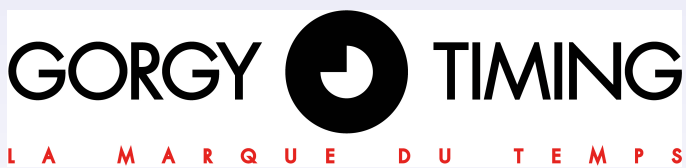
Time transfer and Global Navigation Satellite Systems (GNSS) spoofing, spoofing detection & spoofing cancellation

J.-M Friedt[1], W. Feng[2], G. Goavec-Merou[1], F. Meyer[3]

[1] FEMTO-ST/temps-fréquence & FAST-LAB, Besançon
[2] Xidian University, Xian (China)
[3] OSU Théta/Observatoire de Besançon & FAST-LAB, Besançon
jmfriedt@femto-st.fr



slides at `jmfriedt.free.fr/fosdem2019_gps.pdf`
presentation at `video.fosdem.org/2019/AW1.120/sdr_gps.mp4`

sequel to "Software Defined Radio for processing GNSS signals (FOSDEM 2015)"

GNSS jamming

Jamming:

- North Korea [1], truck drivers [2] [3]
- military will jam GPS: "A 1-kilowatt jammer can block a military GPS receiver from as far away as 80 kilometers. A Russian company recently marketed a 4-[?k?]watt jammer that can deny a standard GPS signal within up to 200 kilometers."[4]
- Russian military [5]
- 9 euro jammer on Amazon $\longrightarrow$
  VCO controlled by a triangle shaped signal sweeping 1.55 to 1.59 GHz jams GPS
  ($\neq$ blocker !) – no emission on GPS L2

[1] www.wired.com/2011/03/north-korea-jams-gps-in-war-game-retaliation/

[2] www.economist.com/technology-quarterly/2011/03/12/no-jam-tomorrow

[3] *Son brouilleur GPS bloque l'aéroport de Nantes* at paris.maville.com/actu/actudet_-son-brouilleur-gps-bloque-l-aeroport-de-nantes_54028-3258706_actu.Htm

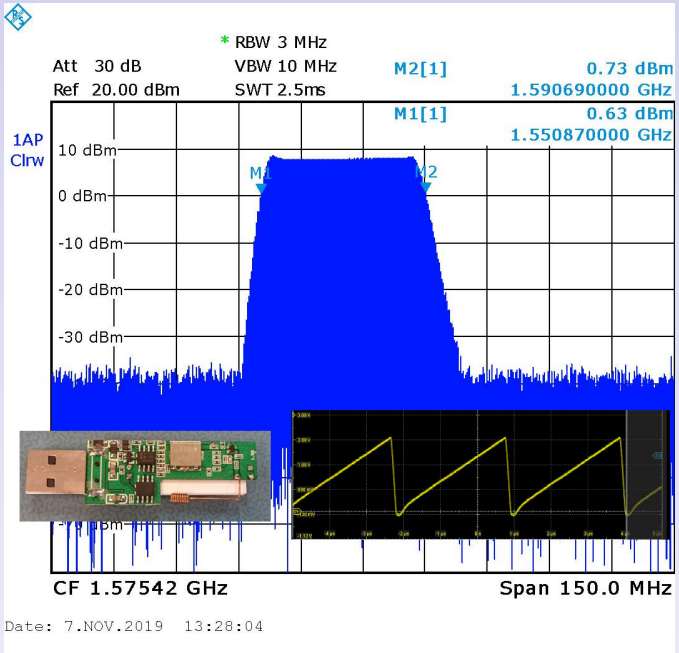
[4] www.afcea.org/content/?q=node/481, 2001

[5] thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark with the establisement of "Northern Fleet Center of Radio-Electronic Warfare (TsREB) in the Murmansk region", jamestown.org/program/russias-new-electronic-warfare-capabilities-in-the-arctic/

GNSS jamming

Jamming:

- North Korea [1], truck drivers [2] [3]
- military will jam GPS: "A 1-kilowatt jammer can block a military GPS receiver from as far away as 80 kilometers. A Russian company recently marketed a 4-[?k?]watt jammer that can deny a standard GPS signal within up to 200 kilometers."[4]
- Russian military [5]
- 9 euro jammer on Amazon $\longrightarrow$
  10 mW output = 1.5 km range if jamming signal is 10 dB above GPS (assuming GPS compression rejects noise by 30 dB)



[1] www.wired.com/2011/03/north-korea-jams-gps-in-war-game-retaliation/

[2] www.economist.com/technology-quarterly/2011/03/12/no-jam-tomorrow

[3] *Son brouilleur GPS bloque l'aéroport de Nantes* at paris.maville.com/actu/actudet_-son-brouilleur-gps-bloque-l-aeroport-de-nantes_54028-3258706_actu.Htm

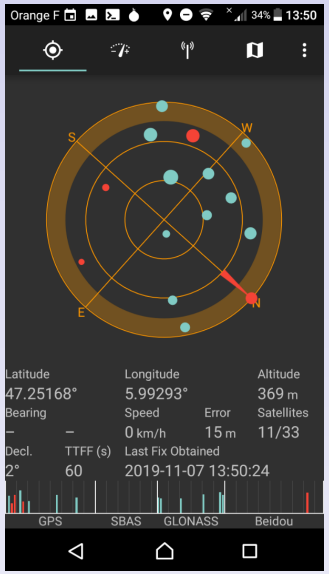
[4] www.afcea.org/content/?q=node/481, 2001

[5] thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark with the establisement of "Northern Fleet Center of Radio-Electronic Warfare (TsREB) in the Murmansk region", jamestown.org/program/russias-new-electronic-warfare-capabilities-in-the-arctic/

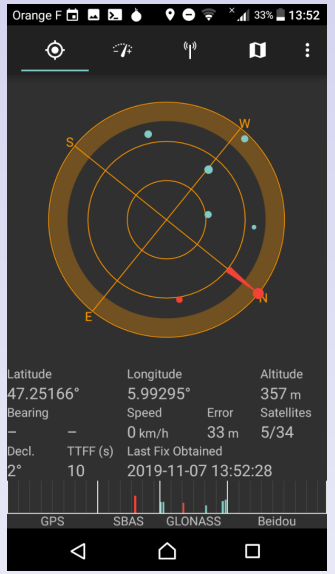
GNSS jamming

Jamming:

- North Korea [1], truck drivers [2] [3]
- military will jam GPS: "A 1-kilowatt jammer can block a military GPS receiver from as far away as 80 kilometers. A Russian company recently marketed a 4-[?k?]watt jammer that can deny a standard GPS signal within up to 200 kilometers."[4]
- Russian military [5]
- 9 euro jammer on Amazon $\longrightarrow$ GLONASS (1602.0-–1615.5 MHz) hardly affected



No jamming



Jamming

[1] www.wired.com/2011/03/north-korea-jams-gps-in-war-game-retaliation/

[2] www.economist.com/technology-quarterly/2011/03/12/no-jam-tomorrow

[3] *Son brouilleur GPS bloque l'aéroport de Nantes* at paris.maville.com/actu/actudet_-son-brouilleur-gps-bloque-l-aeroport-de-nantes_54028-3258706_actu.Htm

[4] www.afcea.org/content/?q=node/481, 2001

[5] thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark with the establisement of "Northern Fleet Center of Radio-Electronic Warfare (TsREB) in the Murmansk region", jamestown.org/program/russias-new-electronic-warfare-capabilities-in-the-arctic/

GNSS spoofing

Spoofing attacks ?

- A US UAV lands in Iran [6]
- Russian GPS spoofing in Crimea [7], Murmansk [8], Syria [9], Moscow [10] (locating the Kremlin close to an airport will force a UAV to land) or near V. Putin [11]
- Recent spoofing reports in port of Shanghai [12]

---

[6] en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

[7] liveuamap.com/en/2019/28-march-study-on-russian-gps-spoofing-tens-of-ships-passing, www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

[8] www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[9] www.popularmechanics.com/military/weapons/a28250133/russia-gps-signals-israel/

[10] money.cnn.com/2016/12/02/technology/kremlin-gps-signals/index.html

[11] c4ads.org/s/Above-Us-Only-Stars.pdf summarized in foreignpolicy.com/2019/04/03/russia-is-tricking-gps-to-protect-putin/ or *Study maps "extensive Russian GPS spoofing"* at www.bbc.com/news/technology-47786248

[12] https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai and https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

GPS in the context of IoT

- "This document proposes an application layer messaging package running over LoRaWAN to synchronize the real-time clock of an end-device to the network's GPS clock with second accuracy. Synchronizing the end-device(s) clock is very useful of many applications like ..." [13]
- "Onboard GPS uBlox Max7W receiver and GPS antenne equipped with GPS time-sync which is needed for class-B operation" [14]
- "1M2M's ED1608 is an out of the box, ready to use universal Low Power WAN Smart Sensor/GPS Tracker. It has on board 3D accelerometer, GPS, temperature..." [15]

[13] LoRaWAN Application Layer Clock Synchronization Specification v1.0.0 https://lora-alliance.org/resource-hub/lorawanr-application-layer-clock-synchronization-specification-v100 (2018)

[14] Modular outdoor IoT gateway specifications at https://abigo4u.com/en/modular-outdoor-iot-gateway.html

[15] 1M2M ED1608 description at https://lora-alliance.org/lorawan-certified-products

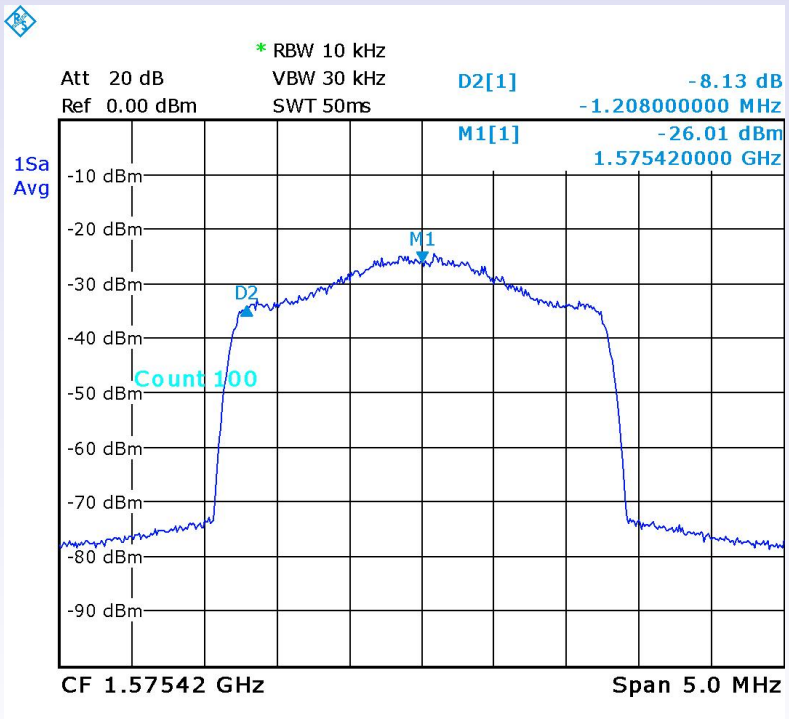
SDR spoofing demonstration

- Analog Devices PlutoSDR: AD9363 (70–6000 MHz) frontend + Zynq SOC
- Collect NAV ephemeris from the internet [16] to simulate existing constellation (period = 12 h ⇒ NAV will be valid for a couple of hours)
- Generate NAV messages for the satellites in view of the receiver (spoof for a region not too far from real location)
- Emit the signal at a level reasonably close but stronger than real signal
- Works easily with mobile phone/consumer electronics
- Insufficient LO stability for higher grade GPS (e.g. cars): replace TCXO with proper OCXO for long term stability

[16] constellation characteristics ⇒ location independent

Spoofing tools

- PlutoSDR emitter : 0 dBm output spread over 2 MHz bandwidth (1023 Mb/s) $\Rightarrow$ 30 dB peak power drop
- Software [17] running on the host PC synthesizing the I/Q coefficients streamed to the modulator, generating navigation messages representative of the simulated constellation (Zynq does not seem powerful enough for real time I/Q generation)



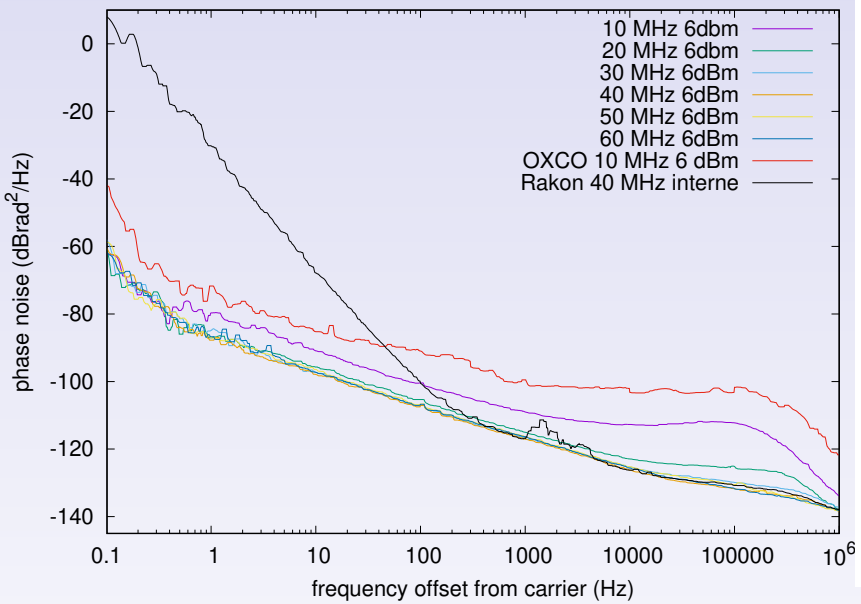
Range of the attack:
RX power [1]
$P_{rcv} \geq -130 + 10$ dBm
FSPL @ 1575.42 MHz
$= 20\log_{10}(d) + 36$ dB $\Rightarrow$
$-120 = TX_{dBm} - FSPL$ or
$20\log_{10}(d) = 84 + TX$
$d \leq 10^{84/20} = 16$ km @ 0 dBm
$\Rightarrow d \leq 500$ m @ -30 dBm
$\Rightarrow d \leq 150$ m @ -40 dBm
in free space

Global Positioning System Standard Positioning Service Signal Specification, p.14 (1995)

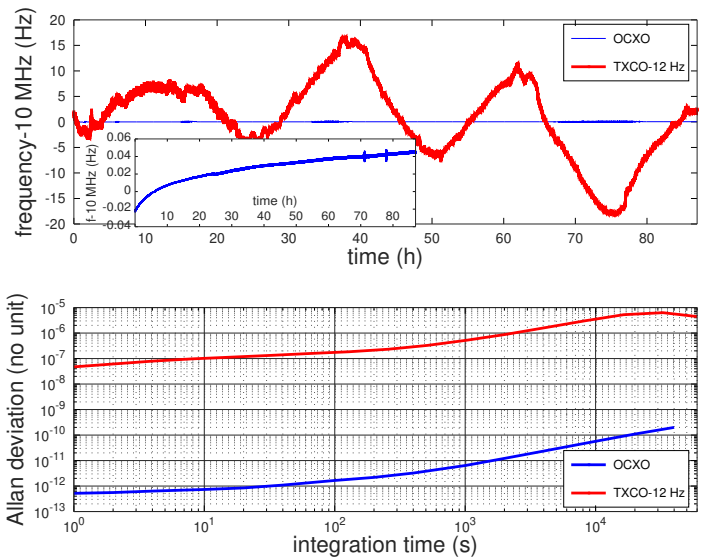
[17] github.com/Mictronics/pluto-gps-sim based on Takuji Ebinuma's github.com/osqzss/gps-sdr-sim

Embedded solution: replacement of the 40 MHz TCXO with a 10 MHz OCXO

Oscillator stability: short term v.s long term stability (phase noise v.s Allan deviation)



Phase noise with carrier frequency

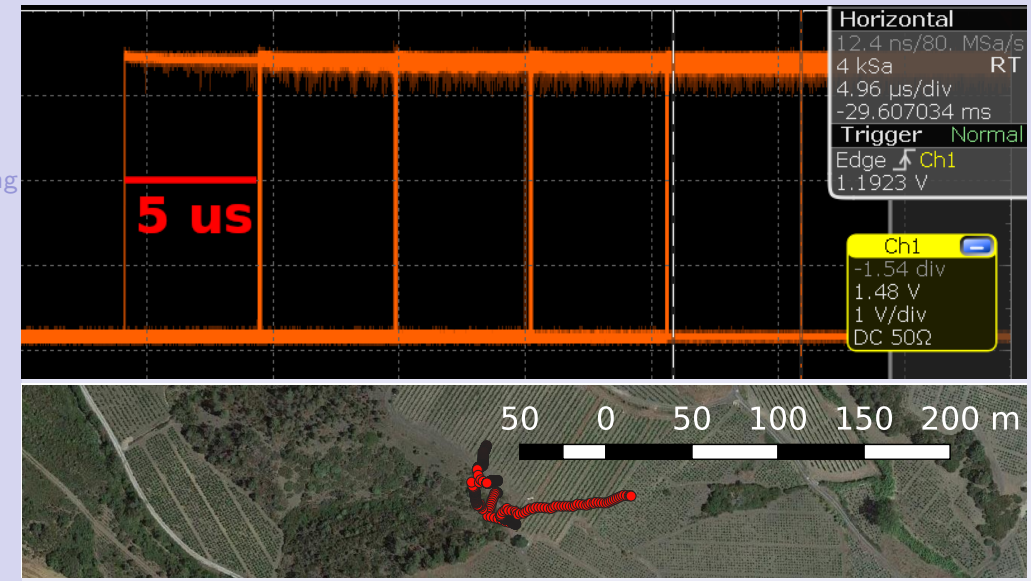


TCXO v.s OCXO

Much improved long term stability but degraded short-term stability (>100 Hz from carrier) ⇒ ideally, generate a clean 40 MHz from the 10 MHz reference

Beyond positioning: timing signal

Many high-grade oscillators rely on GPS for long-term stabilization ("radio-controlled watches")



Never actively tune an atomic clock: measure offset and drift and share information with user
⇒ time offset defined by a constant (AF0), linear (AF1) and quadratic (AF2) offset.
⇒ **dynamically change these parameters** in the NAV messages of all satellites

```
  clk[0] = eph.af0 + tk * (eph.af1 + tk * eph.af2) + relativistic - eph.tgd;
  clk[1] = eph.af1 + 2.0 * tk * eph.af2;
...
  // Subframe 1
...
  sbf[0][5] = 0UL;
  sbf[0][6] = (tgd & 0xFFUL) << 6;
  sbf[0][7] = ((iodc & 0xFFUL) << 22) | ((toc & 0xFFFFUL) << 6);
  sbf[0][8] = ((af2 & 0xFFUL) << 22) | ((af1 & 0xFFFFUL) << 6);
  sbf[0][9] = (af0 & 0x3FFFFFUL) << 8;
```

is updated with

```
for (i = 0; i < MAX_CHAN; i++) { // Generate new subframes if allocated
    if (chan[i].prn != 0)
      {eph[ieph][chan[i].prn-1].af0 += 5 * pow(10,-6);   // add 5 us to AF0 every 2 mins
       eph2sbf(eph[ieph][chan[i].prn - 1], ionoutc, chan[i].sbf);
      }
}
```

Spoofing detection [18]

- Detect excessive power or unrealistic Doppler shifts: U-Blox receivers
- Proper signal generation will fool such strategies
- Our approach: analyze the raw RF signal for unrealistic characteristics

A constellation is spatially distributed, a spoofer is located at a single point ⇒ antenna array measurement and angle of arrival measurement

---

[18] R.G. Hartman, *Spoofing detection system for a satellite positioning system*, Patent US5557284A (1995):
A **pair of antennae** *in combination with a GPS signal receiver system is employed for detecting the reception of satellite information signals from a spoofing signal transmitter as opposed to those satellite information signals transmitted aboard each of the satellite vehicles which form a satellite positioning system. As described herein, an indication of the* **pointing angle between the antennae and the actual transmitter** *transmitting the satellite information signals is detected. The pointing angle and/or alternatively the range difference may be observed by monitoring the behavior of the pseudo random code associated with the carrier of the satellite information signal, or the carrier itself. In turn, pseudo range measurements, ...*

Codeless analysis

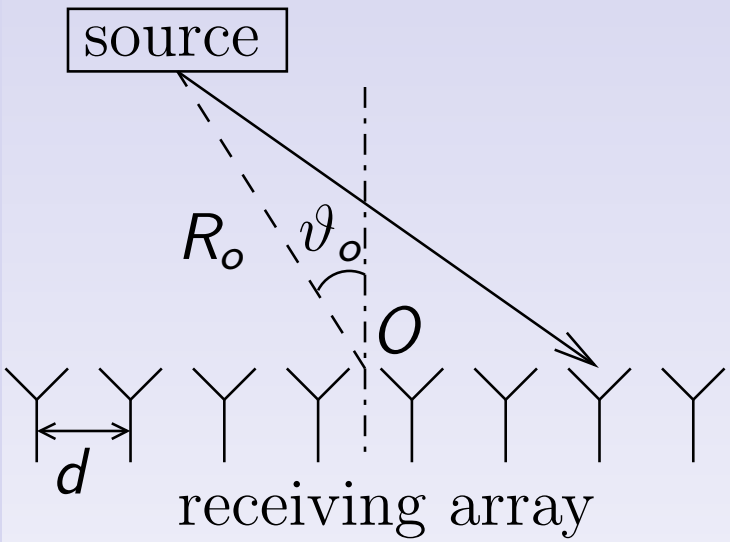
- Code analysis is computationally intensive but provides complete receiver architecture
- Spoofing detection: only analyze $s^2(t)$ which **removes** the BPSK message

$$\text{BPSK: } \varphi \in \{0;\pi\} \Rightarrow \text{BPSK}^2 : \varphi \in \{0;2\pi\} = 0[2\pi]$$

- Satellite identification by different Doppler shift
- Two antennas: add a geometrical term to phase (delay of arrival)
- Direction of arrival by phase difference between antennas (cancels the Doppler from a same satellite): $arg(FFT(s_n^2))$ at the nth antenna

Solution demonstration

Power can be tuned, but **direction of arrival** will be difficult to simulate
⇒ replace single receiving antenna with array for phase analysis [19]



- In the far field ($R_0 \gg 2(Kd)^2/\lambda$) and narrowband ($B \ll c/(Kd)$) approximations, a plane wave hits the antenna array
- the phase shift between elements is $2\pi kd \sin\vartheta/\lambda_0$ for the kth element
- the various satellites with different elevations and azimuth exhibit different ϑ_0 and their signal contribution can be separated by analyzing the phase between antennas of the array

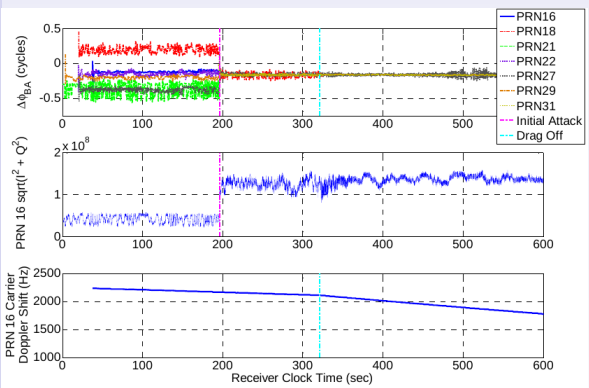


Fig. 15. Indicators of initial capture and drag-off during Libya spoofing attack, as measured by the spoofing detection receiver.

M.A. Psiaki *& al.*, *GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase*, Proc. Radionavigation Laboratory Conference (2014), cited in R. T. Ioannides, T. Pany, & G. Gibbons, *Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques*, Proc. IEEE **104** (6), 1174–1194 (2016). Top=phase, middle=power, bottom=Doppler

[19] $\lambda = 19$ cm $\Rightarrow K = 8$ & $d = \lambda/2 \Rightarrow Kd = 76$ cm: $R_0 > 6$ m & $B \ll 400$ MHz !

Solution demonstration: 2-antennas

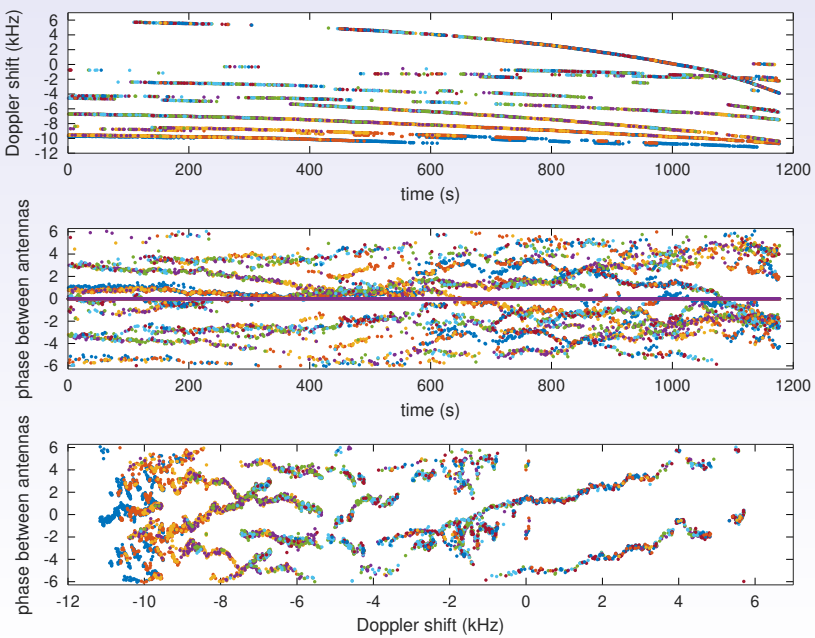
Each antenna a detects the sum of the satellite n signals

$$x_{n,a} \propto \exp\left(j(\underbrace{\delta\omega_n t}_{Doppler} + \underbrace{\varphi_n}_{BPSK} + \underbrace{\varphi_{n,a}}_{geometry}) \right), \varphi_n \in [0, \pi]$$

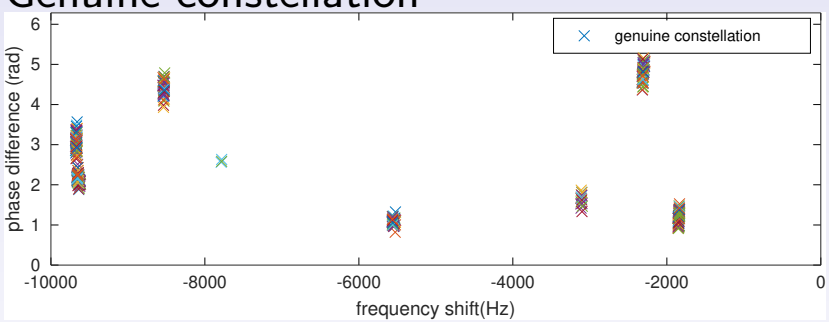
$$\Rightarrow arg(FFT(x_{n,1}^2)) - arg(FFT(x_{n,2}^2)) = \varphi_{n,2} - \varphi_{n,1}$$

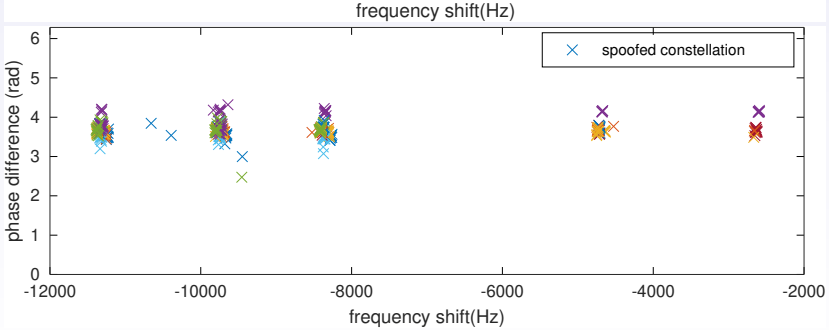
only dependent on antenna geometry and satellite position

Long term Doppler & phase monitoring



Genuine constellation

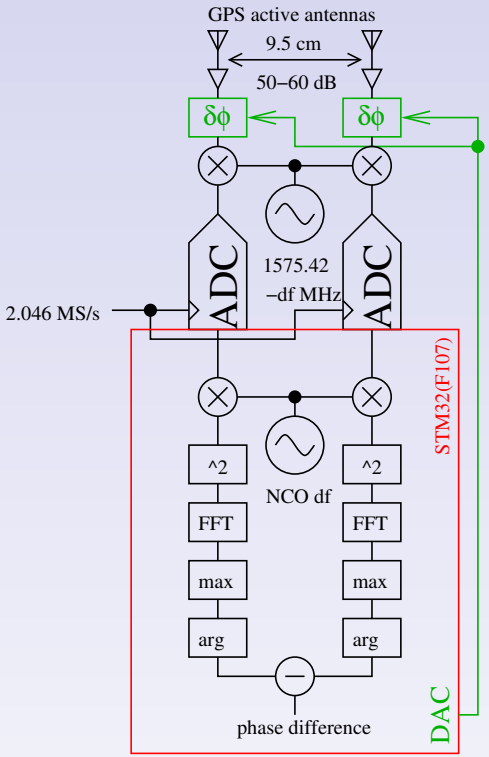




Spoofed constellation

Beamforming

- Spoofing detection is possible ⇒ mitigation [20] ?
- The ground-based signal is stronger than the spaceborne signal
  ⇒ tune antenna radiation pattern so that a null (low reception sensitivity) is directed towards spoofing source
- Also applicable to jamming mitigation
- Antenna array with the "proper" phase conditions between elements will cancel (destructive interference) the signal coming from a given direction



[20] R. Heue, *GNSS Jamming and Spoofing: Hazard or Hype?* at `www.space-of-innovation.com/gnss-jamming-and-spoofing-hazard-or-hype/` (June 2018): "A vital means to counter jammers is the use of an **array antenna, which either is able to steer the radiation pattern of the array to form a spatial null towards the jammer**, or to provide additional gain towards the satellites. However, such controlled radiation pattern antennas (CRPA) are military technology and the availability for civil users is an exception."

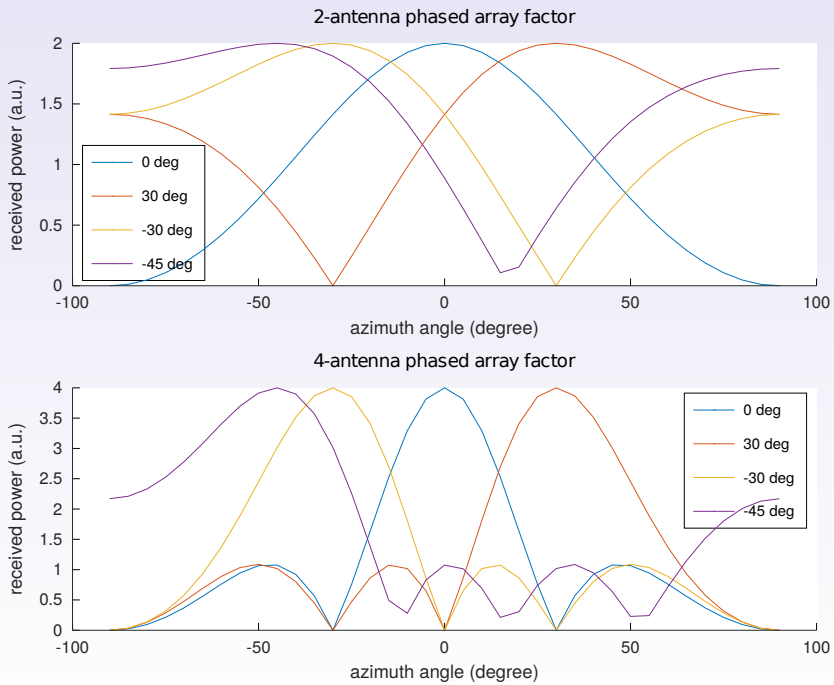
Beamforming

- Spoofing detection is possible ⇒ mitigation ?
- The ground-based signal is stronger than the spaceborne signal ⇒ tune antenna radiation pattern so that a null (low reception sensitivity) is directed towards spoofing source
- Also applicable to jamming mitigation
- Antenna array with the "proper" phase conditions between elements will cancel (destructive interference) the signal coming from a given direction

Phased array factor

$$\sum_{n=0}^{N-1} \exp(jn\Psi),\ \Psi = kd\cos(\vartheta) + \beta$$

where $k = \frac{2\pi}{\lambda}$, d distance between antennas, ϑ incidence angle and β the phase between array elements



Problem: weight and phase offset identification

- 1.57542 GHz with consumer grade GPS antenna: different radiation patterns, different phase offsets, different metallic and dielectric environments
- Efficient destructive interference requires fine tuning weight and phase between antenna signals:

$$cleaned = antenna_1 - weight \times antenna_2 \ (weight \in \mathbb{C})$$

- how to identify *weight* (power ratio and phase shift) with $antenna_1$ and $antenna_2$ long I/Q datasets ?
- Solution : $\boxed{weight = pinv(antenna_2) \times antenna_1}$

  where $pinv(X) = (X^H \cdot X)^{-1} \cdot X^H$, ^{H} the conjugate transpose.
- spoofing/jamming removal:

$$\boxed{\text{cleaned}=(\text{antenna}_1 - weight \times antenna_2)}$$

Least square error solution

Demonstration of the least square solution to the overdetermined problem (more rows than columns: $y = Mx \Rightarrow x \neq M^{-1}y$): y is linear combinations of columns of M with weights x: x must minimize

$$\varepsilon = ||y - Mx||_2 = (y - Mx)^H \cdot (y - Mx) \in \mathbb{R}$$
$$= (y^H y - y^H Mx - \underbrace{x^H M^H y}_{(y^H Mx)^H 20} + \underbrace{x^H M^H Mx}_{\partial/\partial x = 2M^H Mx})$$

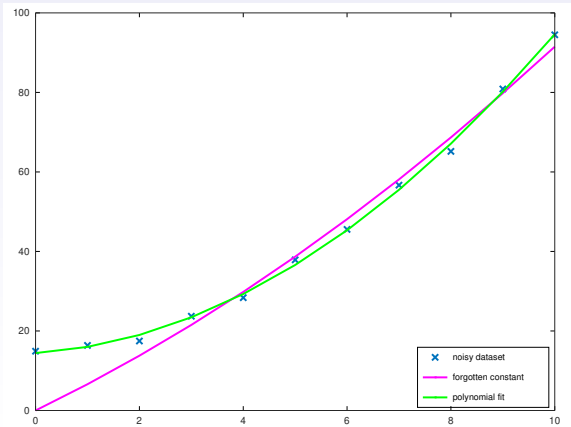
P.J. Dhrymes, *Mathematics for Econometrics*, Springer-Verlag (2013), pp.149–169

R. Penrose, *A generalized inverse for matrices*, Proc. Cambridge Philosophical Society **51** (3) 406-–413 (1955)

$$\Rightarrow \frac{\partial \varepsilon}{\partial x} = \frac{\partial}{\partial x}\left(-2\underbrace{y^H Mx}_{\partial/\partial x = M^H y} + x^H \underbrace{M^H M}_{\text{inversible}} x\right) = 0 \Leftrightarrow M^H y = M^H Mx \text{ and}$$

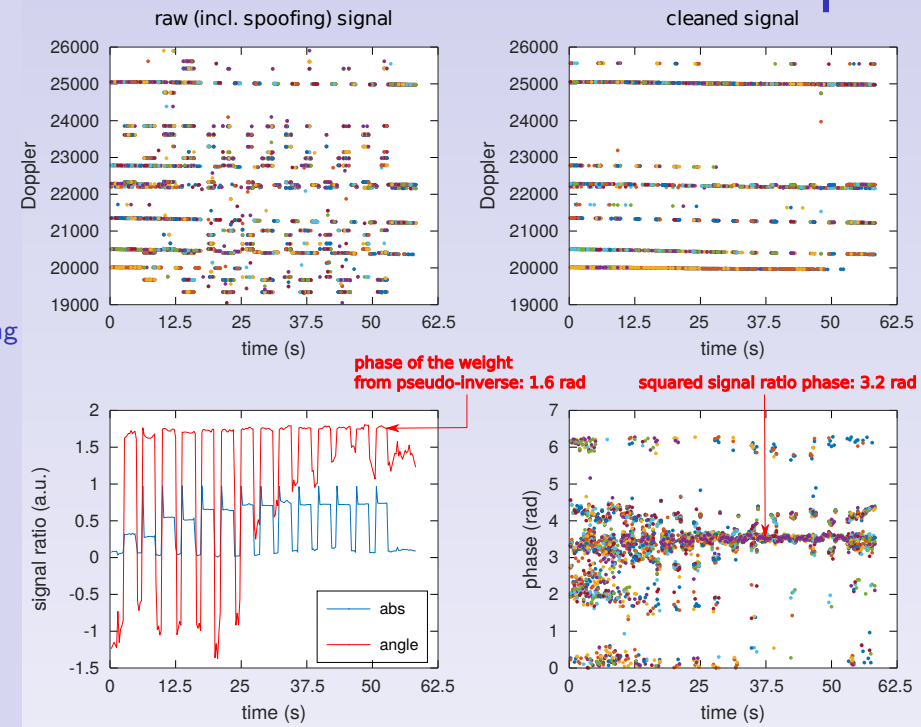
$$x = (M^H M)^{-1} M^H y = \texttt{pinv}(M) \times y$$

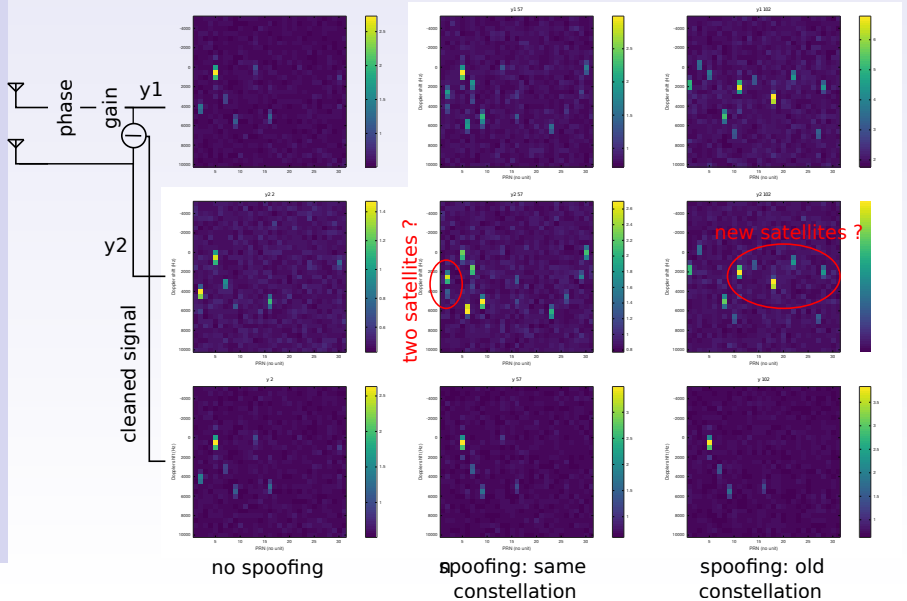
```
x=[0:10]'
y=2*x+0.6*x.^2+13+(5*rand(11,1)-2.5)
a=pinv([x x.^2])*y          %oops no cst
plot(x,a(2)*x.*x+a(1)*x,'m')
a=pinv([x x.^2 ones(11,1)])*y
%    1.86  0.62     13.4 (vs 2 0.6 13)
plot(x,a(2)*x.*x+a(1)*x+a(3),'g')
a=([x x.^2 ones(11,1)])\y % same res.
```



[20] $(y^H Mx)^H = y^H Mx$ since scalar value

Spoofing cancellation





Measurement sequence: spoofing/non-spoofing every 10 s with increasing TX power

↑-←: raw signal φ

↑-→: cleaned signal φ

↓-←: weights (phase and magnitude)

↓-→: codeless analysis

Bottom charts: raw & cleaned PRN-Doppler maps

Conclusion: `pinv()` **and codeless decoding provide consistent phase information**

Question: can the cleaned signal be decoded to the genuine position ?

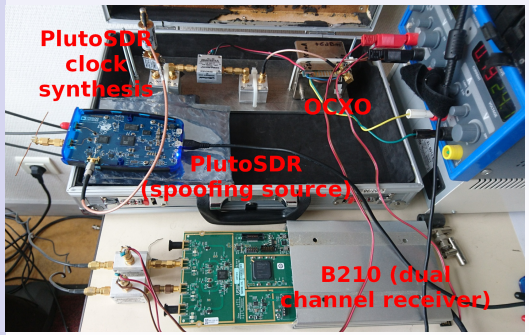
Spoofing cancellation

gnss-sdr [21] for processing spoofed/jammed datasets and cleaned datasets: statistical analysis on 100 runs ($\rightarrow$ %)

```
New GPS NAV message received in channel 15: subframe 5 from satellite GPS PRN 04 (Block Unknown)
New GPS NAV message received in channel 13: subframe 5 from satellite GPS PRN 02 (Block IIR)
New GPS NAV message received in channel 3: subframe 5 from satellite GPS PRN 23 (Block IIR)
New GPS NAV message received in channel 6: subframe 5 from satellite GPS PRN 26 (Block IIF)
Position at 2019-Nov-30 10:59:42.000000 UTC using 4 observations is Lat = 47.251759020 [deg], Long = 5.993861290 [deg],
Velocity: East: -0.092 [m/s], North: -0.091 [m/s], Up = -0.207 [m/s]
```

"before correction" / "after cancellation"

TX power	Constellation	Correct pos.(%)	Wrong pos.(%)	No solution(%)
-35	current	0/90	57/0	43/10
-40	current	0/93	96/0	4/7
-45	current	0/2	61/1	39/97
-50	current	0/3	31/7	69/90
-55	current	52/23	0/0	48/77
-60	current	88/64	0/0	12/36
-40	-6 h	7/100	44/0	49/0
-50	-6 h	6/4	90/96	4/0



[21] https://gnss-sdr.org

Spoofing cancellation

`gnss-sdr` for processing spoofed/jammed datasets and cleaned datasets: statistical analysis on 100 runs ($\rightarrow$ %)

```
New GPS NAV message received in channel 15: subframe 5 from satellite GPS PRN 04 (Block Unknown)
New GPS NAV message received in channel 13: subframe 5 from satellite GPS PRN 02 (Block IIR)
New GPS NAV message received in channel 3: subframe 5 from satellite GPS PRN 23 (Block IIR)
New GPS NAV message received in channel 6: subframe 5 from satellite GPS PRN 26 (Block IIF)
Position at 2019-Nov-30 10:59:42.000000 UTC using 4 observations is Lat = 47.251759020 [deg], Long = 5.993861290 [deg], H
Velocity: East: -0.092 [m/s], North: -0.091 [m/s], Up = -0.207 [m/s]
```

"before correction" / "after cancellation"

TX power	Constellation	Correct pos.(%)	Wrong pos.(%)	No solution(%)
-35	current	0/90	57/0	43/10
-40	current	0/93	96/0	4/7
-45	current	0/2	61/1	39/97
-50	current	0/3	31/7	69/90
-55	current	52/23	0/0	48/77
-60	current	88/64	0/0	12/36
-40	-6 h	7/100	44/0	49/0
-50	-6 h	6/4	90/96	4/0

- at strong power (-35 and -40 dBm): spoofing signal easy to identify $\Rightarrow$ cancellation procedure is efficient
- at weaker signal (-45, -50 dBm): genuine and spoofing signals compete $\Rightarrow$ erroneous position with a lower success rate due to the contribution of the genuine constellation
- low power (-60 dBm): spoofing is inefficient $\Rightarrow$ the correct position is always reached

Jamming cancellation

No antenna, only power radiated by PCB

"before correction" / "after cancellation"

Distance	Correct pos.(%)	No sol.(%)
no jamming	100	0
7m50	0/94	100/6
6m50 (end)	0/49	100/51
6m00	0/79	100/21
5m50	0/0	100/100
5m00	0/0	100/100
4m50	0/0	100/100

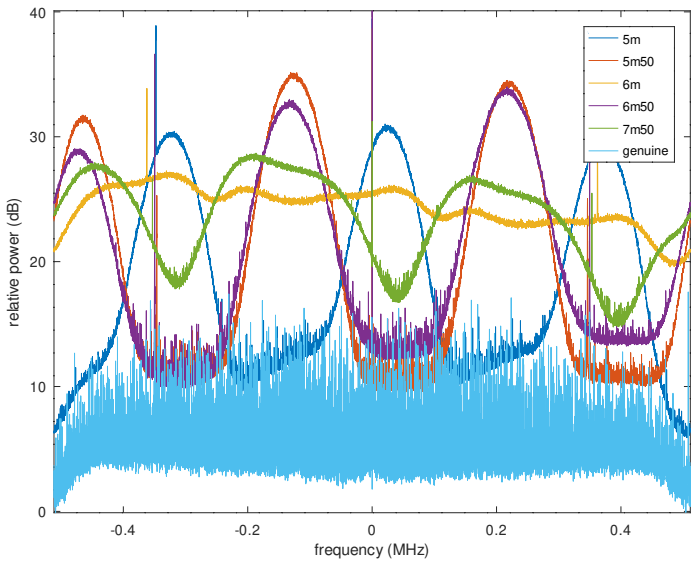
Interfering spectra

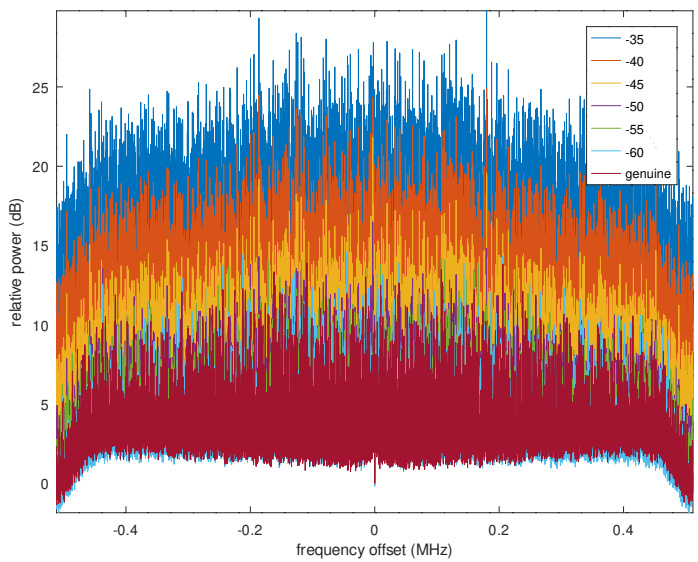
Jamming:

- strong signal might saturate RF frontend
- 300 kHz component=sawtooth signal period

Spoofing:

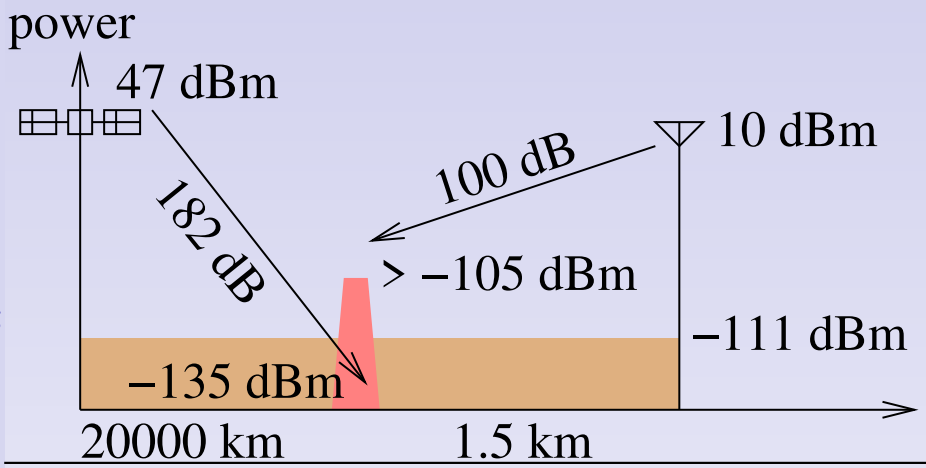
- signal strong enough abive genuine signal can be subtracted
- -60 dBm below genuine signal power





Conclusion: stronger signals are easier to cancel as long as RF frontend does not saturate

Conclusion



Jamming range:

$20log10(d) = 100 + 147.55 - 184$

$\Rightarrow d \simeq 1.5$ km

Spoofing range:

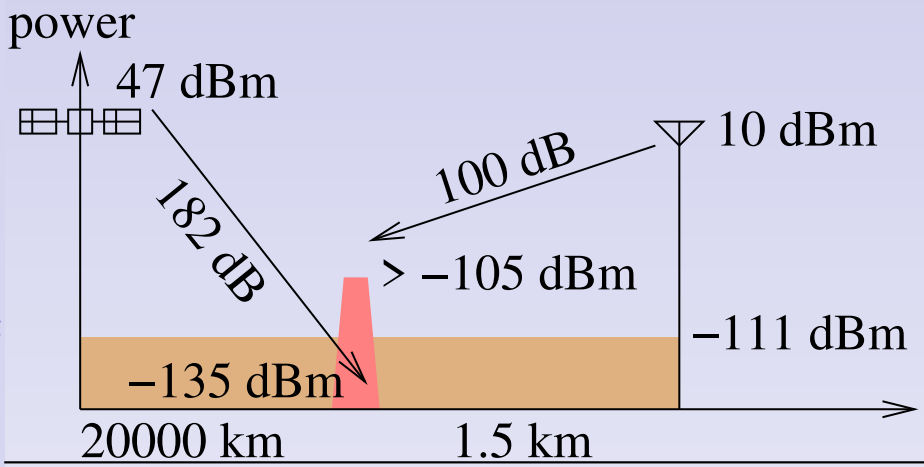
$20log10(d) = \underbrace{130+}_{\text{compression}}\ 147.55 - 184$

$\Rightarrow d \simeq 47$ km

- too close: RF frontent saturates, no usable signal (range unknow [21])
- strong interference: spoofing/jamming can be identified and subtracted (unknown–1.5 km)
- weak jamming/spoofing:
  - jamming below GPS compression: no impact (>1.5 km)
  - spoofing above thermal noise can be identified and subtracted (1.5–24 km)
- spoofing below thermal noise: **no identified solution** (24–47 km)
- spoofing below genuine signal: no impact (>47 km)

[21] MAX2659 LNA: -12 dBm input 1dB compression point ⇒ considering +10 dBm output, 22 dB FSPL reached at 0.2 m !

Conclusion



Jamming range:

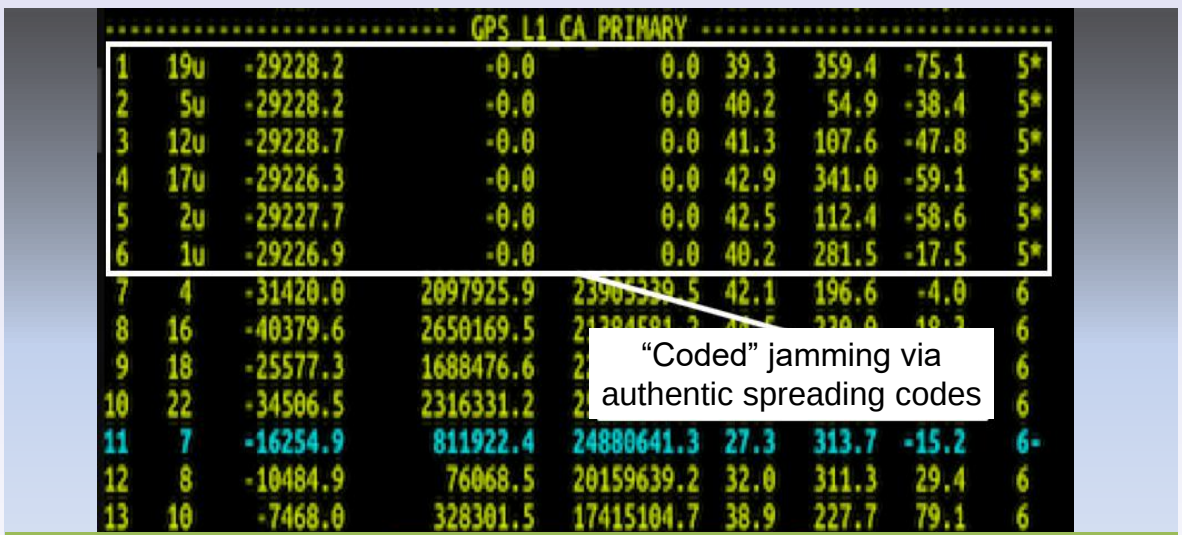
$20log10(d) = 100 + 147.55 - 184$

$\Rightarrow d \simeq 1.5$ km

Spoofing range:

$20log10(d) = \underbrace{130+}_{\text{compression}} 147.55 - 184$

$\Rightarrow d \simeq 47$ km



The Syrian interference source employs *coded jamming.* Its purpose appears to be denial of GPS service, but it achieves this by *spoofing* each of the GPS L1 C/A PRN codes (albeit without LNAV modulation).

T. Humphreys, *GNSS Radio Frequency Interference Detection from LEO*, PNT EXCOM Advisory Board Semi-Annual Meeting (2019)