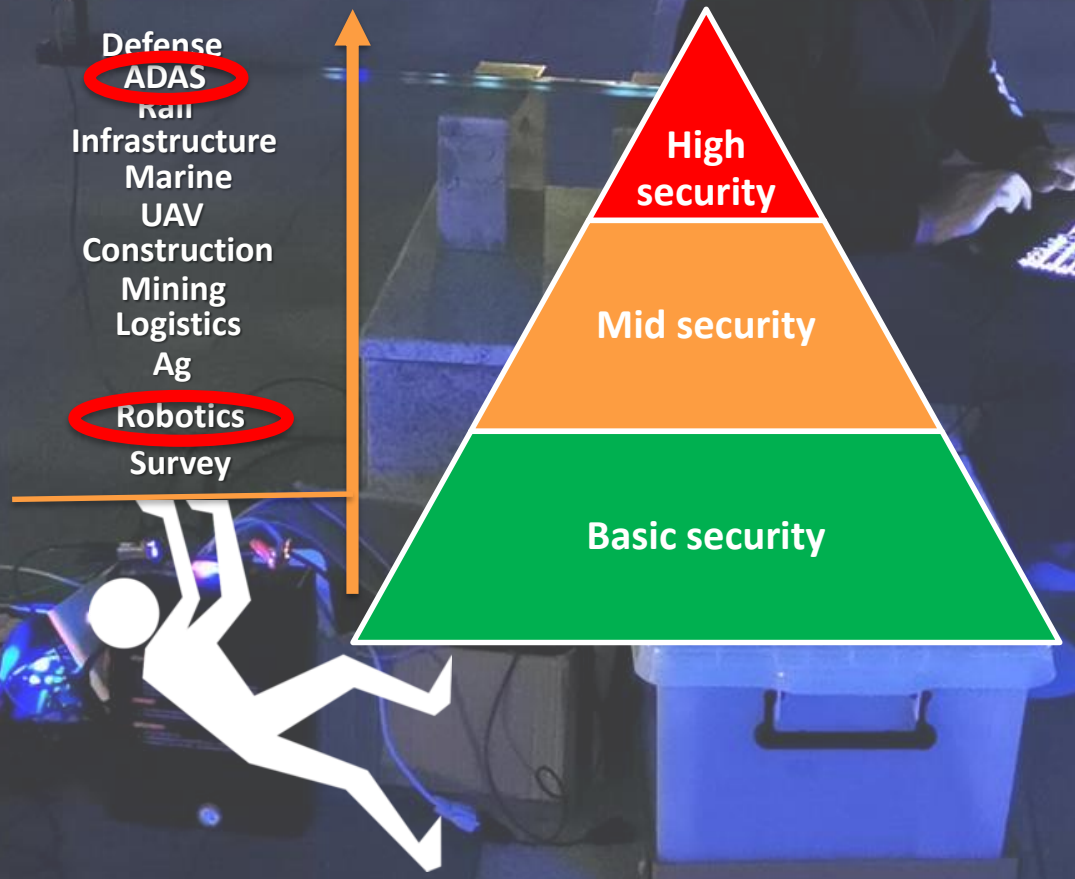


Scientific Receivers

GNSS used more & more in critical applications

Sensitivity by market

Different users & needs => all being pushed higher in reliability



septentrio

Do people know about jamming?

Or spoofing?

1. What is GPS spoofing?

- A GPS signal destroyed
- A signal pretending to be a GPS signal
- A computer virus affecting my GPS
- A weak signal which does not allow me to know my GPS location
- Do not know

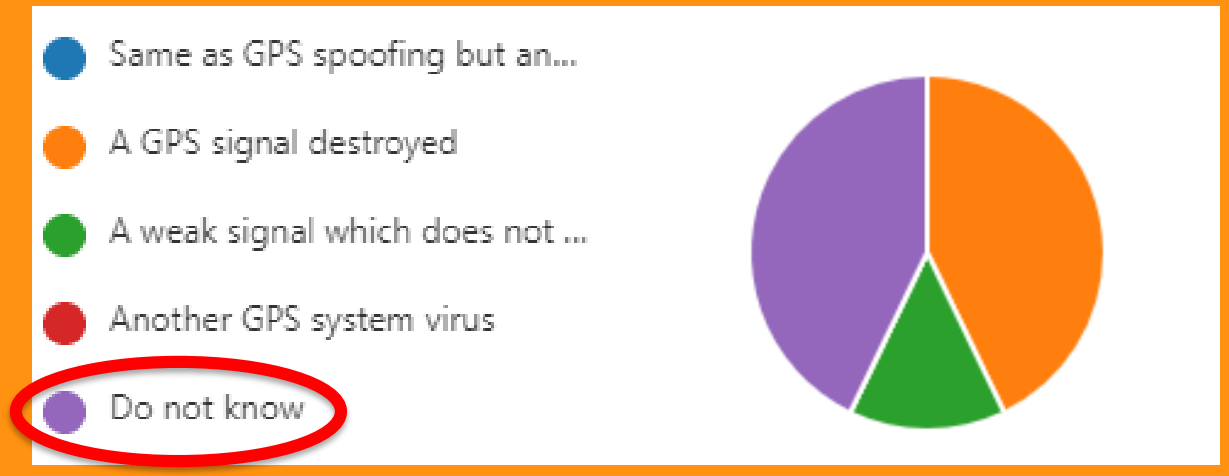
SPOOFING?

septentrio

2. Do you know what is GPS jamming?

- Same as GPS spoofing but another name
- A GPS signal destroyed
- A weak signal which does not allow me to know my GPS location
- Another GPS system virus
- Do not know

JAMMING?

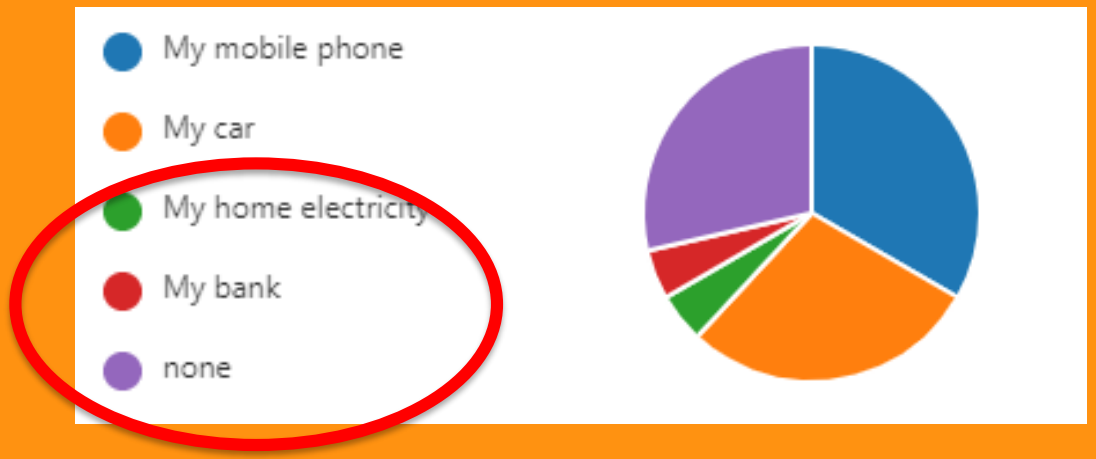


septentrio

3. If GPS fails what is going to be affected

- [ ] My mobile phone
- [ ] My car
- [ ] My home electricity
- [ ] My bank
- [ ] none

RISK?

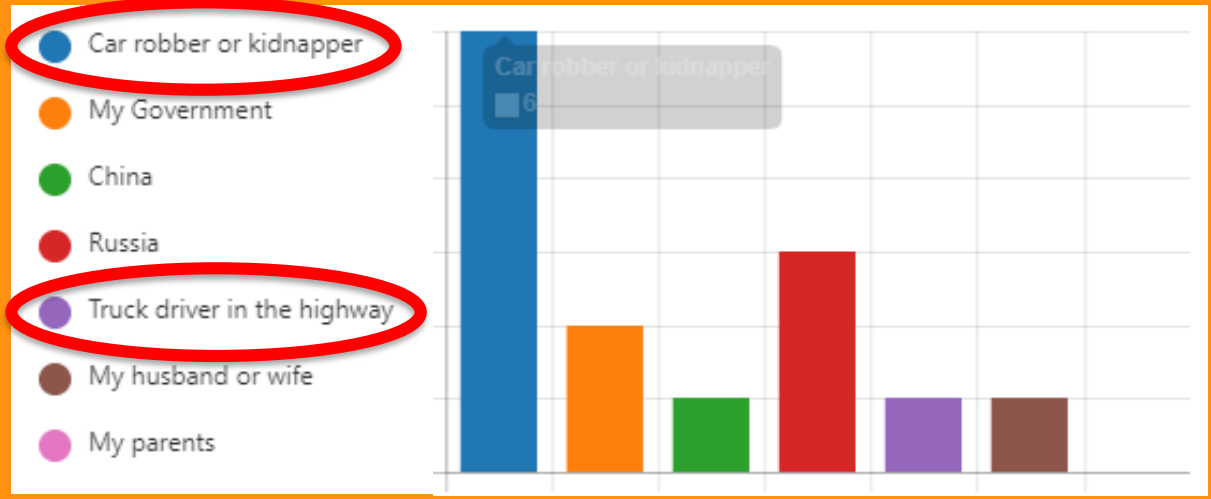


septentrio

6. Who could be more likely to hack your GPS position?

- Car robber or kidnapper
- My Government
- China
- Russia
- Truck driver in the highway
- My husband or wife
- My parents

WHO IS THE ATTACKER?



septentrio

Failed ☹

People do not really know about Spoofing or Jamming

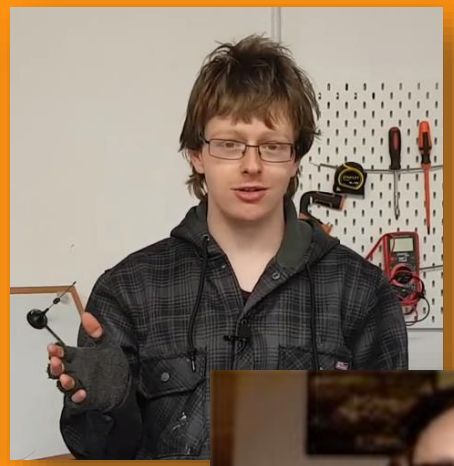
septentrio

Computer Security

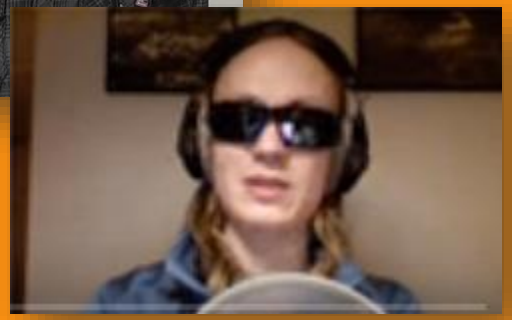
Bob Thomas

Jamming/Spoofing

Todd Humphreys

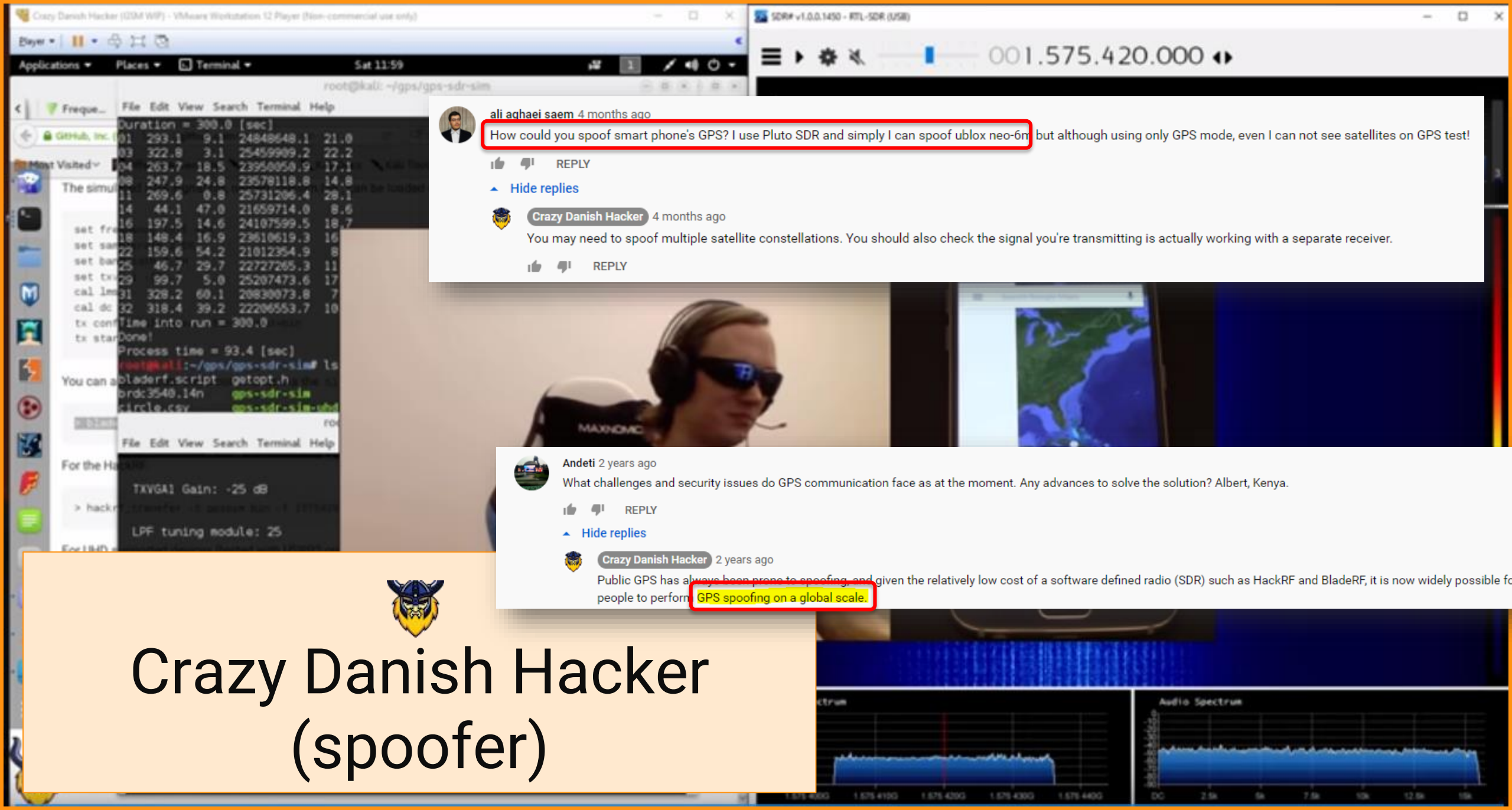


Maker Vlog



Crazy Danish Hacker

septentrio



Crazy Danish Hacker (spoofer)

Tunakann 2 months ago

So all you need is the Arduino? The transmitter and power just affect the strength and range?

3 REPLY

Hide replies

Maker Vlog 2 months ago

Pretty much

3 REPLY

Love Revolution 2 weeks ago

Anyone know where they're not illegal, lol. How could they know if you're using it? I want to build one for my home that neutralizes all frequencies, including satellite, for mind body protection. Are the frequencies transmitted by the jammer equally malignant or Benin? Could natural sound waves, ocean etc be used? ♥

Tabish khan 1 month ago

how about GPS signal. Is it easy to design a jamming devise for GPS signal.

REPLY

Hide replies

Maker Vlog 1 month ago

All you need is a device that can transmit on those frequencys

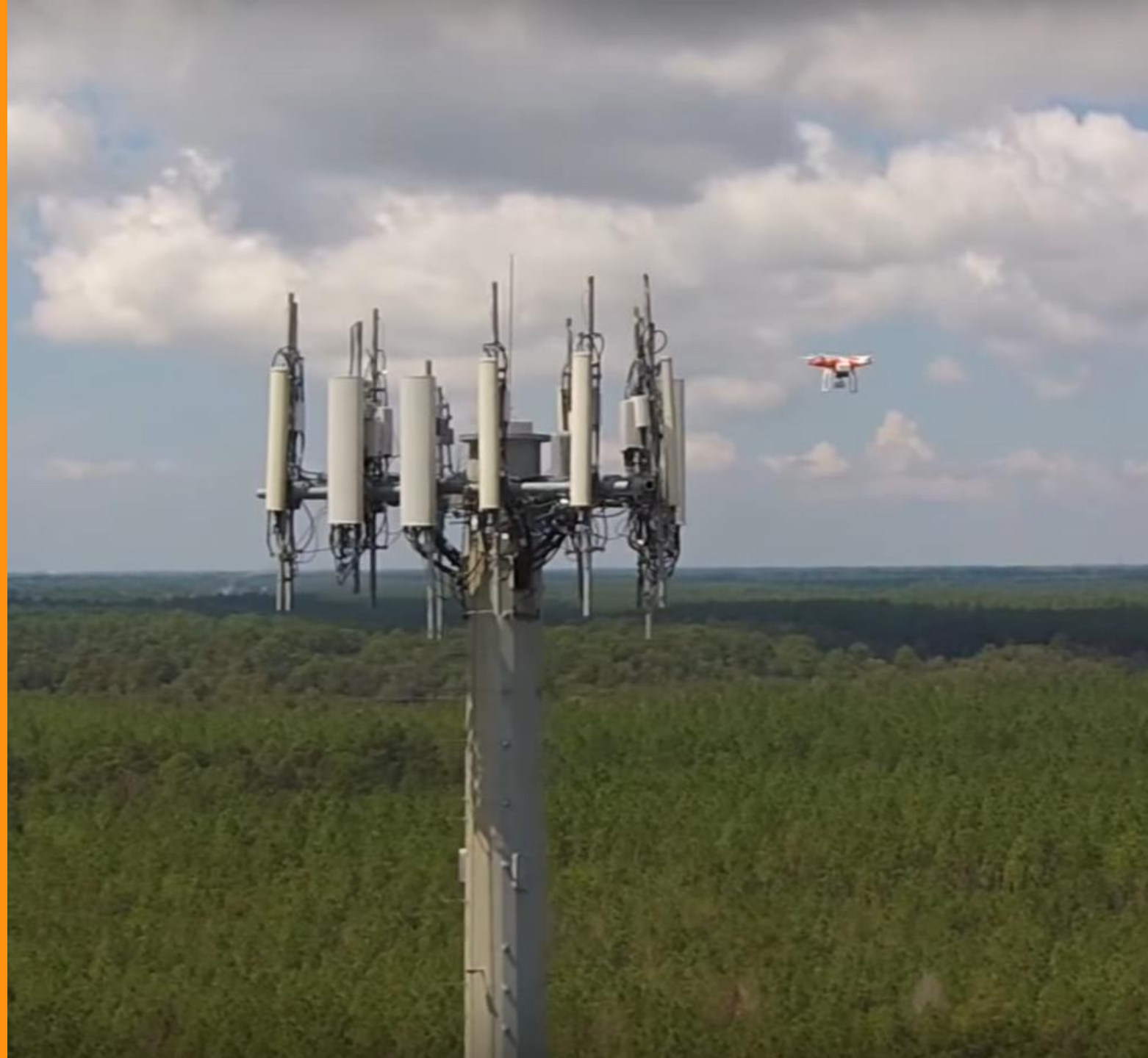
REPLY

How to Make A Mobile Multi Frequency Jammer

Maker Vlog (jammer)

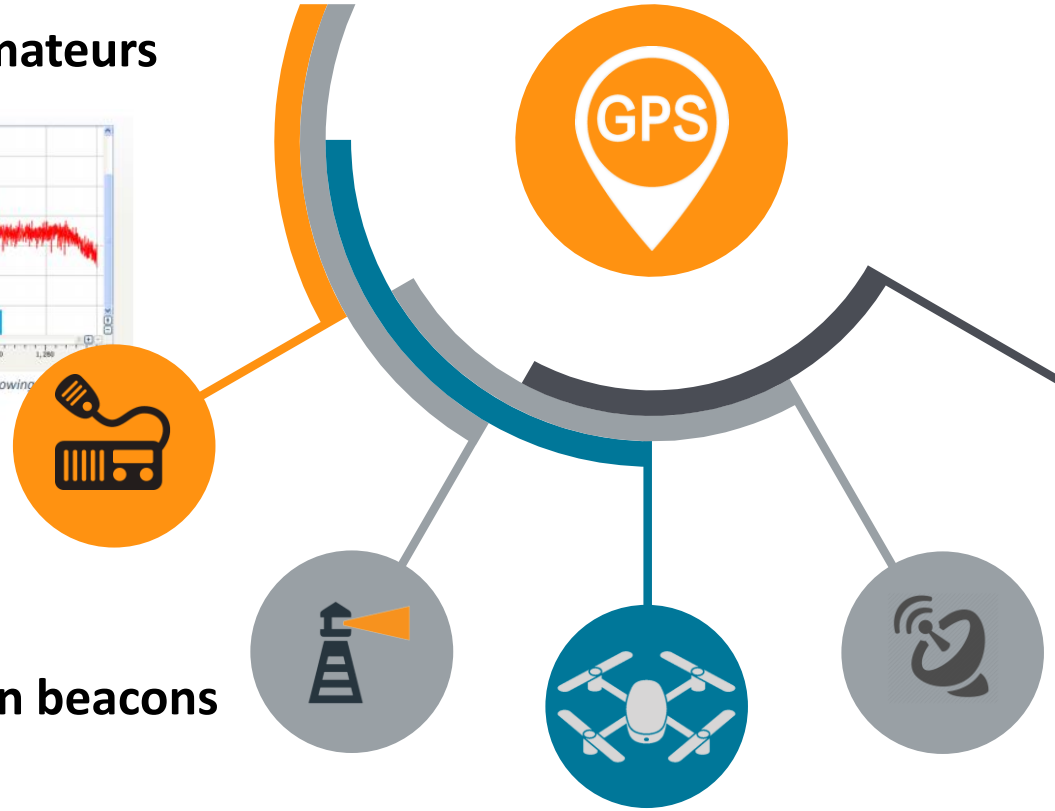
Interference (Jamming)

Examples



septentrio

Common cases of interference



Radio amateurs

Figure 2: construction site at Ostend harbour

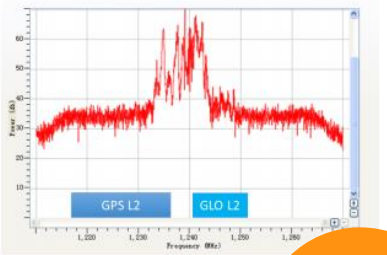


Figure 3: spectrum plot of the L2 band showing from an amateur television transmission

Intentional Jammers

Figure 7: typical in-car chirp jammers (PPDs (Personal Privacy Devices))

http://Jammers.Store

Navigation beacons

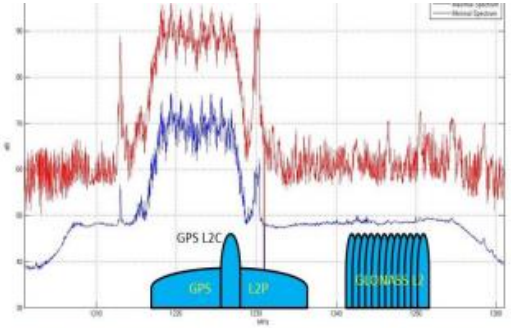


Figure 4: spectrum plot of the L2 band showing the signal from a navigation beacon in relation to the GPS and GLONASS L2 signals

Self-interference

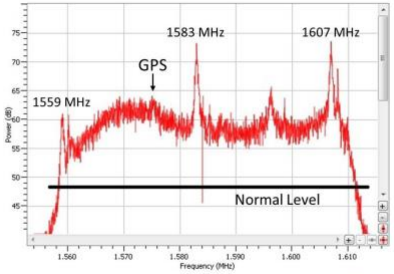


Figure 5: interference from a GoPro Hero 2 video camera picked up by a GNSS antenna

Other communications (Immarsat/Iridium/LTE)

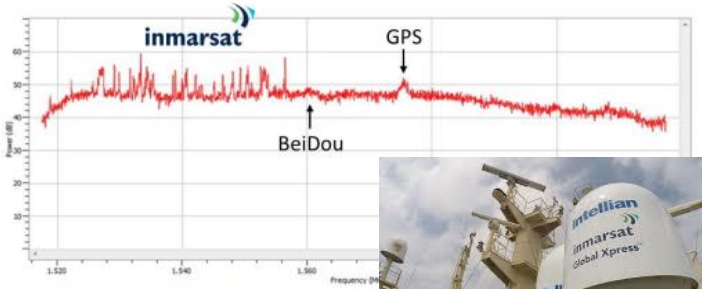
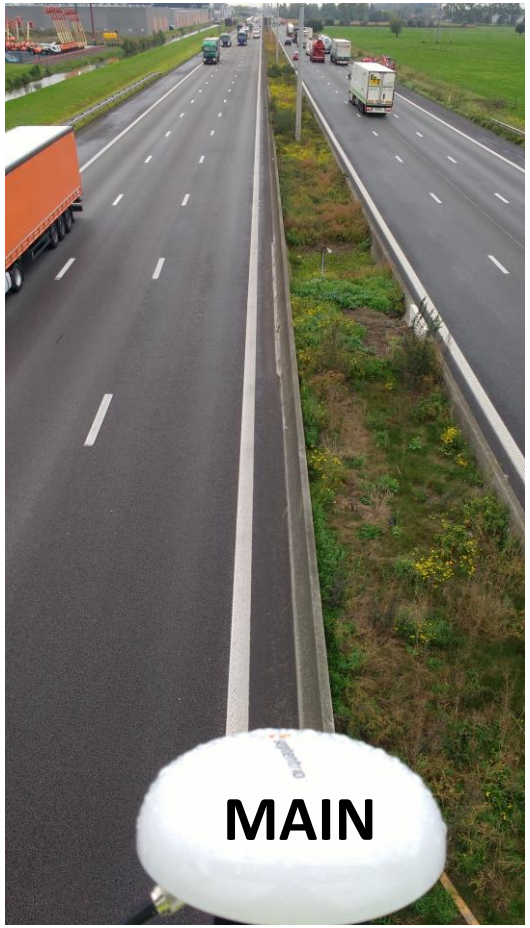


Figure 6: spectrum plot of the L1 band showing the location of transmissions are located at higher frequencies

Set-Up – Interference Lane detection



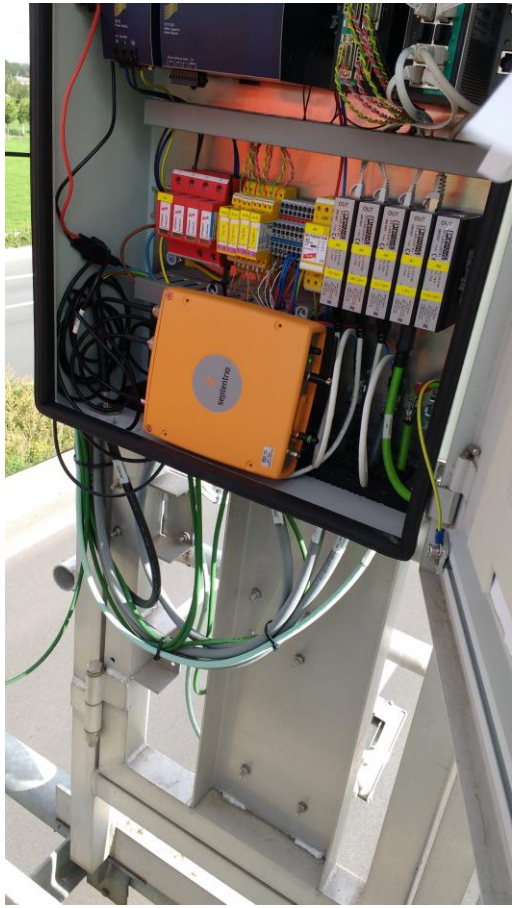
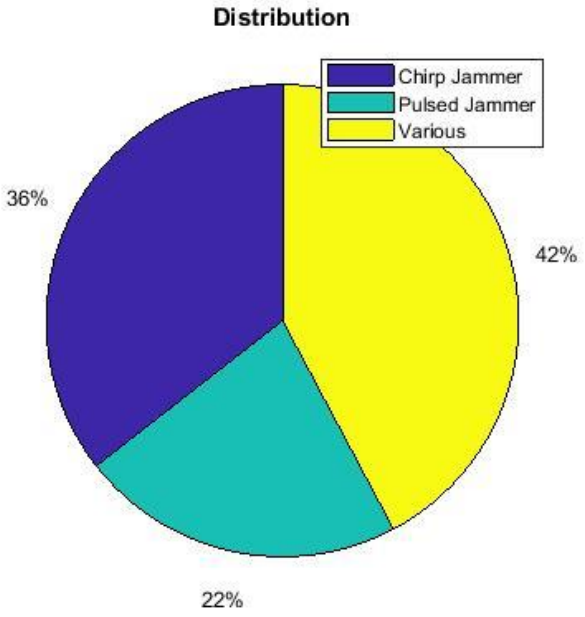


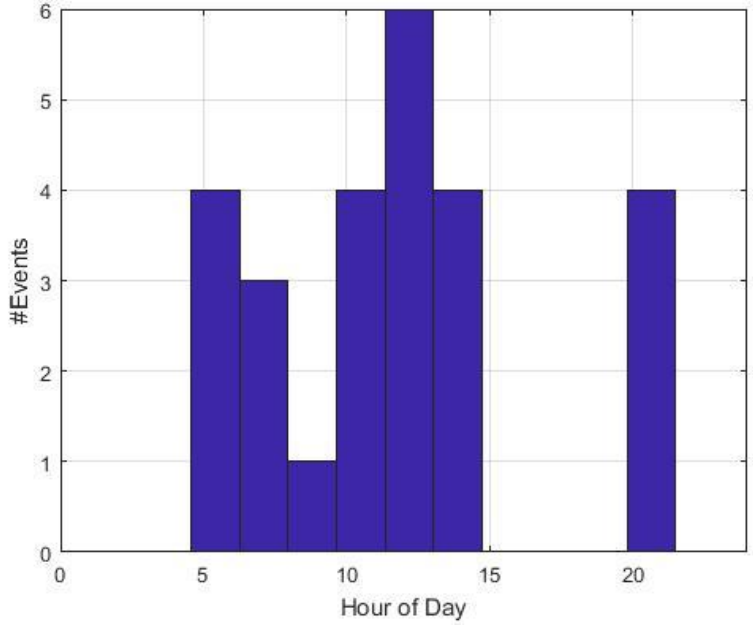
Figure 7: typical in-car chirp jammers (PPDs (Personal Privacy Devices))

Overview

- **45 Events of Heavy Interference in 4,8 Days**
- **3 Classes**

Figure 7: typical in-car chirp jammers (PPDs (Personal Privacy Devices))

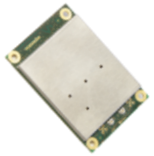


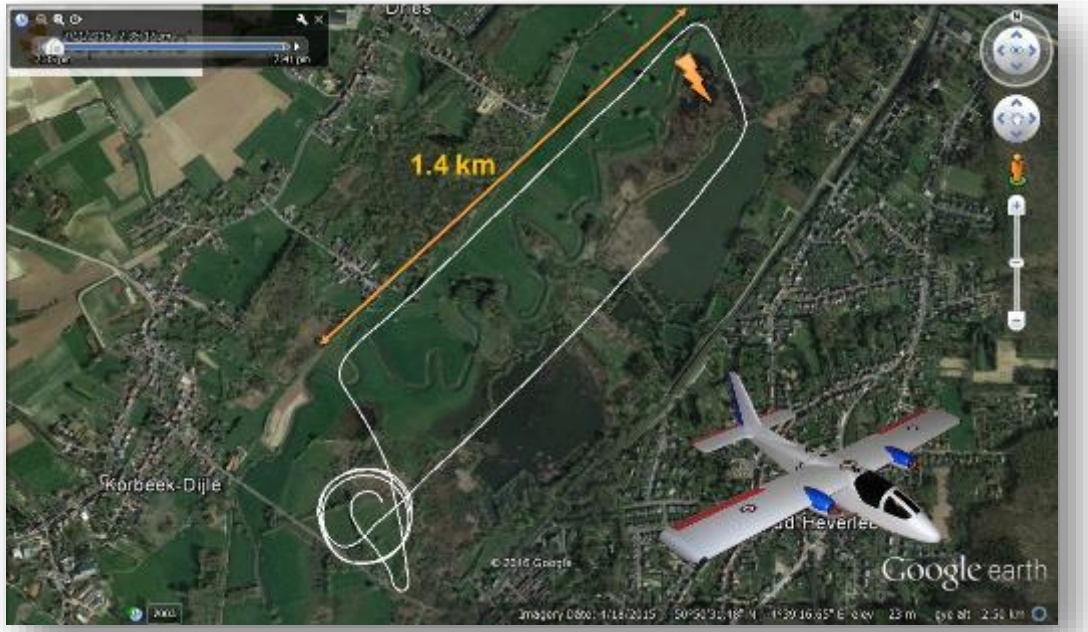


Interference mitigation - Test study

external interference

- **Test done with a Chirp jammer and the following GNSS receivers:**
  - **Septentrio GNSS receiver (AsteRx4)**
    - RTK GPS+GLO
    - L1 stand-alone GPS+GLO
  - **Other High-Precision Receiver**
  - **Consumer grade L1 Receiver**



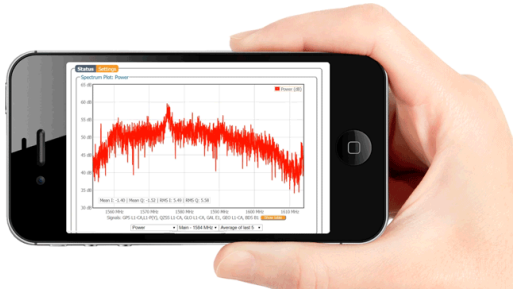


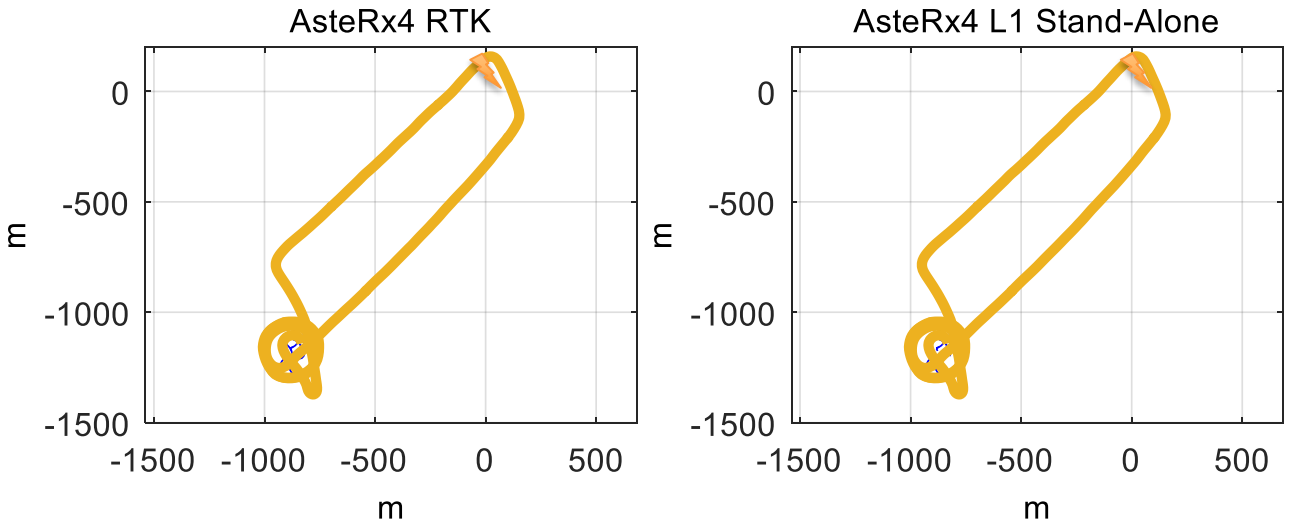
septentrio

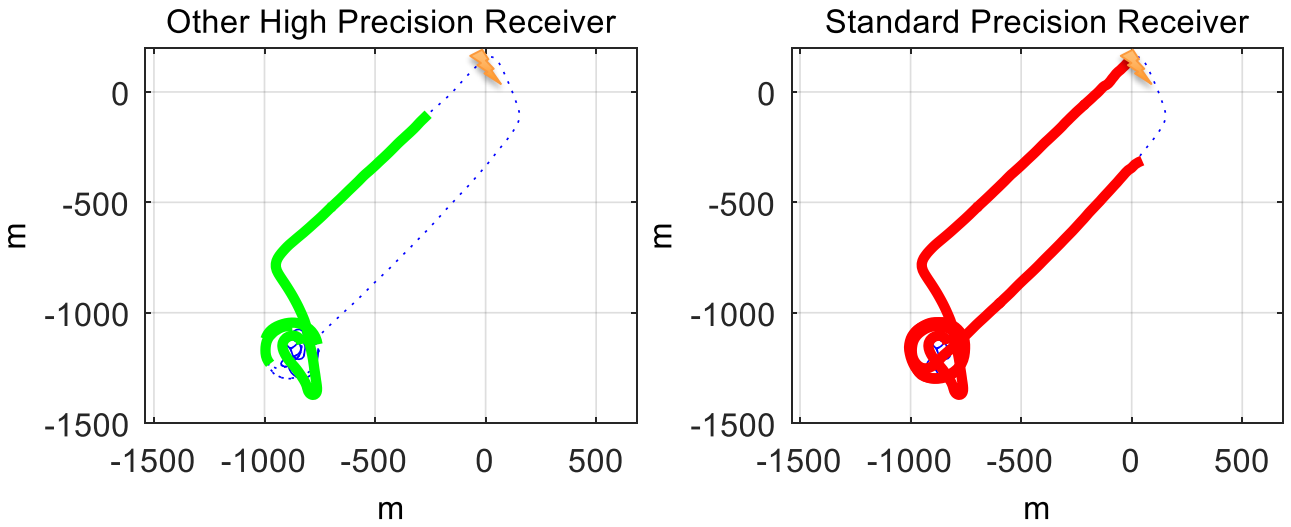
10 mW Commercial L1 Chirp Jammer

external interference

AIM+

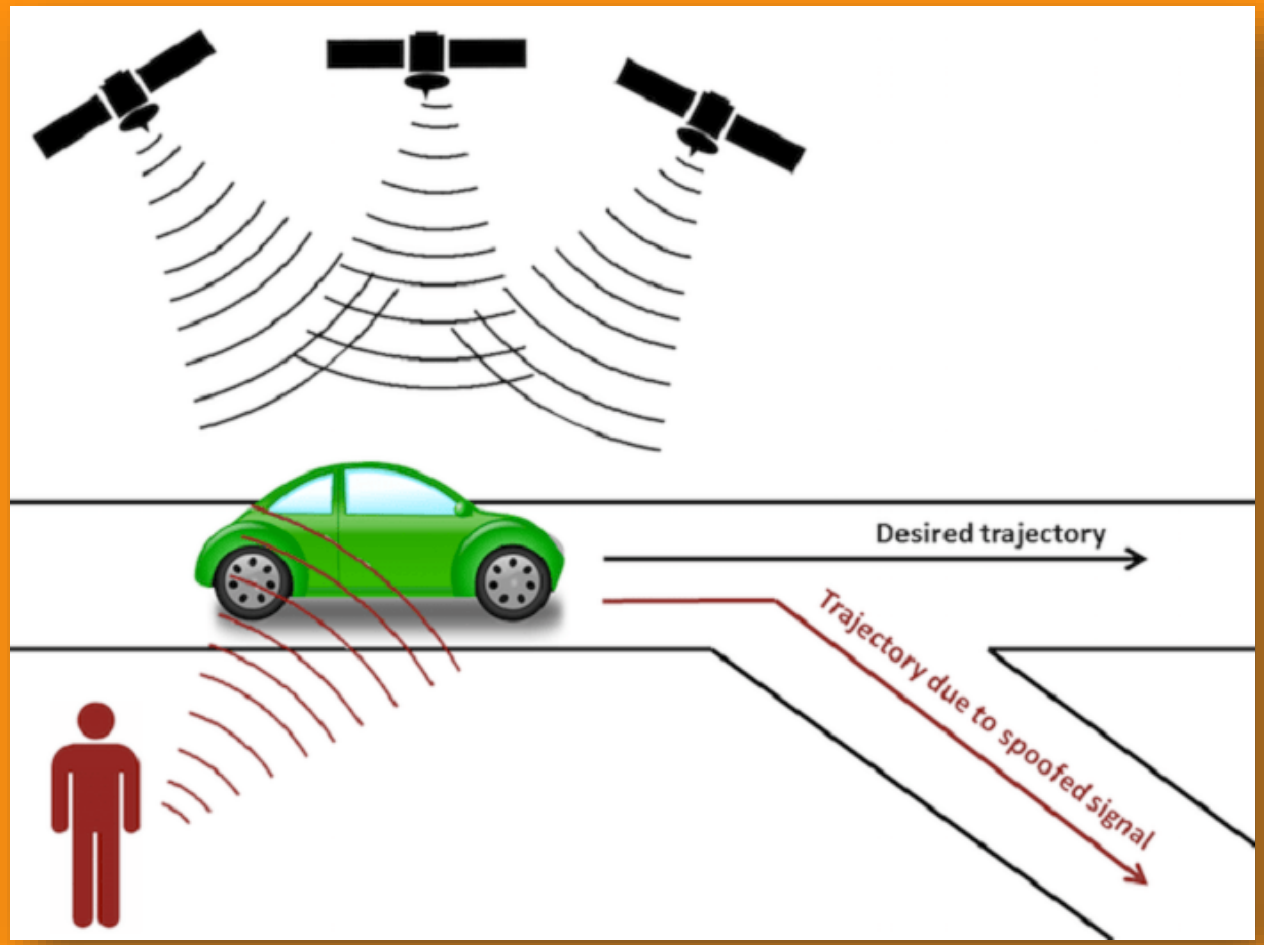


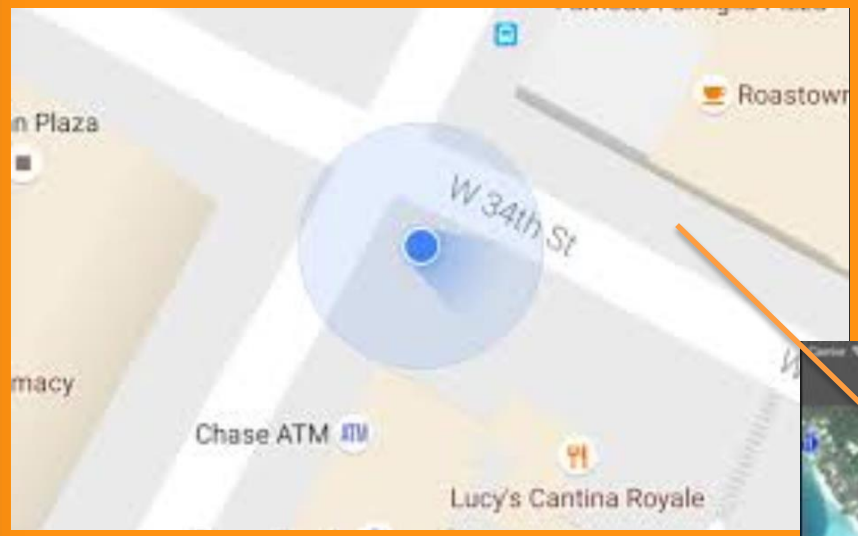


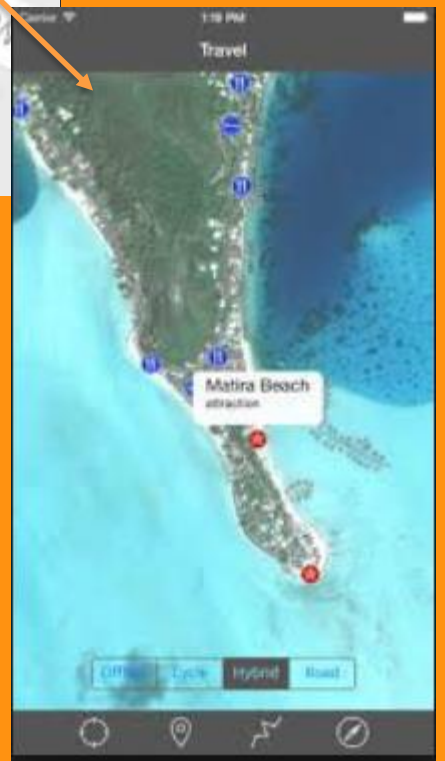


septentrio

Spoofing







septentrio

Cheap & Easy

- (mini-)PC + Software Defined Radio

USB

I/Q Samples

$150 RF

amazon

GPS L1

- Open source software
  - *gps-sdr-sim*
- Even cheaper: USB3.0-to-VGA dongle
  - *osmo-fl2k*

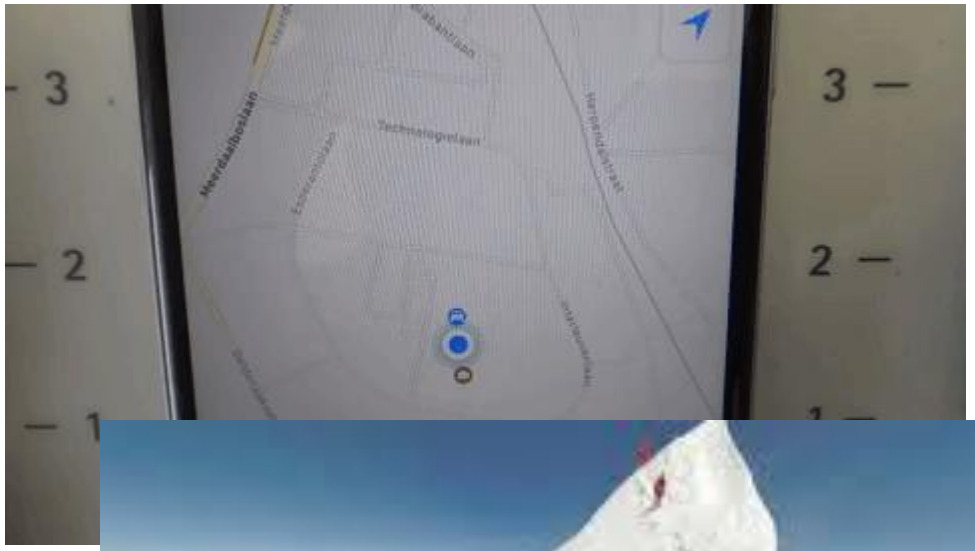
Harmonics @ GPS

$5

Wire antenna

septentrio

iPhone 6 under Attack



- Very Easily Spoofed
  - Even with Pico Watts

General Anti-Spoofing Coutermeasures

TIME/POSITION SHIFT

- Can be detected
- Alignment still possible with real time or position signals

ACCURATE CLOCKS

- HW design needs to consider high quality clocks

MULTI-FREQ MULTI-CONSTELLATION

- Backup signals
- Receivers need to be able to keep other signals alive

GNSS/INS

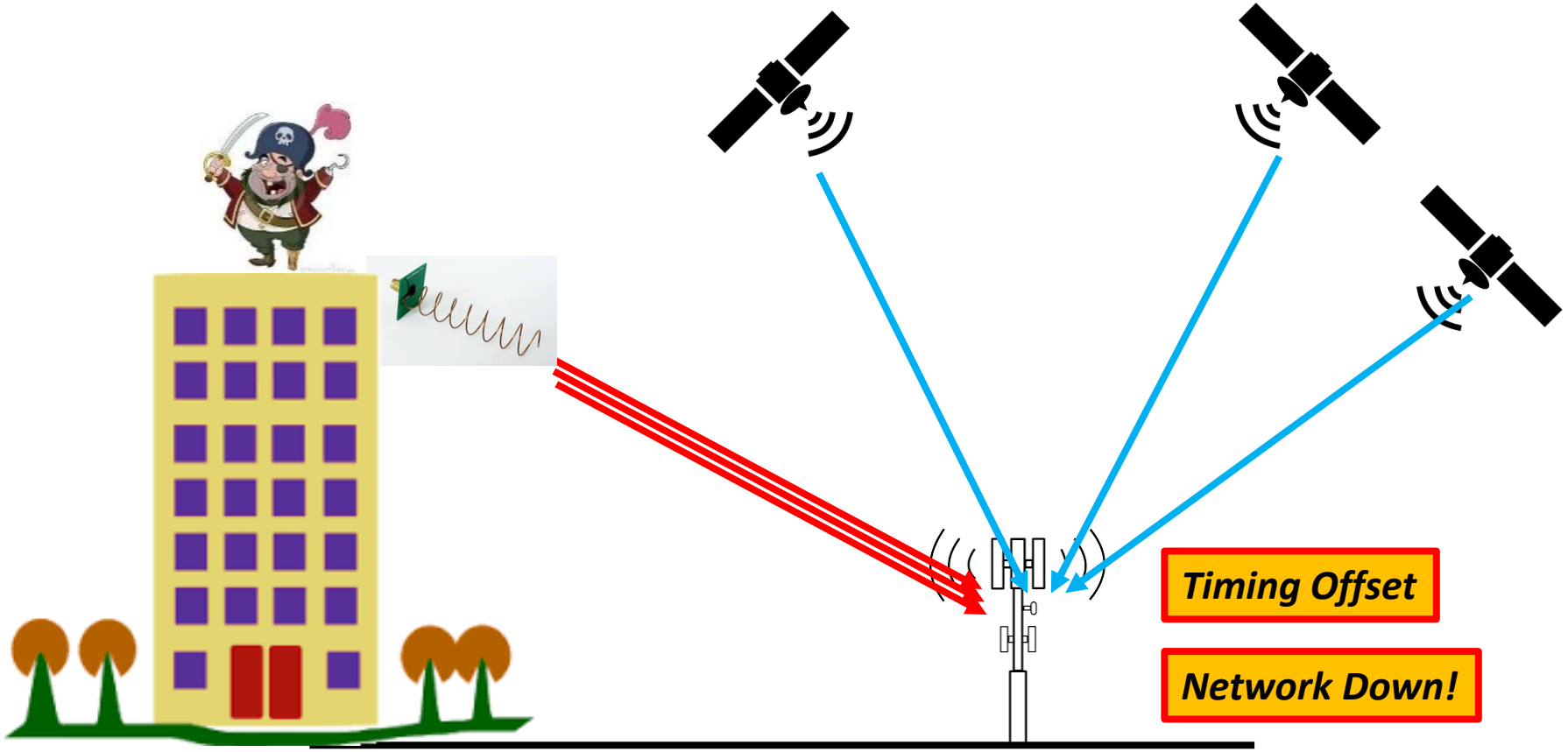
- Proper usage of IMUs

MESSAGE AUTHENTICATION

- GAL OSNMA
- GPS Chimera
- Signal readiness is important
- CPU will be important

septentrio

What about different types of spoofers?



septentrio

Regular Spoofing Attack Mitigation

- Look for anomalies in the signal

GPS L1

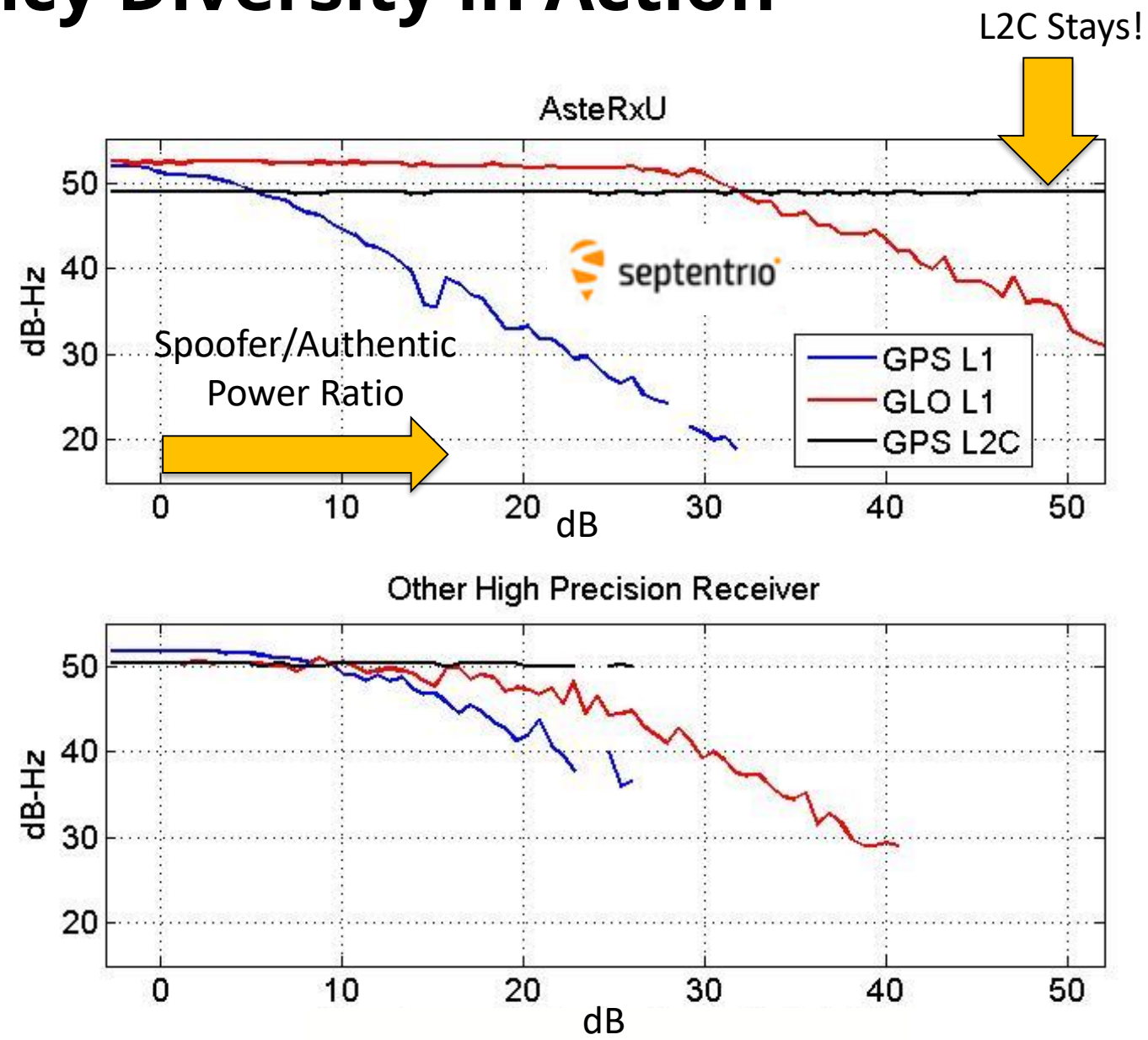
Missing Signals?
Inconsistent Signals?
Clock Anomalies?
Spectral Anomalies?
Navdata Issues?
...

Spoofing Detected!

SBF::RFStatus → spoofing likely

septentrio

Frequency Diversity in Action

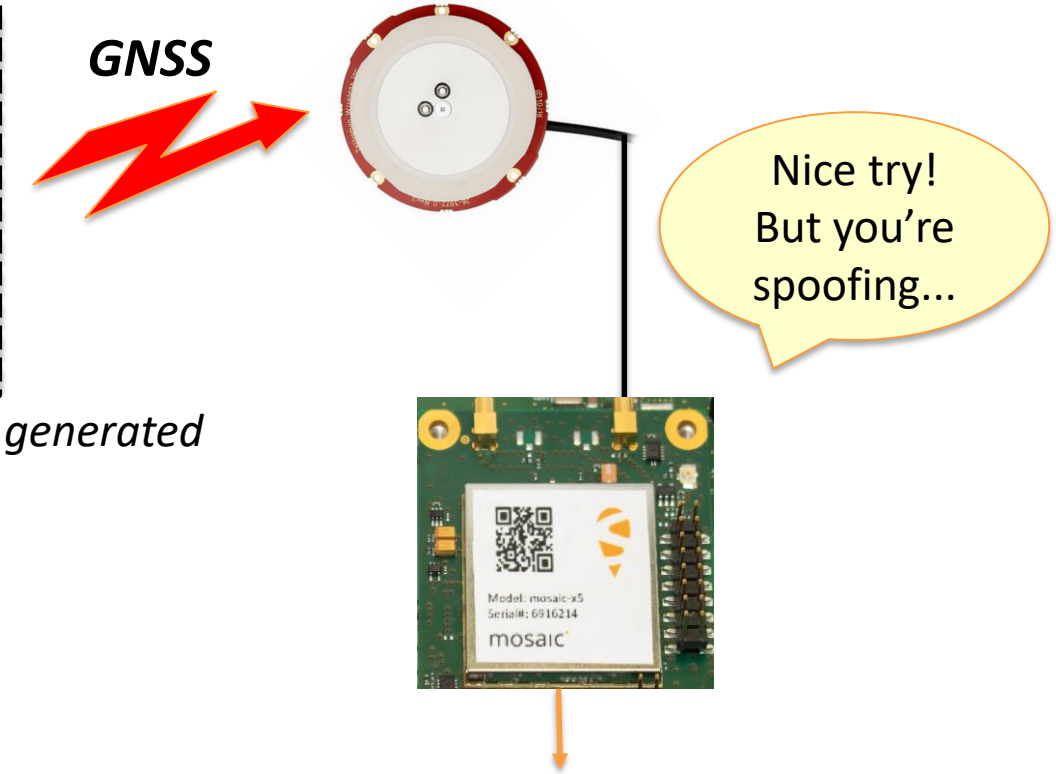


septentrio

Making it more difficult…

- Use high-end GNSS constellation generator

All signals, including military, cleanly generated

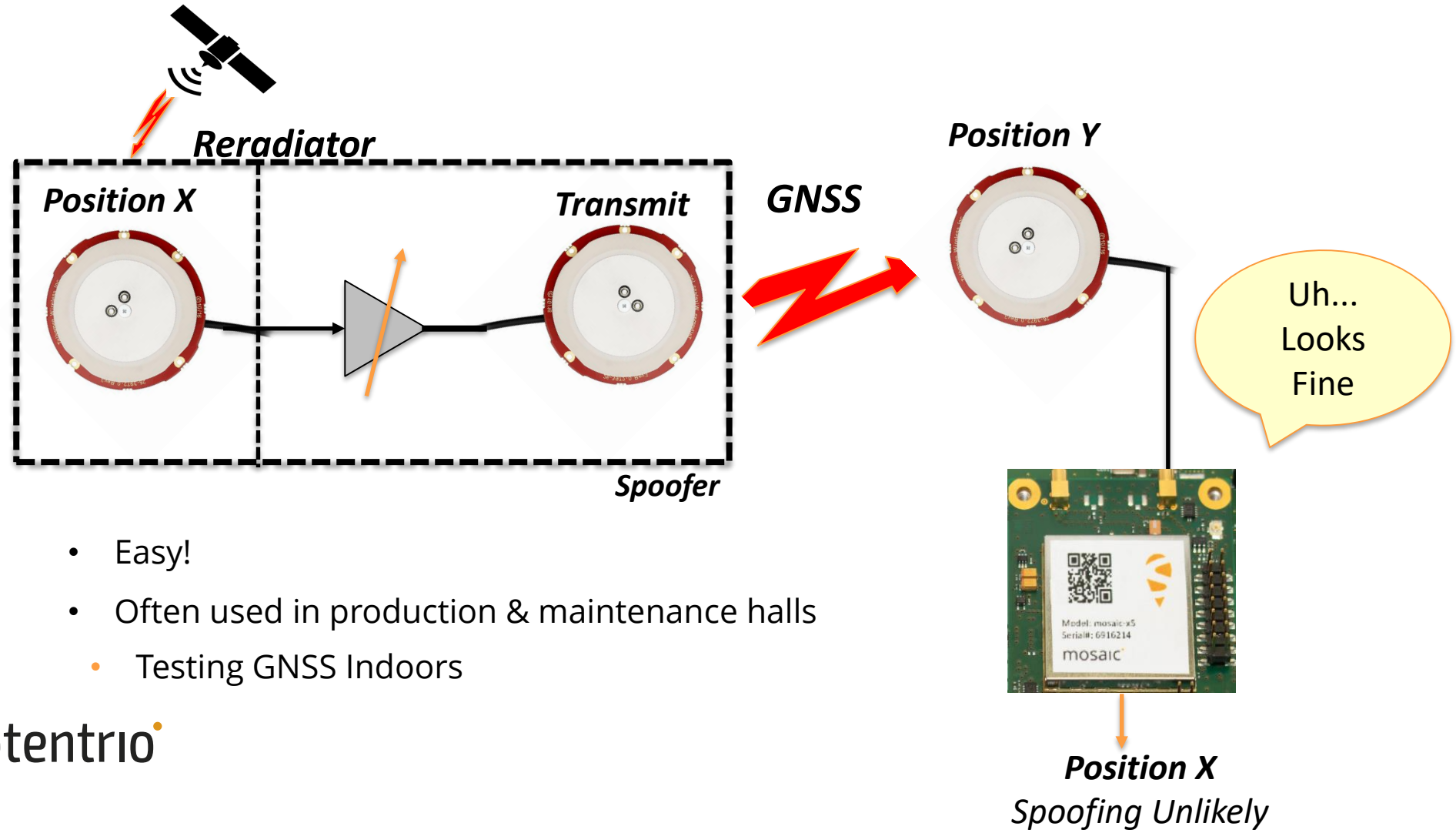


SBF::RFStatus → spoofing likely

septentrio

Making it even more difficult…

- Reradiate actual GNSS from other location or with small time delay

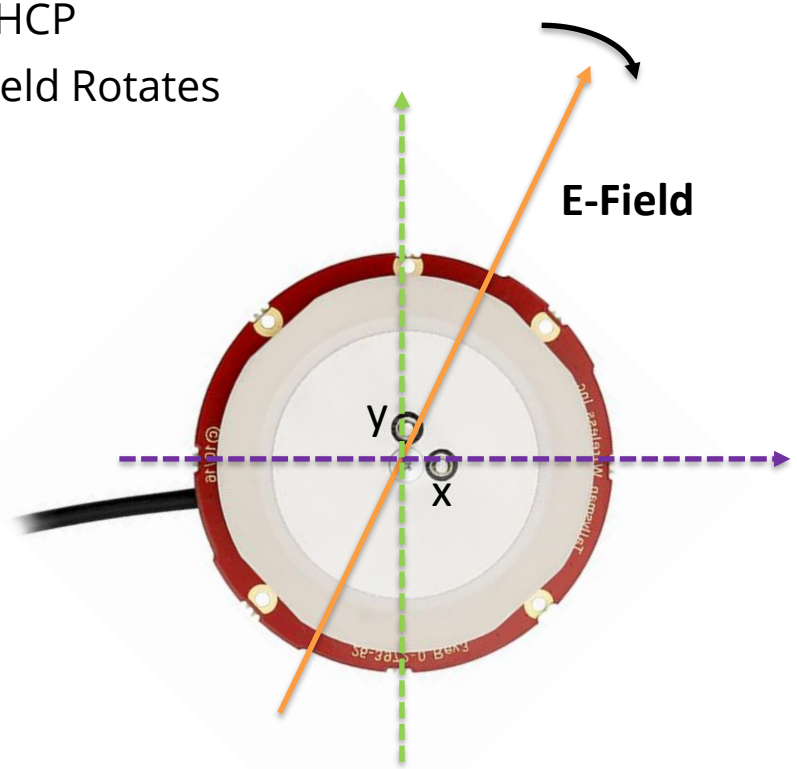


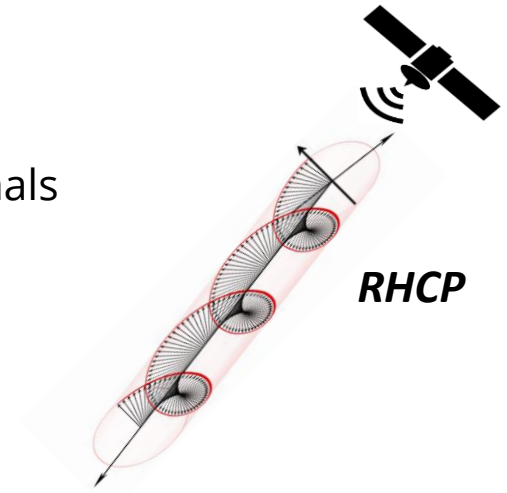
- Easy!
- Often used in production & maintenance halls
  - Testing GNSS Indoors

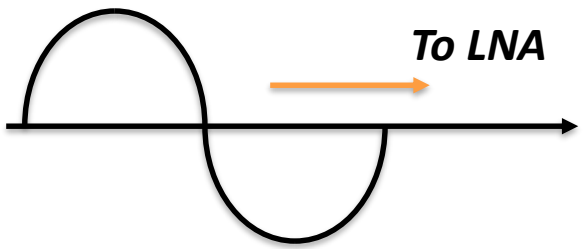
septentrio

EM Field Property: Polarization

- Satellites Transmit **R**ight **H**and **Ci**rculary **P**olarized Signals
  - RHCP
  - Field Rotates





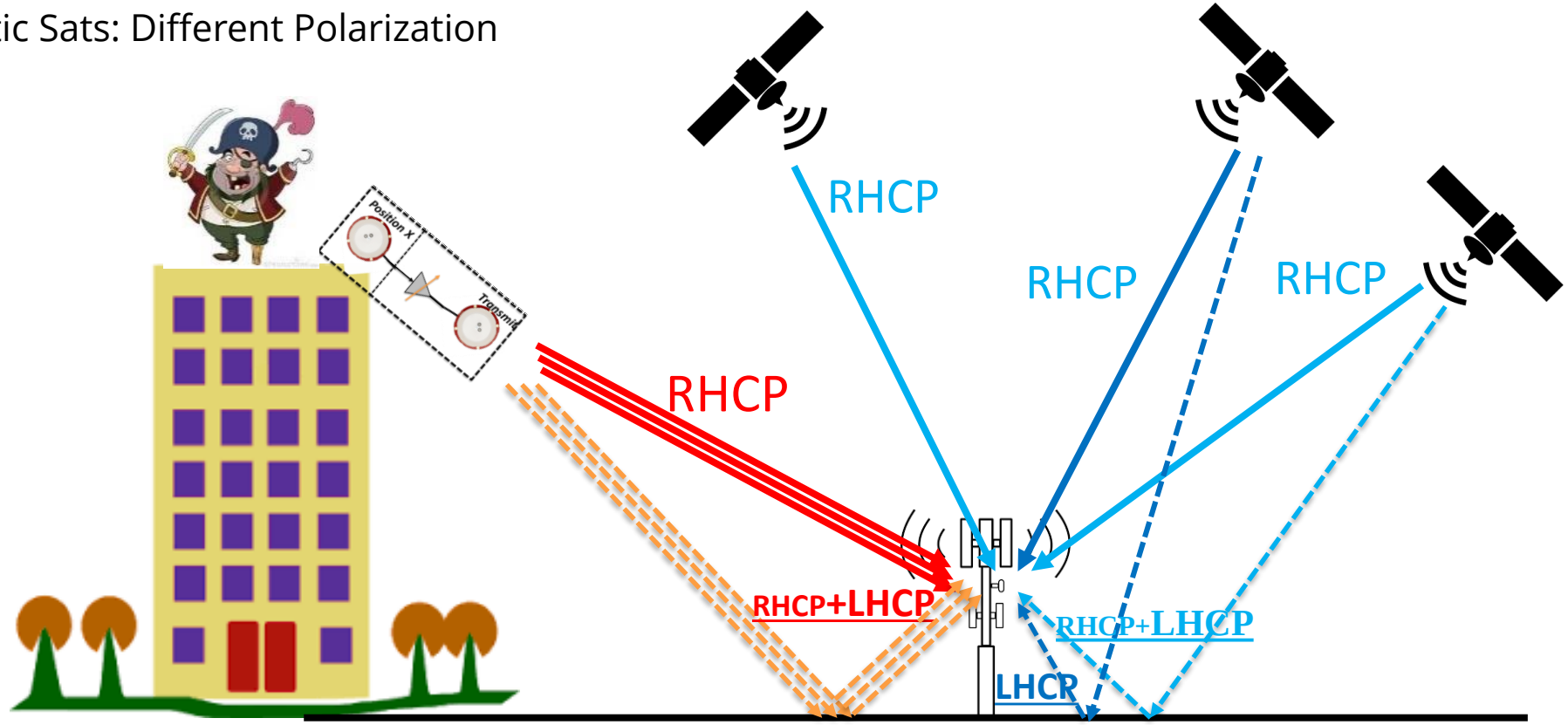


How about Left Hand (LHCP)?
→Just reverse shift
→ Signal already available in many antennas

septentrio

Difference Between Spoofed and Authentic Satellites

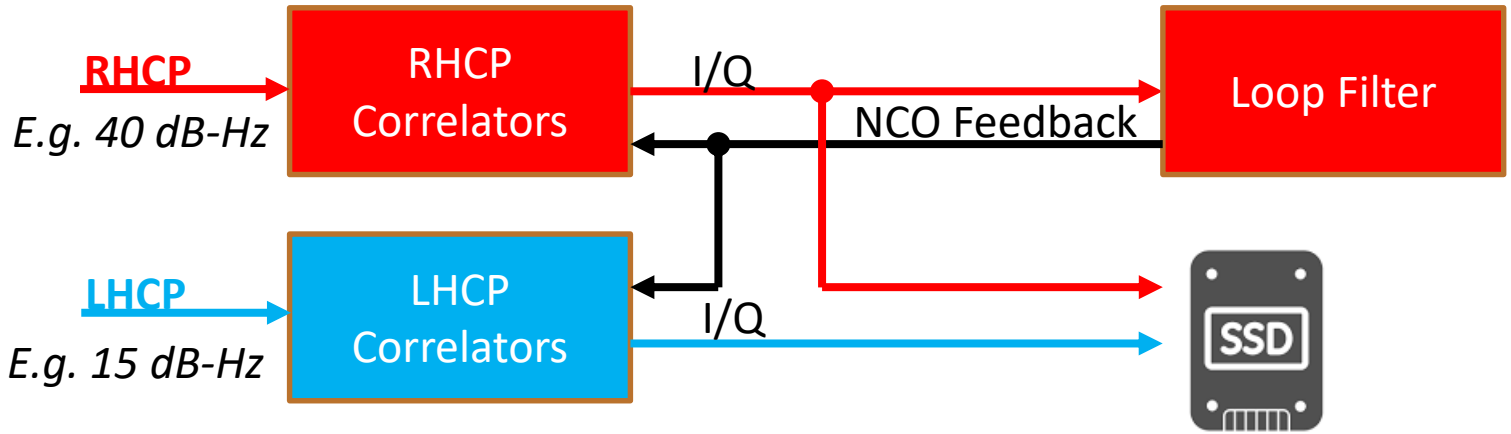
- Spoofed Sats: Same Polarization
- Authentic Sats: Different Polarization



Reflection changes polarization

Septentrio's Polarization-Aware Receiver Prototype

- Permanent Monitoring of RHCP and LHCP
  - *Aided Tracking of LHCP to Capture Polarization at low C/No*

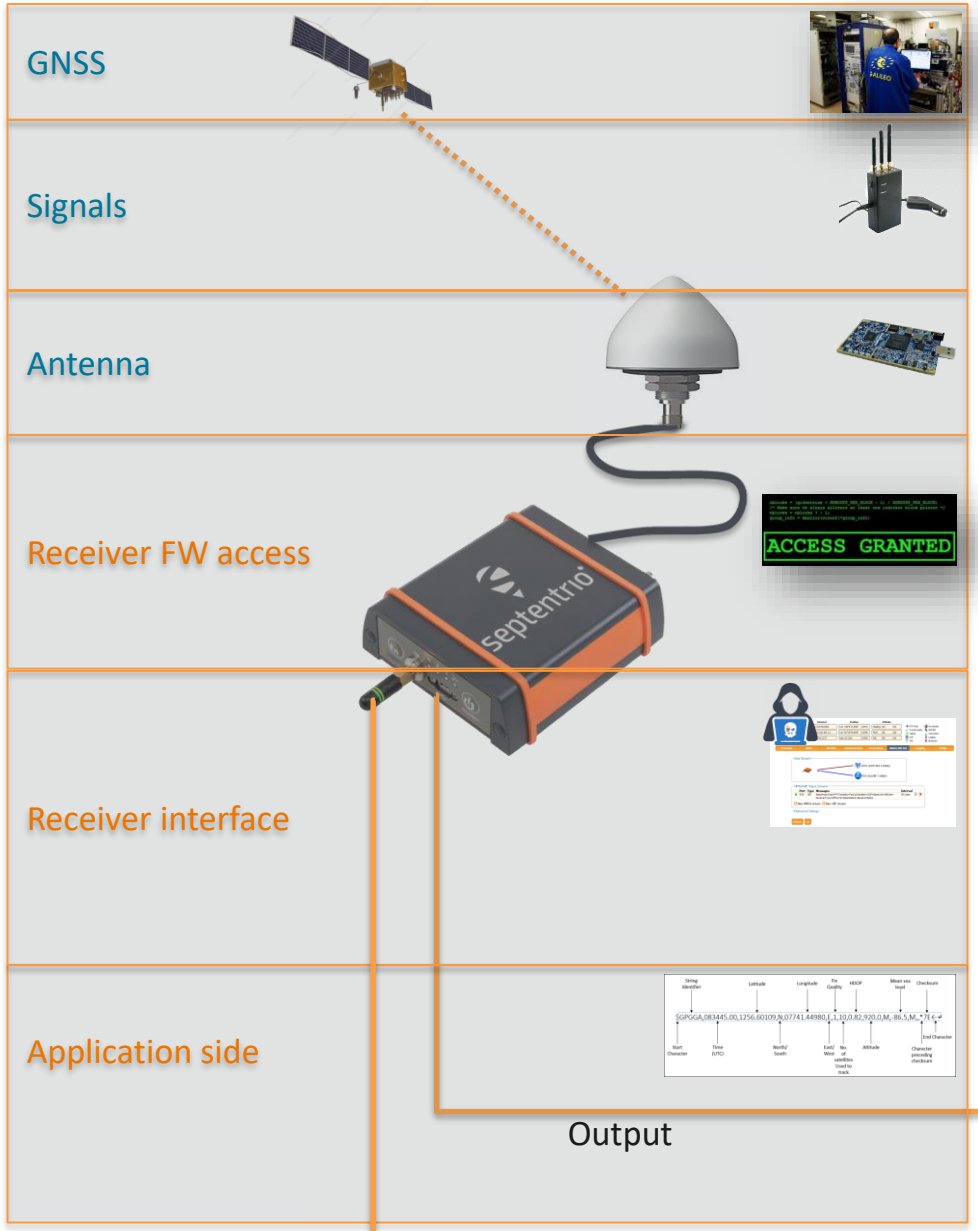


FANTASTIC
FIELD AWARE NAVIGATION AND TIMING AUTHENTICATION SENSOR FOR TIMING INFRASTRUCTURE AND CENTIMETER LEVEL POSITIONING

European Global Navigation Satellite Systems Agency

septentrio

Is not only about
Spoofing & Jamming



Satellite or control segment malfunctions

Unintentional interference

- Radio-frequency interference (RFI) from external sources
- Testing at system level
- Ionospheric influence (solar maxima, magnetic storms, scintillations)
- Multipath

Intentional interference

- Jamming
- Spoofing (false signals into the receiver)
- Meaconing (interception and re-broadcast of navigation signals).

Receiver FW access

- Hacking into root access (admin)
- Upgrading receiver with different FW
- Loading extra permissions on receiver
- Access to FW for malicious actions (trojan horse)
- Access to uBoot

Receiver Interface

- Access to settings of receiver
- Access to data of receiver
- Access to monitoring of receiver
- Access to users & passwords stored in receiver
- Corrections

Application side

- Intercepting output
- Changing output over communication
- Pretending being someone else

septentrio

Conclusion

- **Good GNSS tracking technology** allows proper resiliance against jamming/spoofing (e.g. Septentrio AIM+)
- Creating a proper anti-spoofing or anti-jamming technique requires:
  - **proper HW/SW design**
- Latest spoofing detection on polarization is **capable to detect** very accurately generated spoofing signals (e.g. reradiators)

→Awareness is critical in society

septentrio

septentrio

EMEA (HQ)

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

Americas

Los Angeles, **USA**

Asia-Pacific

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

septentrio.com

sales@septentrio.com