Robust Global Navigation Satellite Systems

Focus on anti-jamming

Pau Closas

Assistant Professor
Northeastern University
Department of Electrical and Computer Engineering
Boston, Massachusetts (USA)

closas@northeastern.edu
http://www.ece.neu.edu/people/closas-pau

Northeastern University

Robust GNSS Day @ TéSA, 10 July 2019

In·ter·fere [in-ter-feer]

- From Old French *s'entreferir* 'strike each other', from *entre-* 'between' + ferir (from Latin *ferire* 'to strike')
  1. prevent (a process or activity) from continuing or being carried out properly. (JAMMING)
  2. take part or intervene in an activity without invitation or necessity. (SPOOFING)

In·ter·fere [in-ter-feer]

- From Old French *s'entreferir* 'strike each other', from *entre-* 'between' + ferir (from Latin *ferire* 'to strike')
  1. prevent (a process or activity) from continuing or being carried out properly. (JAMMING)
  2. take part or intervene in an activity without invitation or necessity. (SPOOFING)
- Using maths (to say the same):

$$\begin{aligned} y(t) = &\quad x_\theta(t) + \eta(t) &\Rightarrow &\quad \text{Signal plus noise} \\ y(t) = &\quad x_\theta(t) + i(t) + \eta(t) &\Rightarrow &\quad \text{Signal plus interference plus noise} \\ y(t) = &\quad x_\theta(t) + x_{\tilde{\theta}}(t) + \eta(t) &\Rightarrow &\quad \text{Signal plus spoofer plus noise} \end{aligned}$$

where $x_\theta(t)$ is the desired signal, parameterized by θ.

Goals

At the end of this course we should be able to:

- Understand the threats and impacts of interfering GNSS receivers;
- Classify interferences according to their signal characteristics;
- Model mathematically interference signals;
- Evaluate the impact at various stages of a GNSS receiver;
- Understand the main mitigation approaches and methods;
- Simulate (not generate, ok?) interferences.

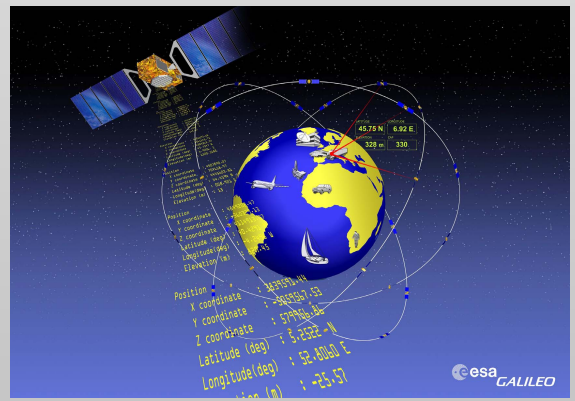
It would be excellent if this material triggers some research ideas: lot of interest in GNSS security/reliability aspects!

Outline

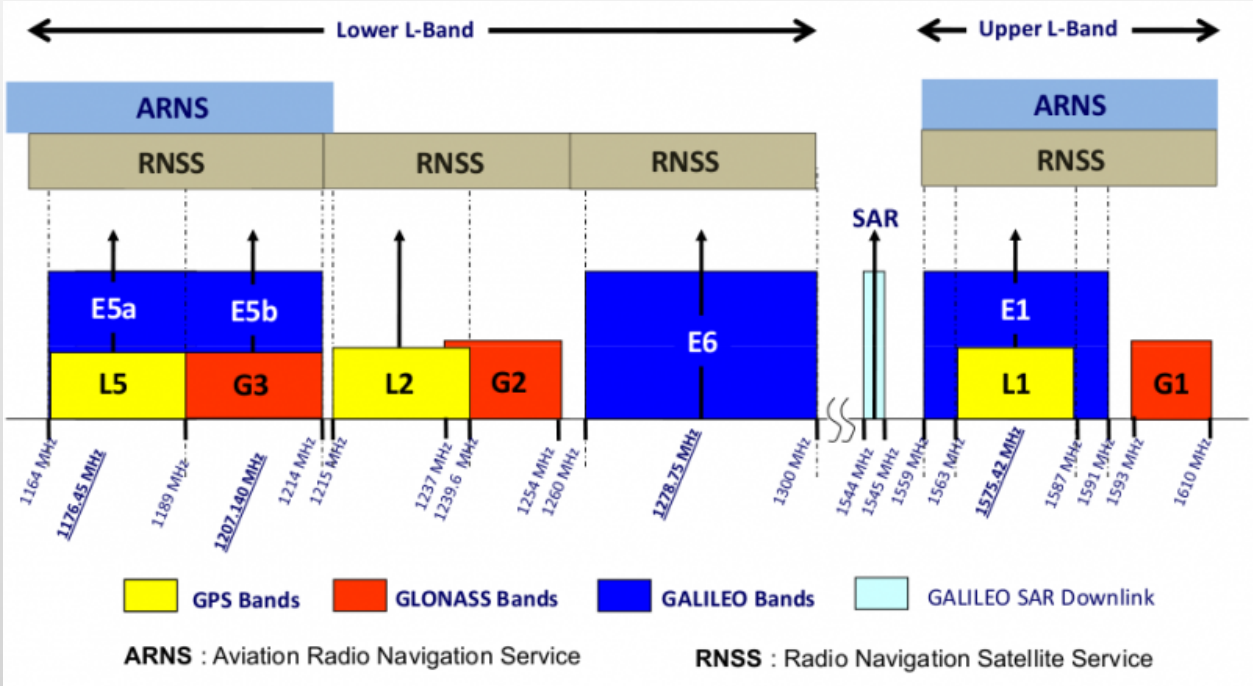
Outline

Positioning is everywhere (...and GNSS is a key technology)

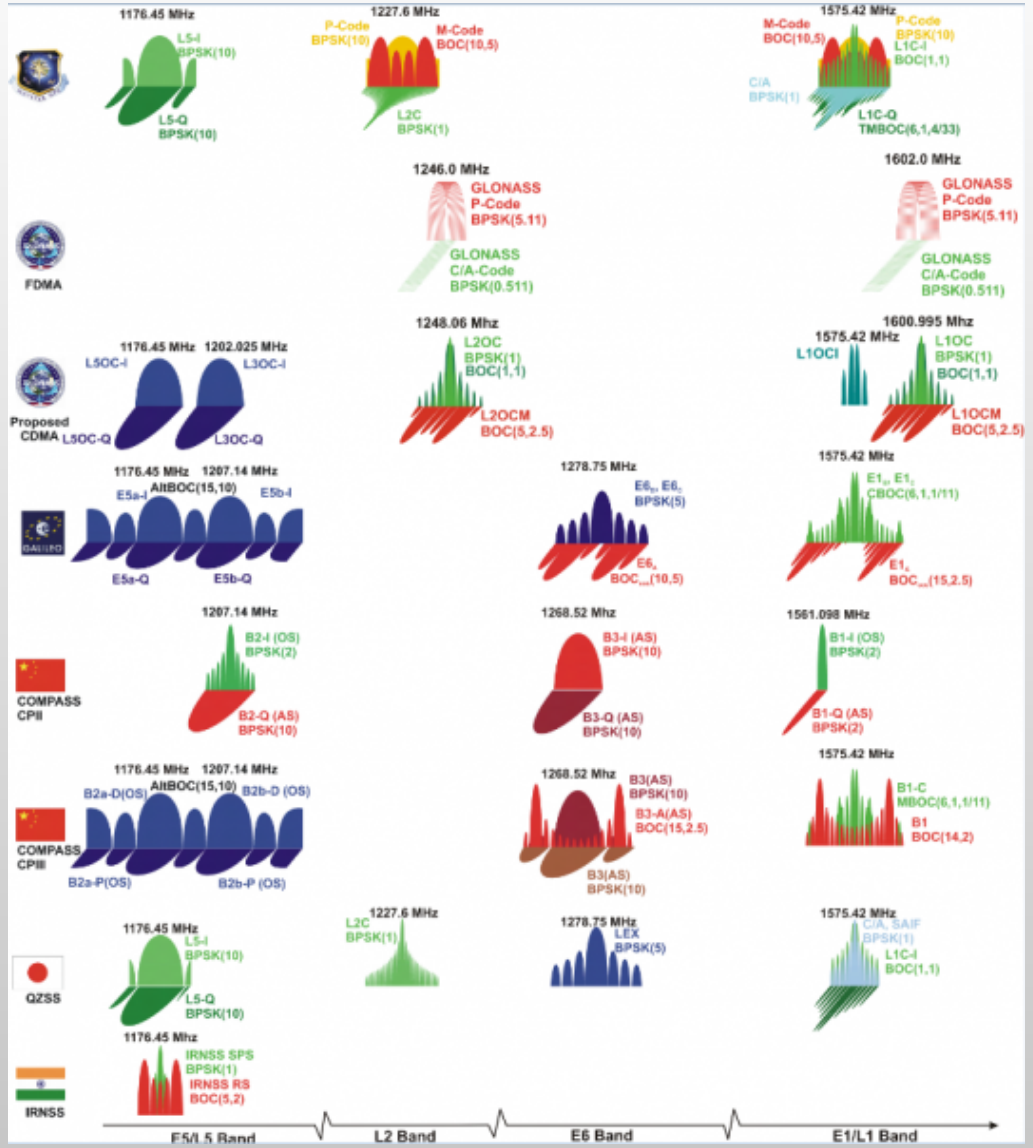
- Positioning systems have been gaining relevance due to the widespread advances of devices and technologies and the necessity for seamless solutions in Location-based Services (LBS).
- There are many applications, services, and technologies leveraging on location information. You name it!
- Global Navigation Satellite Systems:
  GNSS is the general concept used to identify those systems that allow user positioning based on a constellation of satellites.



...and GNSS is a key technology



- GNSS signals coexist in L-band.
- Each signal offers its own service.
- GNSS receivers are multiconstellation.

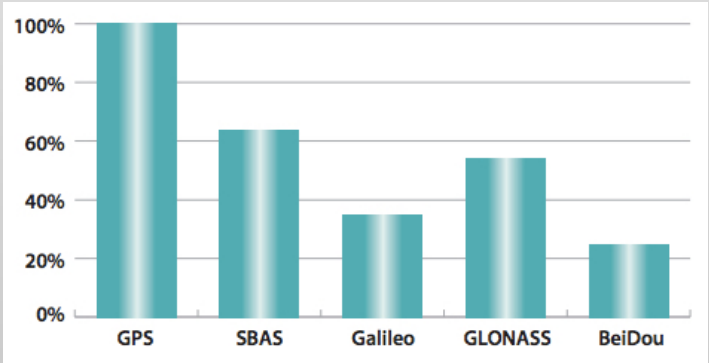

1176.45 MHz
L5-I BPSK(10)
L5-Q BPSK(10)
1227.6 MHz
P-Code BPSK(10)
M-Code BOC(10,5)
L2C BPSK(1)
1575.42 MHz
M-Code BOC(10,5)
P-Code BPSK(10)
L1C-I BOC(1,1)
C/A BPSK(1)
L1C-Q TMBOC(6,1,4/33)
FDMA
1246.0 MHz
GLONASS P-Code BPSK(5.11)
GLONASS C/A-Code BPSK(0.511)
1602.0 MHz
GLONASS P-Code BPSK(5.11)
GLONASS C/A-Code BPSK(0.511)
Proposed CDMA
1176.45 MHz
L5OC-I
L5OC-Q
1202.025 MHz
L3OC-I
L3OC-Q
1248.06 Mhz
L2OC BPSK(1) BOC(1,1)
L2OCM BOC(5,2.5)
1575.42 MHz
L1OCI
L1OC BPSK(1) BOC(1,1)
1600.995 Mhz
L1OCM BOC(5,2.5)
1176.45 MHz
1207.14 MHz
E5a-I
AltBOC(15,10)
E5b-I
E5a-Q
E5b-Q
1278.75 MHz
E6A, E6B BPSK(5)
E6A BOCcos(10,5)
1575.42 MHz
E1B, E1C CBOC(6,1,1/11)
E1A BOCcos(15,2.5)
COMPASS CPII
1207.14 MHz
B2-I (OS) BPSK(2)
B2-Q (AS) BPSK(10)
1268.52 Mhz
B3-I (AS) BPSK(10)
B3-Q (AS) BPSK(10)
1561.098 MHz
B1-I (OS) BPSK(2)
B1-Q (AS) BPSK(2)
COMPASS CPIII
1176.45 MHz
1207.14 MHz
B2a-D(OS)
AltBOC(15,10)
B2b-D (OS)
B2a-P(OS)
B2b-P (OS)
1268.52 Mhz
B3(AS) BPSK(10)
B3-A(AS) BOC(15,2.5)
B3(AS) BPSK(10)
1575.42 MHz
B1-C MBOC(6,1,1/11)
B1 BOC(14,2)
QZSS
1176.45 MHz
L5-I BPSK(10)
L5-Q BPSK(10)
1227.6 MHz
L2C BPSK(1)
1278.75 MHz
LEX BPSK(5)
1575.42 MHz
C/A, SAIF BPSK(1)
L1C-I BOC(1,1)
IRNSS
1176.45 Mhz
IRNSS SPS BPSK(1)
IRNSS RS BOC(5,2)
E5/L5 Band
L2 Band
E6 Band
E1/L1 Band

Global Navigation Satellite Systems in 2019

- **GPS**: 24 satellites
  - **L1 C/A**: 1575.42 MHz, BPSK(1). Used by your smartphone.
  - **L2C**: 1227.60 MHz, BPSK(1)
  - **L5**: 1176.45 MHz, BPSK(10)
- **GLONASS**: 24 satellites
  - **L1**: 1602.00 MHz, FDMA + BPSK(0.5)
  - **L2**: 1246.00 MHz, FDMA + BPSK(0.5)
- **Galileo**: currently, 22 operational satellites
  - **E1b/c**: 1575.42 MHz, CBOC(6,1,1/11)
  - **E6B**: 1278.75 MHz, BPSK(5)
  - **E5a / E5b**: 1176.45 / 1207.14 MHz, QPSK(10) / QPSK(10).
- **Beidou**: 35 satellites (2020)
  - **B1I**: 1561.098 MHz, BPSK(1)
  - **B2I**: 1207.140 MHz, BPSK(2)
  - **B3I**: 1268.520 MHz, BPSK(10)

...and GNSS is a key technology

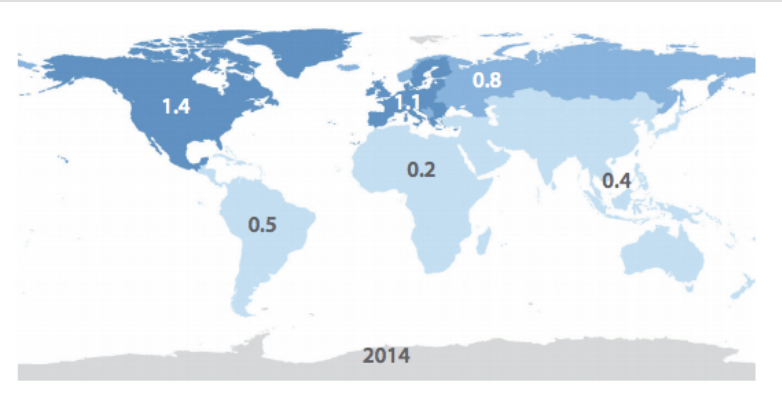
- GNSS is recognized to be the *de facto* technology, when available.
  - Dedicated infrastructure (satellital)
  - Earth scale coverage (and beyond?)
  - Medium to high accuracy performance (depending on positioning method)
  - High market penetration (don't tell me your smartphone does not have an integrated GNSS...)
- GNSS penetration in smartphones per system (as 2014):

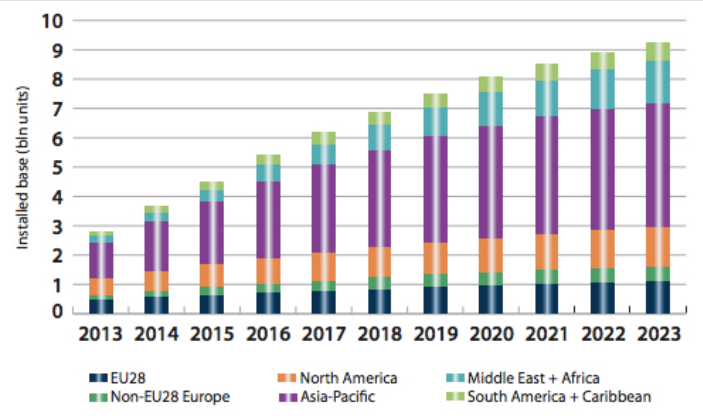


[GMR14] European GNSS Agency (GSA), "GNSS Market Report," Issue 4, March 2015

...and GNSS is a key technology

- GNSS is used around the globe, with 3.6 bln GNSS devices in use in 2014.
  - Smartphones continue to dominate (3.08 bln in 2014),
  - followed by devices used for road applications (0.26 bln).
- (True) numbers for 2014 and (Predicted) numbers through 2023:





(3σ confidence intervals for the predictions?)

[GMR14] European GNSS Agency (GSA), "GNSS Market Report," Issue 4, March 2015

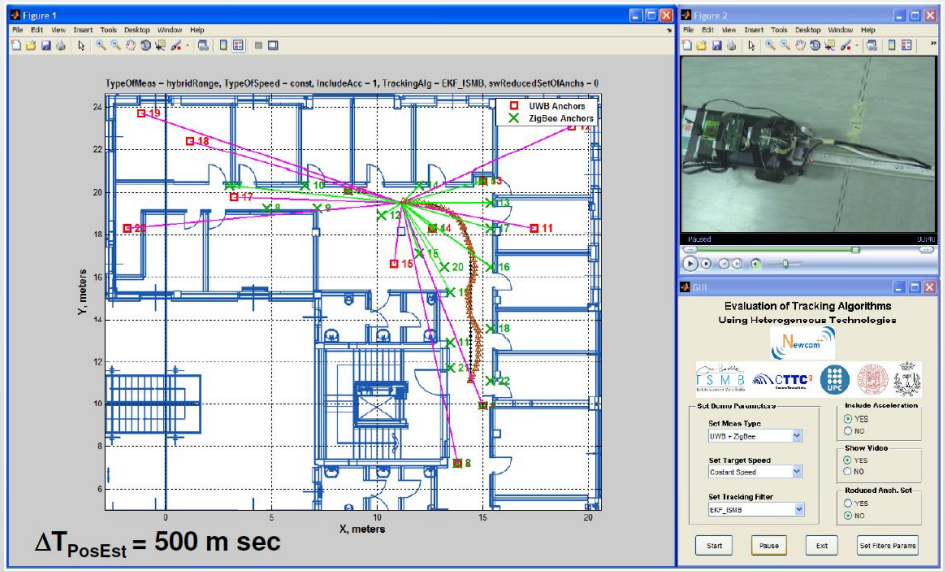
GNSS limitations (indoors)

- GNSS is the legacy solution outdoors. However, its performance is severely degraded in indoor scenarios, in addition to other vulnerabilities.
  - An important component of LBS is indoor tracking where object or people are tracked within a building or any enclosed structure.
  - For indoor applications, there is not a single dominant technology able to cover the wide range of requirements.
  - The trend is to combine standard, low-cost, and already-deployed technologies by statistical data fusion methods.
- In this course, we do not discuss indoor positioning, which would require a separate course *per se*.

[Dar15] D. Dardari, P. Closas, P. Djurić, "*Indoor Tracking: Theory, Methods, and Technologies*", IEEE Trans. on Vehicular Technologies, Vol. 64, No. 4, pp. 1263-1278, 2015.

GNSS limitations (indoors)

- An example of indoor localization and tracking in wireless sensor networks:

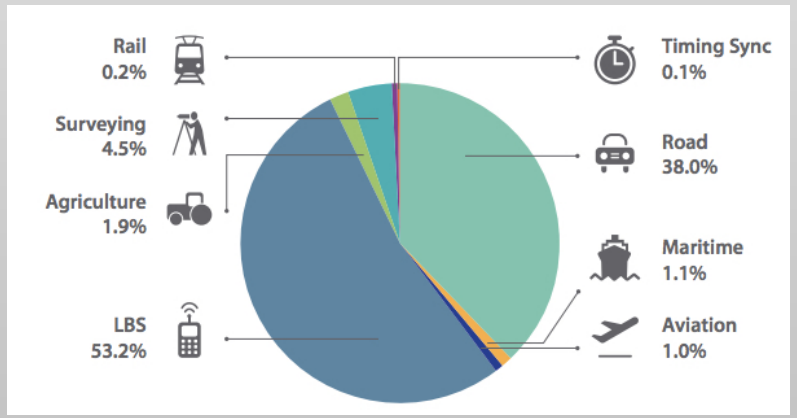


- Tracking of a robot by UWB and ZigBee sensors.
- Robot moved on a calibrated track, while emitting ranging signals to reference nodes.
- Fusion sensor gathered and processed these ranges to compute estimates sequentially.
- Algorithms were run using data from a measurement campaign (FP7 project: Newcom++).

$$\underbrace{\begin{pmatrix} x_n \\ y_n \\ \dot{x}_n \\ \dot{y}_n \end{pmatrix}}_{\mathbf{x}_n} = \underbrace{\begin{pmatrix} 1 & 0 & T & 0 \\ 0 & 1 & 0 & T \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\mathbf{F}_n} \mathbf{x}_{n-1} + \mathbf{w}_n \quad , \quad \mathbf{y}_n = \underbrace{\begin{pmatrix} \|\mathbf{p}_n - \mathbf{p}^{(1)}\| \\ \vdots \\ \|\mathbf{p}_n - \mathbf{p}^{(N)}\| \end{pmatrix}}_{\mathbf{h}_n(\mathbf{x}_n)} + \underbrace{\begin{pmatrix} \nu_{1,n} \\ \vdots \\ \nu_{N,n} \end{pmatrix}}_{\boldsymbol{\nu}_n}$$

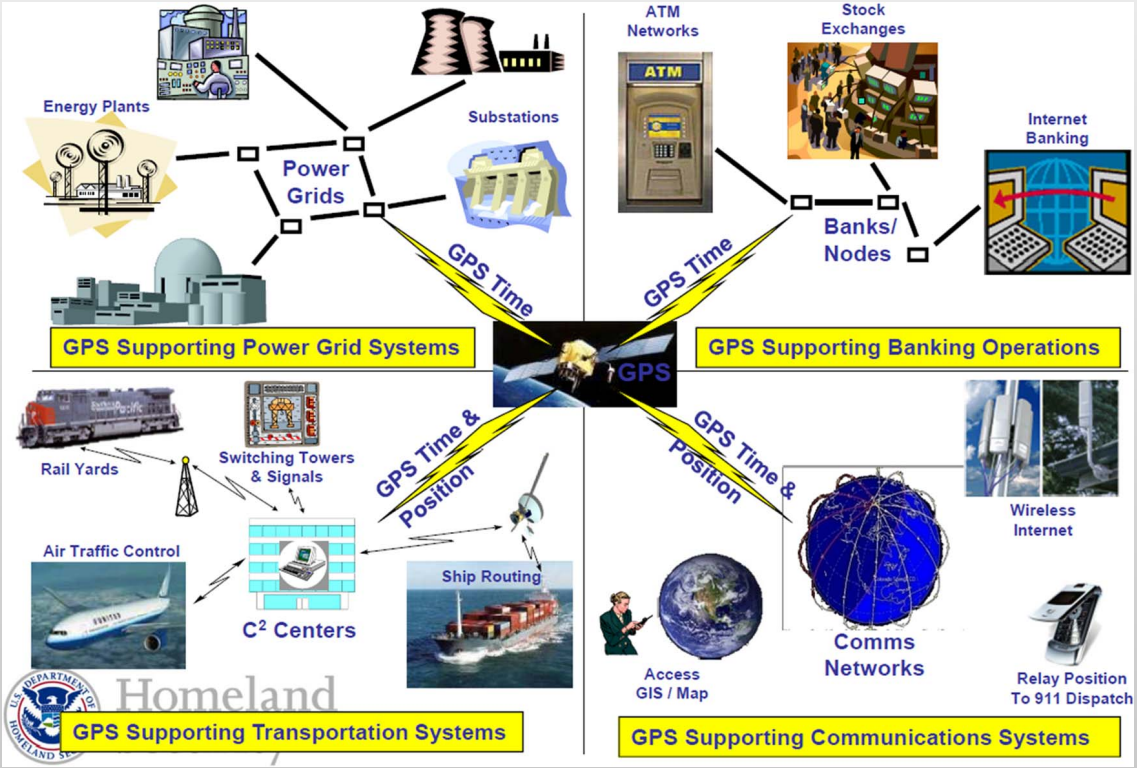
GNSS limitations (interferences)

- GNSS is the legacy solution outdoors. However, its performance is severely degraded in indoor scenarios, in addition to other vulnerabilities.
- Need for protecting GNSS against intentional and unintentional interference sources:
  - Ubiquitous use of GNSS in civilian, security, and defense applications.
  - Growing dependence on GNSS within critical infrastructures.
  - Potential disruption of GNSS can lead to catastrophic consequences.



GNSS limitations (interferences)

"15 of the 19 Critical Infrastructure & Key Resources Sectors have some degree of GPS timing usage" – US DHS



[Mer12] J. Merrill, "Patriot Watch: Vigilance Safeguarding America," presented at the Presentation Telcordia-NIST-ATIS Workshop Synchronization Telecommun. Syst. (WSTS'12), Mar. 2022, 2012.

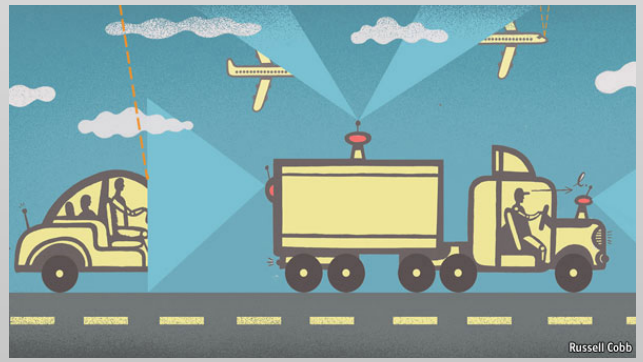
GNSS limitations (interferences)

- Jammers are:
  - Illegal in most countries...
  - ...but cheap/easy to buy.
- Jammers can disrupt GNSS-based services in wide geographical areas (several kilometers)

[Mit11] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Signal characteristics of civil GPS jammers," in Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS), Portland, OR, Sep. 2011, pp. 19071919.

GNSS limitations (interferences)

- A well-known jamming example is the case of a truck driver periodically passing close to the Newark Liberty International Airport.
- The driver was using a GNSS jammer to prevent his company from tracking his position.
- The jammer was however so powerful that problems were caused to the reception of WAAS and GNSS signals.
- Eventually, after 3 months of investigation, the authorities were able to identify the problem, locate the jammer, and fine the truck driver.



"No jam tomorrow," The Economist, Mar. 10 2011. [Online]. Available: http:// www.economist.com/node/18304246

GNSS limitations (interferences)

- In this course, we focus on the effects of interferences on GNSS receivers. We discuss
  - Taxonomy,
  - Characterization,
  - Effects, and
  - Countermeasures.
- The articles in the 2016 Special Issue of the Proceedings of the IEEE are extremely relevant to this topic. Some material of this course is based on them. Check them out!

[Ami16] M. Amin, P. Closas, A. Broumandan, J. Volakis (Eds.), "*Scanning the Issue: Vulnerabilities, Threats, and Authentication of Satellite-Based Navigation Systems*", in Proceedings of the IEEE, vol 104, no 6, pp 1169–1173, June 2016.

Outline

The art of navigation

- The art of finding the way from one place to another is called navigation.
- Until the 20-th century, the term referred mainly to guiding ships across the seas. Indeed, the word *navigate* comes from the Latin *navis* (meaning "ship") and *agere* (meaning "to move or direct").
- Today, the word also encompasses the guidance of travel on land, in the air, and in inner and outer space.
- In the past, civilizations able to effectively navigate the seas were typically more prosperous due to trading.

The art of navigation

- For several thousand years, humanity has developed ingenious ways of navigating from A to B. Celestial navigation has been the main solution, but also compass has been an important tool.
- The problem was not the latitude, easy to calculate from the Sun's position, but the longitude.
- The longitude of a location is directly related to the difference between the local time and the Greenwich reference time.

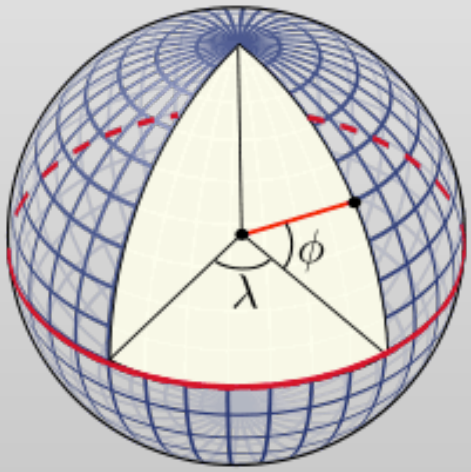


Figure: Latitude (ϕ) and longitude (λ) on a graticule.

Dead Reckoning

- Process of estimating one's position based on previous known position and measured changed in position, velocity, attitude, etc. over a time interval.
- *Modern* methods include:
  - Odometer: wheel-rotation counting.
  - Pedometer: pace counting.
  - Magnetic compass: heading measurement.
  - Inertial Navigation System (INS): accelerometers and gyroscopes

E.g., positioning by accelerometer integration (simplified version...);

$$\begin{aligned}
(\text{known}) \quad & \mathbf{p}(t_0), \dot{\mathbf{p}}(t_0) \\
(\text{measured}) \quad & \ddot{\mathbf{p}}(t) \\
(\text{velocity integration}) \quad & \dot{\mathbf{p}}(t) = \dot{\mathbf{p}}(t_0) + \int_{t_0}^{t} \ddot{\mathbf{p}}(\tau) d\tau \\
(\text{position integration}) \quad & \mathbf{p}(t) = \mathbf{p}(t_0) + (t - t_0)\dot{\mathbf{p}}(t_0) + \int_{t_0}^{t} \int_{t_0}^{\tau} \ddot{\mathbf{p}}(\tau') d\tau' d\tau
\end{aligned}$$

Dead Reckoning

- Process of estimating one's position based on previous known position and measured changed in position, velocity, attitude, etc. over a time interval.
- ...but dead reckoning has been used extensively in the *past*, e.g.
  - Heaving the log: throw a wood log into the water and observe how fast it moves away from the ship.
  - Chip log: a small weighted wood panel, attached to a rope. The rope had equispaced knots tied. Sailors would throw the wood panel into the sea, counting the number of knots in a given time interval (*precisely* measured with a sand glass).
  - That's the origin of the nautical speed unit: *knot* ($= 1$ nmi/hour)

Dead Reckoning

- Achievable precision and accuracy depend on each *technology*.
- For instance, inertial sensors are known to have biased acceleration measures, causing position errors that grow quadratic with time due to double integration.

$$\begin{aligned} &(\text{velocity integration}) \quad \dot{\mathbf{p}}(t) \quad \propto (\text{Velocity at t}) + \text{bias} \cdot t \\ &(\text{position integration}) \quad \mathbf{p}(t) \quad \propto (\text{Position at t}) + \text{bias} \cdot t^2 \end{aligned}$$

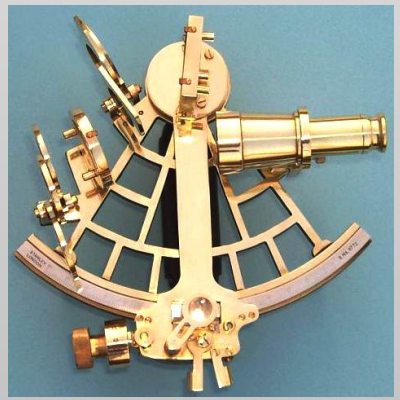
- In general, positioning errors grow over time in dead reckoning methods. There is a need for precise resetting of initial conditions.
- There was a need to engineer methods that provided absolute position fixes (used, or not, jointly with dead reckoning techniques):
  - First, we used celestial navigation.
  - Then, radionavigation and satellite-based navigation was developed.

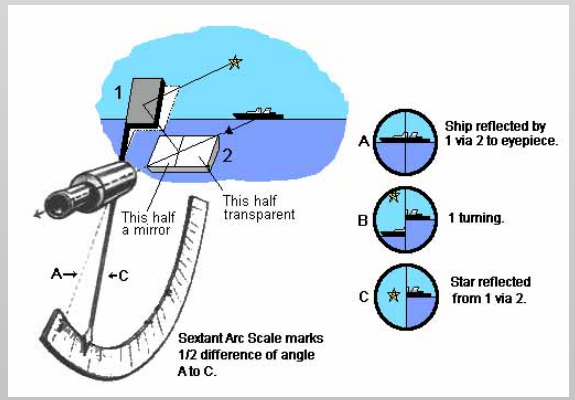
Historical remarks

- Astrolabe
  - from Greek *astrolabos*: *astron* "star" and *lambanein* "to take". Later, in the medieval Islamic world the Arabic word "al-Asturlab"
  - Consists of a disk and several flat plates, each made for a specific latitude. The plates are a stereographic projection of the celestial sphere above the local horizon.
    1. Local latitude ⇒ Time: Observing a star altitude, one could estimate time (e.g. longitude).
    2. Time ⇒ Local latitude: Given time and date are known, one could predict a star altitude.

Historical remarks

- Sextant
  - Is a navigation instrument that measures (day or night) the angular distance between two visible objects (e.g. astronomical object and horizon, $\angle(\star, -)$)
  - Estimation of $\angle(\star, -)$ and the observation time can be mapped in aeronautical charts to estimate latitude.
  - Held horizontally, can also be used to measure the distance between the moon and another celestial object in order to determine Greenwich Mean Time and hence longitude.
  - Provides relative measures, so no need for steady measurements (e.g. moving ship)





Historical remarks

- Angular measurements to celestial objects were extremely important.
- Equally important was measuring time accurately.
- The local time could conveniently be fixed by a noon sighting of the Sun (at its maximum altitude)
- At other times in the day, a reliable clock was required (or some other way of distant time synchronization)
- With the advent of worldwide trading, precise navigation became a real need.
- As a consequence, it was necessary to build precise clocks:
  - pendulum or sand clocks were not appropriate on-board: mechanical instruments affected by ship's movements.
  - accurate astronomical observations were impracticable, anytime/anywhere.

Historical remarks

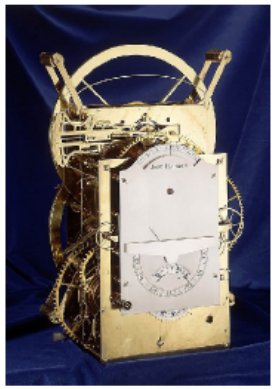
- Around 1700, after a tragic accident in the Isles of Scilly, the British Government got concerned about navigation and set up in 1714 the Board of Longitude (formally, The Commissioners for the Discovery of the Longitude at Sea)
- The Board of Longitude offered a reward to obtain a solution that could provide longitude (and usable at sea!). Prizes depend on level of accuracy:
  - $£10,000$ (equivalent to $£1.3$ million in 2016) for a method that could determine longitude within 1 degree (equivalent to 60 nautical miles or 110 km).
  - $£15,000$ (equivalent to $£2$ million in 2016) for a method that could determine longitude within 40 minutes (40 nautical miles or 74 km).
  - $£20,000$ (equivalent to $£2.7$ million in 2016) for a method that could determine longitude within 30 minutes (30 nautical miles or 56 km).

Historical remarks

- A number of methods were proposed, clearly superior to existing methods (e.g. observation of Jupiter's satellites by Galileo)
- Those were used to reform maps (with the according displeasure of the French King Louis XV...)
- None achieved the requirements of precision and usability at sea.
- The man who had the best solution was a humble carpenter called John Harrison (1693–1776), who developed very precise and gravity-independent mechanical clocks. The Board never awarded the prize...

(a) H1 (1730-1735)

(b) H2 (1737-1740)



(c) H3 (1740-1759)

(d) H4 (1755-1759)

- H4 lost 24 seconds every 9 days (i.e. $\sim 2'67$ sec/day)

Historical remarks

- More recently, with the development of radios, another class of navigation aids was possible.
- Ground-based infrastructure (developed in the 40s) like:
  - VHF omni directional radio range (VOR), ~ 100 MHz
  - Distance measuring equipment (DME), 100 kHz at ~ 1000 MHz
  - Long range navigation (LORAN), ~ 2 MHz

...operating on low freqs:

large coverage but *poor accuracy*

Historical remarks

- More recently, with the development of radios, another class of navigation aids was possible.
- Satellite-based infrastructure (started in the early 60s)
  - U.S. Air Force and Navy were, competitively, studying improved navigation from space.
  - Predecessors of GPS:

1. U.S. Navy Navigation Satellite System (Transit), 60s.
   - A constellation of 5 circular polar orbiting satellites. Low Earth Orbit (LEO), ~ 1075 km altitude.
   - Satellites emitting two tones at 150 and 400 MHz, to remove ionospheric effects.
   - Doppler–shift based positioning.
   - Limited coverage: unavailability periods 35–100 min
   - Originally intended for navigation of U.S. submarines, but extensively adopted by commercial marine navigators.
   - Accuracy $\sim 100 - 500$ meters.
   - **Contribution to GPS**: developing satellite prediction algorithms.

Historical remarks

- More recently, with the development of radios, another class of navigation aids was possible.
- Satellite-based infrastructure (started in the early 60s)
  - U.S. Air Force and Navy were, competitively, studying improved navigation from space.
  - Predecessors of GPS:

  2. U.S. Navy's Timation (TIMe navigATION), 1972.
     - Satellites were equipped with an onboard very precise clocks.
     - 3 satellites in inclined orbits.
     - Initially, *quartz-crystal* oscillators, later *atomic* clocks were orbit for the first time.
     - Frequency stability improved the orbit prediction and facilitated ground control (extending time between updates).
     - **Contribution to GPS**: developing space-qualified time standards. Third satellite was used as technology demonstrator for GPS.

Historical remarks

- More recently, with the development of radios, another class of navigation aids was possible.
- Satellite-based infrastructure (started in the 60s)
  - U.S. Air Force and Navy were, competitively, studying improved navigation from space.
  - Predecessors of GPS:

3. U.S. Air Force project 621B, 1972.
   - Satellites emitted a modulated pseudo-random noise (PRN) signal, i.e. a repeated digital sequence.
   - PRN sequences possessed useful cross- and auto-correlation properties.
   - PRN were easily generated using shift registers or storing the sequence.
   - Signals could be detected even when their power density was much lower to that of ambient noise (low power, undetectable, anti-jamming).
   - It had a slow communication channel (50 bps), which allowed reception of ephemeris (i.e. satellite location) and clock information.
   - **Contribution to GPS**: demonstrating the operation of PRN signals for ranging.

Historical remarks

- All these efforts led to the development of the NAVSTAR Global Positioning System (GPS) Program, a Joint Program born in 1973.
- Instead of *angular measurements* to natural stars, the system should... ...use *ranging measurements* to artificial NAVSTARs.
- (Original) requirements:
  - User position errors $< 10 - 30$ meters;
  - Real-time navigation, even for users with high-dynamics;
  - Worldwide coverage;
  - Should tolerate interferences;
  - Users are not require to have accurate clocks;
  - Cold start should take minutes, not hours;
  - Antenna size should be small.
- The Russian satellite-based navigation system is called *GLObalnaya Navigasionnay Sputnikovaya Sistema*, GLONASS. Started in the Soviet Union in 1976.

Historical remarks

- GNSS history in a nutshell:
  - December **1973**, GPS program was approved.
  - **1976**, GLONASS program started.
  - **1978**, first GPS satellite launched.
  - October **1982**, the first GLONASS type spacecraft was launched.
  - August **1993**, GPS had 24 satellites in orbit.
  - September **1993**, GLONASS system was officially put into operation.
  - December **1993**, GPS initial operational capability was established.
  - February **1994**, the Federal Aviation Agency (FAA) declared GPS ready for aviation use.
  - **1995**, GLONASS constellation completed.
  - **2000**, the first *Beidou-1* satellite was launched. Beidou-1 is the regional Chinese system.
  - **2002**, the European Union (EU) agreed the launching of the *Galileo* program.
  - **2003**, Beidou-1 became operational (with 3 satellites, a fourth joined in 2007)

Historical remarks

- GNSS history in a nutshell:
  - **2005**, first Galileo experimental satellite launched.
  - November **2007** the 27 EU transportation ministers involved reached an agreement that it should be operational by "2013".
  - **2007**, first *Beidou-2* satellite launched. Beidou-2 is the Chinese GNSS.
  - **2011**, after some operation disruptions in the late 1990s, a full GLONASS constellation enabling world coverage was restored.
  - **2012**, a regional version of Beidou-2 was completed. Full coverage expected in 2020.
  - Since **2014**, a series of Full Operational Capability satellites have been launched to complete Galileo's constellation. Full service expected in 2020.
  - **2016**, Galileo becomes operational.
  - Currently, there are plans to modernize most GNSS signals/satellites.

Outline

GNSS operation

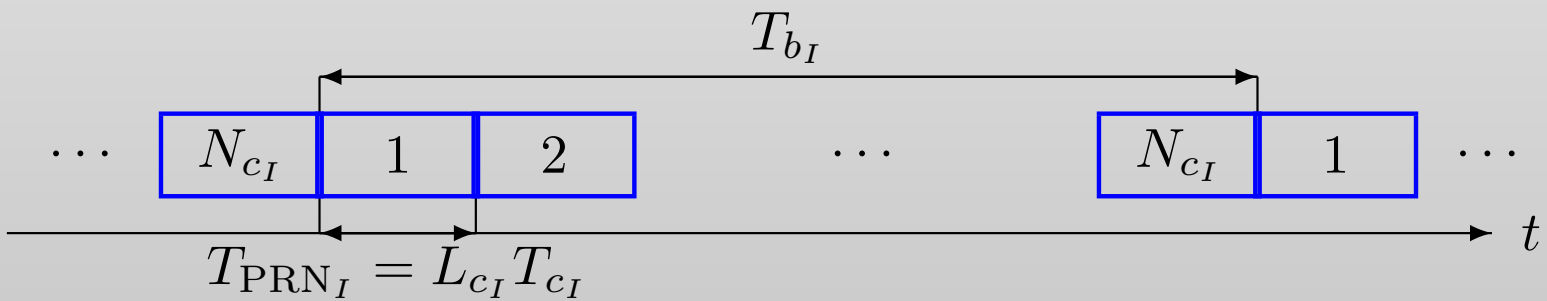
- GNSS satellites continuously transmit navigation signals at two or more frequencies in L band.
- GNSS receivers process all or some of the signals transmitted by satellites:
  - Single-frequency receivers,
  - Dual-frequency receivers, or
  - Triple-frequency receivers.
- These signals have two main goals:
  1. Enable accurate ranging for the user. This would allow estimation of Observables for a given satellite.
  2. Transmit the navigation data to the user with a convenient rate and ensuring and acceptable Bit and Word Error Rate. This would allow users to compute the satellite coordinates at any epoch, used in Navigation Solution algorithms to estimate PVT.

- The complex baseband model of the CDMA signal transmitted by the i-th satellite reads as

$$s_{T,i}(t) = s_{I,i}(t) + j s_{Q,i}(t) \ ,$$

where the inphase component is defined as

$$s_{I,i}(t) = \sqrt{2P_I} \sum_{m_I=-\infty}^{\infty} b_{I,i}(m_I) \sum_{u_I=1}^{N_{c_I}} \sum_{k_I=1}^{L_{c_I}} c_{I,i}\left(k_I\right) g_I\left(t - m_I T_{b_I} - u_I T_{\mathrm{PRN}_I} - k_I T_{c_I}\right)$$



Similarly for the quadrature component...

Signal model

- A receiver observes signals from M satellites plus noise:

$$y(t) = \underbrace{\sum_{i=1}^{M} x_{\theta,i}(t)}_{x_\theta(t)} + \eta(t)$$

where

$$x_{\theta,i}(t) = \sqrt{2C_i} b_i(t - \tau_i(t)) c_i(t - \tau_i(t)) \cos(2\pi f_c(t - \tau_i(t)) + \phi_i)$$

with

- C_i the power of the i-th received signal,
- $b_i(\cdot)$ the data bits of the i-th navigation message,
- $c_i(\cdot)$ the spreading code of the i-th satellite,
- f_c the RF carrier frequency (varies if multifreq signals are considered),
- $\tau_i(t)$ the time-evolving delay of the i-th satellite, and
- ϕ_i a carrier-phase term introduced by the channel.

Signal model

- A receiver observes signals from M satellites plus noise.

$$y(t) = x_\theta(t) + \eta(t)$$

where

$$x_\theta(t) = \sum_{i=1}^{M} \underbrace{\sqrt{2C_i}}_{\alpha_i} b_i(t-\tau_i(t)) c_i(t-\tau_i(t)) \cos(2\pi f_c(t-\tau_i(t)) + \phi_i)$$

- Doppler frequency results from the first-order term in the Taylor expansion of $\tau_i(t)$ as

$$f_{d,i} = -\frac{f_c}{c}\frac{d\tau_i(t)}{dt}$$

with $c \approx 3 \cdot 10^8$ m/s being the speed of light.

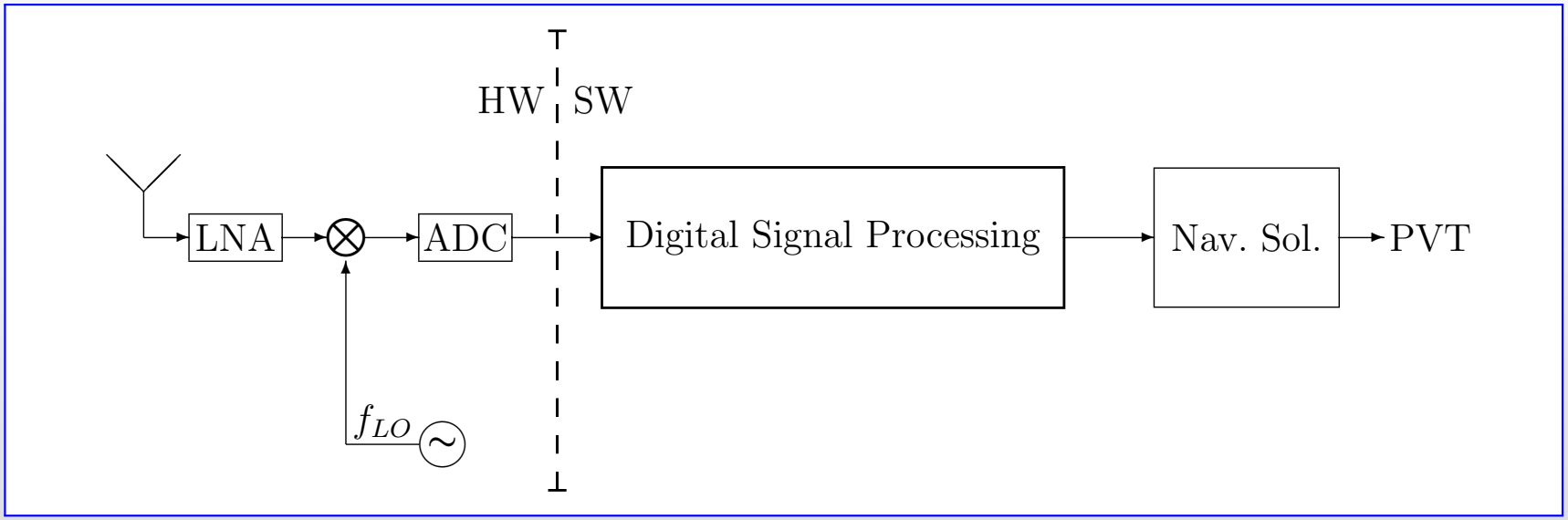
- $\boldsymbol{\theta}$ includes the unknown parameters of the model (e.g. delay, Doppler, and amplitude):

$$\boldsymbol{\theta}^\top = (\boldsymbol{\theta}_1^\top, \ldots, \boldsymbol{\theta}_M^\top) \quad \text{s.t.} \quad \boldsymbol{\theta}_i = (\alpha_i, \phi_i, \tau_i, f_{d_i})^\top$$

GNSS Receivers

- Summary of the building blocks of a GNSS receiver:
  - **RF front-end**, observes the GNSS signal at the antenna, amplifies it and brings it to baseband after filtering.
  - **Digital signal processing**, detects presence of satellites and estimates relevant parameters of the signal. Navigation message demodulation.
  - **Navigation solution**, computes receiver's position from a set of pseudoranges.
- The baseband processing of a GNSS receiver consists of a two-steps process:

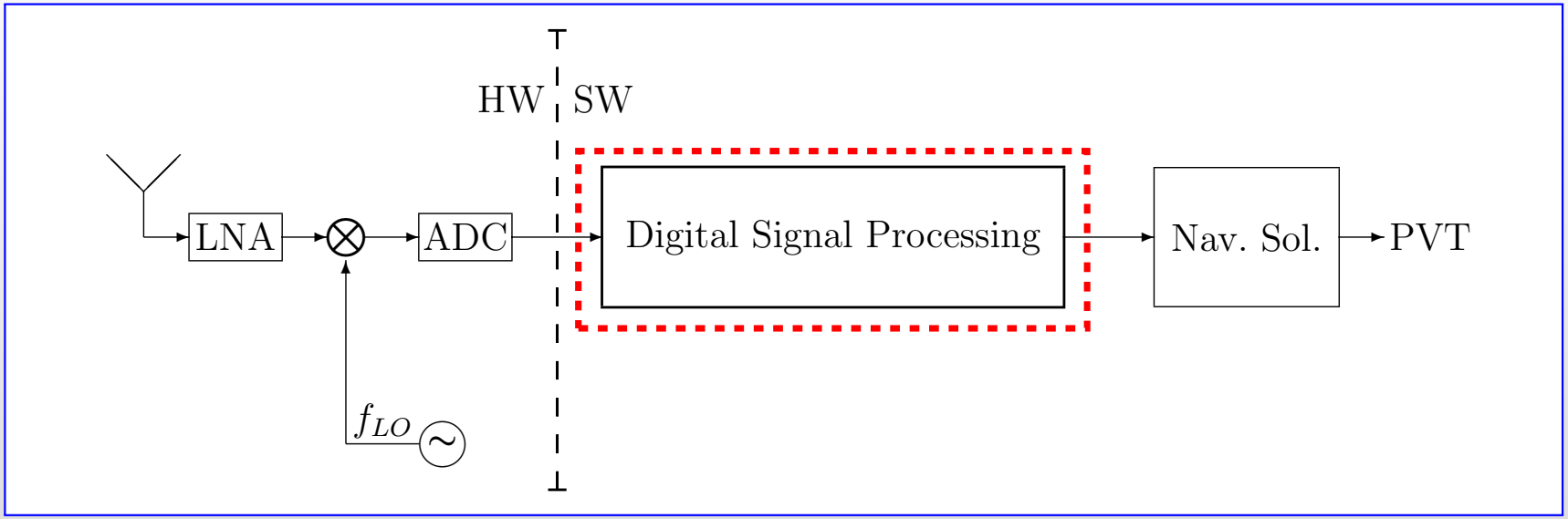
2-steps procedure: $\underbrace{\text{Time delay estimates} \Rightarrow \text{Pseudoranges}}_{\text{Synchronization}} \Rightarrow \text{Position}$



- Simplified scheme of a GNSS receiver.

HW : Amplification, downconversion and digitation.

SW : $\underbrace{\text{Time delay estimates} \Rightarrow \text{Pseudoranges}}_{\text{Synchronization}} \Rightarrow \text{PVT solution}$



$$y[n] = \sum_{i=1}^{M} \sqrt{2C_i} b_i(nT_s - \tau_i) c_i(nT_s - \tau_i) \exp(2\pi(f_{\text{IF}} + f_{d,i})nT_s + \phi_i) + \eta[n]$$

- A GNSS receiver has two basic stages:

  Acquisition: Detect visible satellites and obtain a rough estimation of synchronization parameters.

  Tracking: Fine estimates of time-delays, Doppler-shifts and carrier-phases.

Acquisition

- To detect the presence of the i-th satellite (Detection problem):

$$\begin{aligned} \mathcal{H}_0 &: i\text{-th satellite is not present} \\ \mathcal{H}_1 &: i\text{-th satellite is present} \end{aligned}$$

- For the i-th satellite, if present, to provide an initial rough estimate of the delay and Doppler between the incoming code and the local replica of the code.

$$y[n] = \sum_{i=1}^{M} \sqrt{2C_i} b_i(nT_s - \tau_i) c_i(nT_s - \tau_i) \exp(2\pi(f_{\text{IF}} + f_{d,i})nT_s + \phi_i) + \eta[n]$$

- These coarse delay/Doppler estimates are fed to the tracking loops, which refine the estimates.
- In general, hypothesis testing builds a test statistic ($\mathcal{T}$) and compares it to a threshold (γ) to determine the preferred hypothesis:

$$\mathcal{T}(\mathbf{y}) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma$$

with $\mathbf{y} = (y[0], y[1], \ldots, y[N-1])^\top$.

Detection problem

- Acquisition is an hypothesis testing problem (if we know exactly the received waveform $x_{\theta,i}[n]$).
- In which case, we have to decide between two competing options

$$\begin{aligned} \mathcal{H}_0 &: y[n] = \eta[n] \\ \mathcal{H}_1 &: y[n] = x_{\theta,i}[n] + \eta[n] \end{aligned}$$

such that $n = 0, \ldots, N-1$ and

$$x_{\theta,i}[n] \triangleq \alpha_i c_i(n\mathrm{T}_s - \tau_i) \exp(j2\pi(f_{\mathrm{IF}} + f_{d,i})n\mathrm{T}_s + j\phi_i)$$

is the local replica generated at the receiver.

- Assuming the receiver knows the parameters $\boldsymbol{\theta}_i = (\alpha_i, \phi_i, \tau_i, f_{d_i})^\top$, which is never the case!

Detection/Estimation problem

- Acquisition is an hypothesis testing problem (if we do not know exactly the received waveform $x_{\hat{\theta},i}[n]$).
- In which case, we have to decide between two competing options

$$\begin{aligned} \mathcal{H}_0 &: y[n] = \eta[n] \\ \mathcal{H}_1 &: y[n] = x_{\theta,i}[n] + \eta[n] \end{aligned}$$

  such that $n = 0, \ldots, N-1$ and

$$x_{\hat{\theta},i}[n] \triangleq \hat{\alpha}_i c_i(n\mathrm{T}_s - \hat{\tau}_i) \exp(j2\pi(f_{\mathrm{IF}} + \hat{f}_{d,i})n\mathrm{T}_s + j\hat{\phi}_i)$$

  is the local replica generate at the receiver.
- The Generalized Likelihood Ratio Test (GLRT) is the optimal detection framework (in the maximum likelihood (ML) sense).
- GLRT estimates $\hat{\boldsymbol{\theta}}_i = (\hat{\alpha}_i, \hat{\phi}_i, \hat{\tau}_i, \hat{f}_{d_i})^\top$ through ML estimation (MLE).

Cross ambiguity function

- Given a set of N observations,

$$\mathbf{y} = (y[0], y[1], \ldots, y[N-1])^\top$$

the MLE of $\boldsymbol{\theta}$ is defined as

$$\hat{\boldsymbol{\theta}}_{\mathrm{ML}} = \arg\max_{\boldsymbol{\theta}} p(\mathbf{y}|\boldsymbol{\theta})$$

- In general, it is a commonly accepted assumption that noise samples are i.i.d. complex Gaussian, $\eta[n] \sim \mathcal{CN}(0, \sigma^2)$, in which case

$$\begin{aligned}
\hat{\boldsymbol{\theta}}_{\mathrm{ML}} &= \arg\min_{\boldsymbol{\theta}} \sum_{n=0}^{N-1} |y[n] - x_{\theta,i}[n]|^2 \\
&= \arg\min_{\boldsymbol{\theta}} \sum_{n=0}^{N-1} -2\,\mathrm{Re}\left\{y[n]x^*_{\theta,i}[n]\right\} + |x_{\theta,i}[n]|^2
\end{aligned}$$

Cross ambiguity function

- Taking derivative w.r.t. complex amplitude $a_i = \alpha_i e^{j\phi_i}$, one can obtain that

$$\hat{a}_i = \frac{1}{N}\sum_{n=0}^{N-1} y[n]c_i(n\mathrm{T}_s - \hat{\tau}_i)\mathrm{e}^{-j2\pi(f_{\mathrm{IF}}+\hat{f}_{d,i})n\mathrm{T}_s}$$

where

$$\sum_{n=0}^{N-1} c_i[n]c_i[n] = N$$

is the spreading code length (or ACF evaluated at its maximum value).

- We plug this complex amplitude estimate in the cost function

$$(\hat{\tau}_i, \hat{f}_{d_i}) \quad = \quad \arg\max_{\tau, f_d}\{|\mathcal{C}_i(\tau, f_d)|\}$$

with

$$\mathcal{C}_i(\tau, f_d) \triangleq \frac{1}{N}\sum_{n=0}^{N-1} y[n]c_i(n\mathrm{T}_s - \tau_i)\mathrm{e}^{-j2\pi(f_{\mathrm{IF}}+f_{d_i})n\mathrm{T}_s}$$

Cross ambiguity function

- GLRT results in maximization of the correlation between the received signal and a locally generated code:

$$\begin{aligned}(\hat{\tau}_i, \hat{f}_{d_i}) &= \arg\max_{\tau, f_d} \{|\mathcal{C}_i(\tau, f_d)|\} \\ \hat{\alpha}_i &= \left|\mathcal{C}_i(\hat{\tau}_i, \hat{f}_{d_i})\right| \\ \hat{\phi}_i &= \angle\mathcal{C}_i(\hat{\tau}_i, \hat{f}_{d_i})\end{aligned}$$

  where $\mathcal{C}_i(\tau, f_d)$ is known as the Cross Ambiguity Function (CAF)

$$\mathcal{C}_i(\cdot,\cdot) : \mathcal{X}_\tau \times \mathcal{X}_{f_d} \longmapsto \mathbb{C}$$

- $\mathcal{X}_\tau$ and $\mathcal{X}_{f_d}$ represent the set of possible code-delay and Doppler-shift values, respectively, which depend on the type of acquisition.

Cross ambiguity function

- The CAF is nothing but the correlation between $y[n]$ and the spreading code of the i-th satellite, at a given delay/Doppler pair (in discrete-time):

$$\mathcal{C}_i(\tau, f_d) = \frac{1}{N}\sum_{n=0}^{N-1} y[n]\underbrace{c_i(n\mathrm{T}_s - \tau_i)\exp\{-j2\pi(f_{\mathrm{IF}} + f_{d_i})n\mathrm{T}_s\}}_{\text{Local replica}} = \frac{\mathbf{y}\mathbf{c}_i^{\top}}{N}$$

  where N samples are used and gathered in $\mathbf{y}, \mathbf{c}_i \in \mathbb{C}^{1\times N}$ for convenient vector notation.

- T_{coh} is the coherent integration time, such that $N = T_{coh}f_s$. For instance, for GPS L1 C/A, we have that $T_{coh} = 1$ ms at least.

- The CAF is exploiting the *desirable* auto-/cross-correlation properties of PRN sequences.

CAF and acquisition

- Optimization of the CAF-based cost function, provides reliable estimates of $\boldsymbol{\theta}$ only when the satellite is present AND the local replica is aligned with the received signal.
- Therefore, a detection threshold needs to be specified to determine which $(\hat{\tau}_i, \hat{f}_{d_i})$ pairs yield to relevant CAF values.
- We select the CAF envelope

$$\mathcal{T}(\mathbf{y}) \triangleq |\mathcal{C}_i(\tau, f_d)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma$$

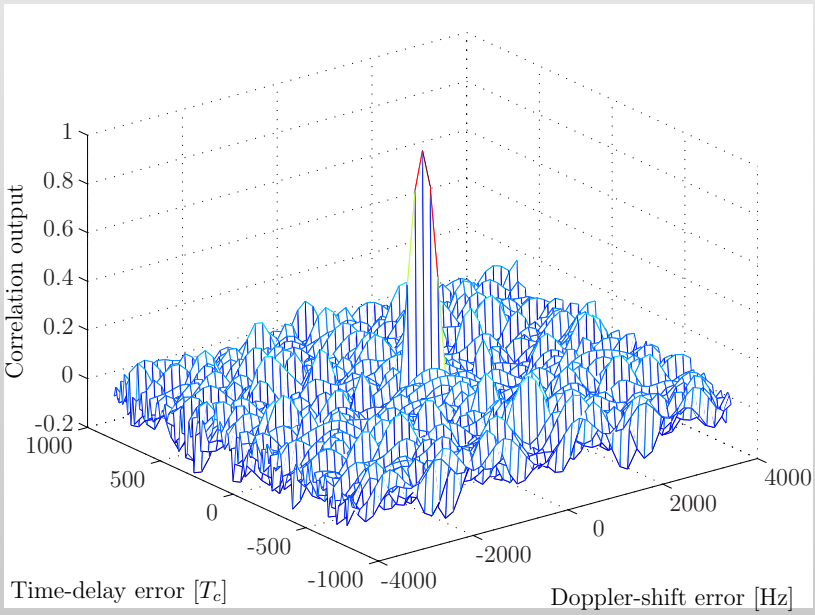
  as the test statistic (others can be considered!)
- Notice that

$$|\mathcal{C}_i(\tau, f_d)|^2 = \mathcal{C}_{R,i}^2(\tau, f_d) + \mathcal{C}_{I,i}^2(\tau, f_d)$$

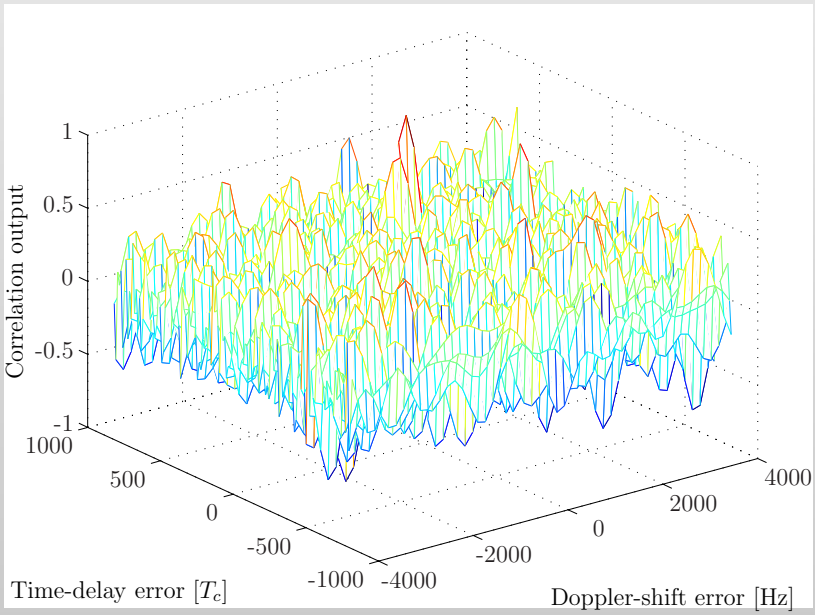
  with $\mathcal{C}_{R,i}(\tau, f_d) = \mathrm{Re}\{\mathcal{C}_i(\tau, f_d)\}$ and $\mathcal{C}_{I,i}(\tau, f_d) = \mathrm{Im}\{\mathcal{C}_i(\tau, f_d)\}$

CAF and Acquisition

- Detection is performed setting a threshold according to a required false alarm probability.
- The search space is a delay/Doppler grid where the CAF is evaluated (several strategies exist...)



(a) satellite is present



(b) satellite is not present

CAF and ROC

- A decision is made based on

$$\mathcal{T}(\mathbf{y}) \triangleq |\mathcal{C}_i(\tau, f_d)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma$$

  which involves setting a threshold.

- $\mathcal{T}(\mathbf{y})$ is a random variable, primarily characterized by two probability density functions (PDFs), and their corresponding complementary cumulative distributions
  - **Detection probability** ($P_d(\gamma)$): the probability of correctly determining $\mathcal{H}_1$ if the satellite is present

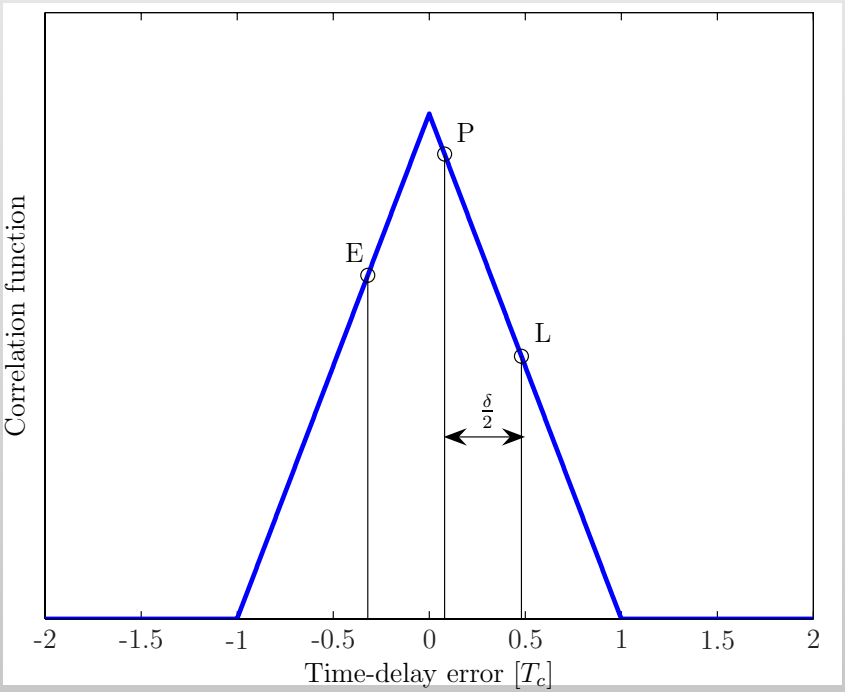
$$P_d(\gamma) = P(\mathcal{T}(\mathbf{y}) > \gamma \mid \mathcal{H}_1)$$

  - **False alarm probability** ($P_{fa}(\gamma)$): the probability of accepting $\mathcal{H}_1$ when the satellite is not present

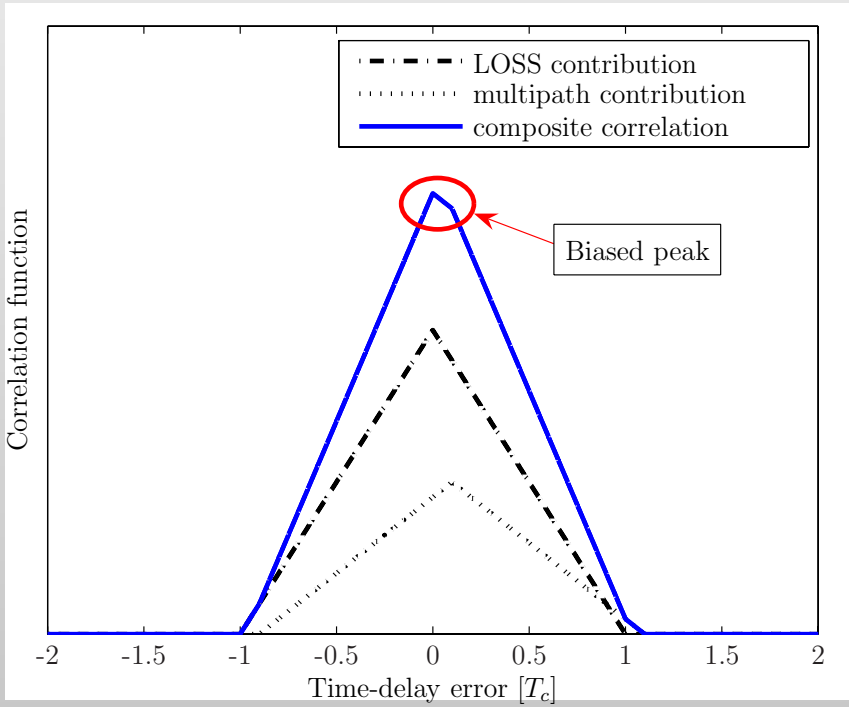
$$P_{fa}(\gamma) = P(\mathcal{T}(\mathbf{y}) > \gamma \mid \mathcal{H}_0)$$

Tracking

- Tracking loops can be seen as a refinement of acquisition strategies, with a reduced search space. Most receivers consider
  - PLL for $\hat{f}_{d_i}$, and
  - DLL for $\hat{\tau}_i$ (combining ELP samples in different ways)

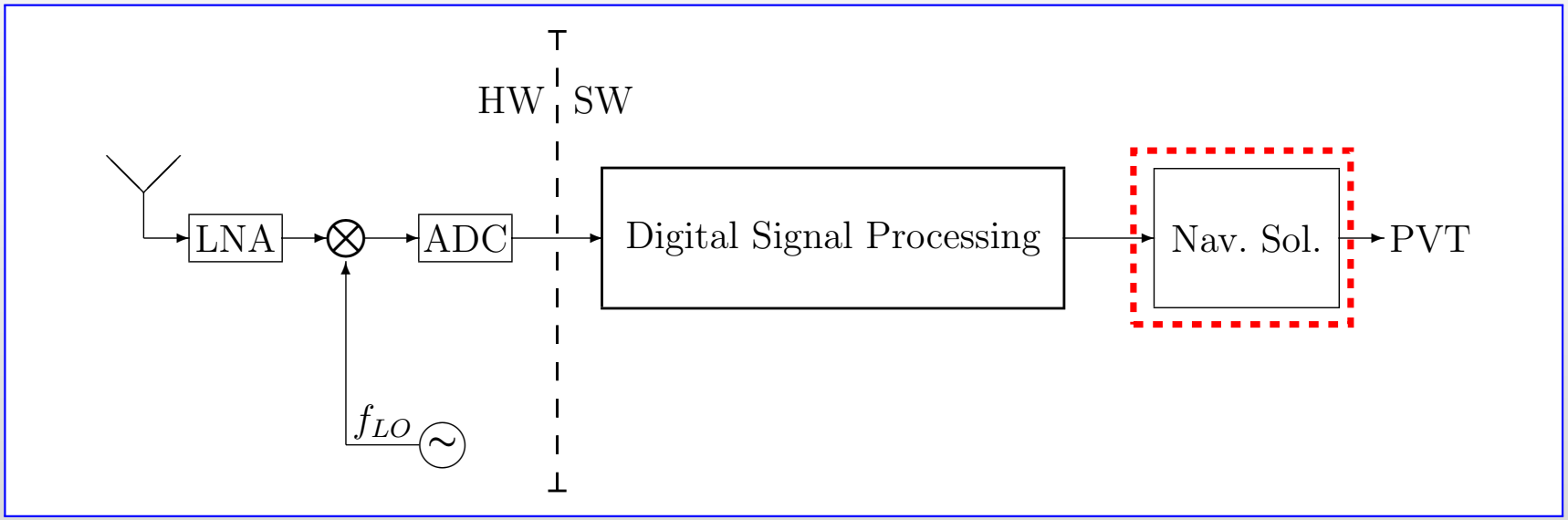


(a) DLL-based techniques

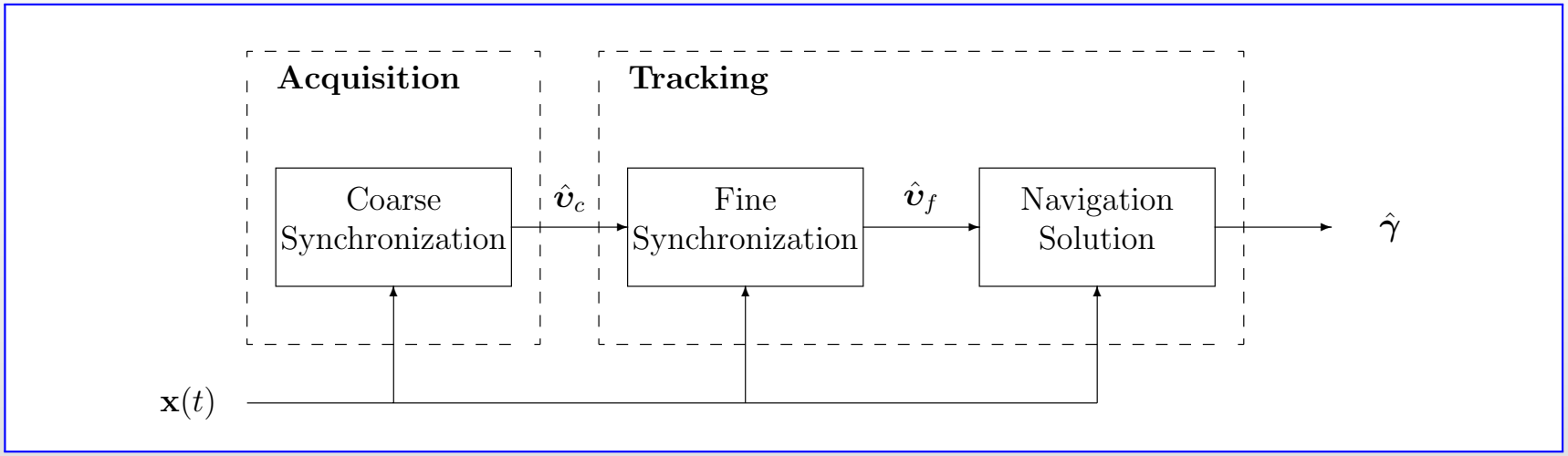


(b) The multipath problem

Navigation



- Conventional positioning is a 2-steps procedure:
  1. With the estimated sync. parameters we have a measure of the relative distance between the satellites and the receiver (*pseudoranges*).
  2. These distances are used to solve a geometrical problem referred to as *trilateration*. Typically solved through a Weighted Least Squares or a Kalman filter.



$\hat{\boldsymbol{\upsilon}}$: Estimates of synchronization parameters.

$\hat{\boldsymbol{\gamma}}$: PVT solution.

- Summary of a receiver's tasks:
  - Detect satellites and acquire their signal parameters (coarse estimates).
  - Concurrent tracking of synchronization parameters (fine estimates) and position calculation by trilateration.

Outline

Types of Interferences

- Unintentional interferences from other communication systems.

$$y(t) = x_\theta(t) + i(t) + \eta(t)$$

- Intentional jamming, aimed at denying GNSS service.

$$y(t) = x_\theta(t) + i(t) + \eta(t)$$

- Spoofing, aimed at counterfeiting satellite signals to deceive a receiver.

$$y(t) = x_\theta(t) + x_{\tilde{\theta}}(t) + \eta(t)$$

- Nature-made interferences: causing severe perturbations of the signal emitted by the satellites.

$$y(t) = x_{\tilde{\theta}}(t) + \eta(t)$$

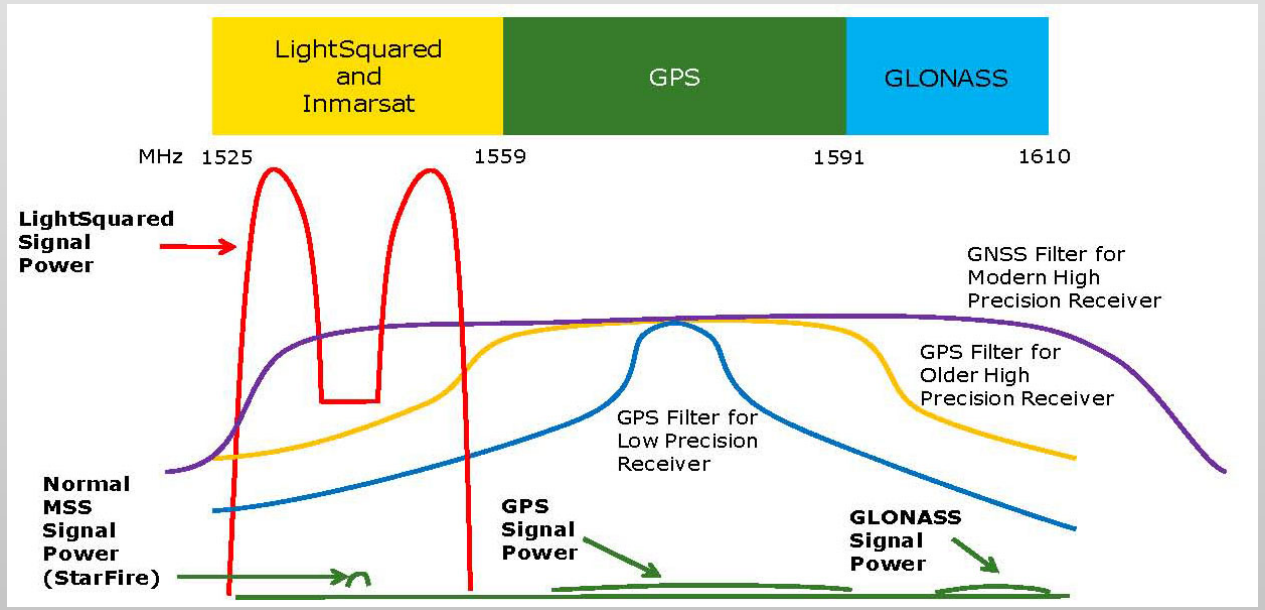
Types of Interferences (Unintentional interferences)

1. Out-of-band interference caused by harmonics and intermodulation products, as for example from
   - terrestrial digital video broadcasting (DVB-T),
   - very-high frequency (VHF) omnidirectional range (VOR) plus instrument landing system (ILS) signals,
   - multicarrier modulated satellite communication systems, and
   - amateur radio services.

2. In-band interference, including
   - civilian and military terrestrial navigation systems as distance measuring equipment (DME) and tactical air navigation (TACAN),
   - military spread-spectrum communication systems like the joint tactical information distribution system (JTIDS)
   - multifunctional information distribution system (MIDS), and
   - wind profiler radars and civilian radars (1215–1400 MHz)

Types of Interferences (Unintentional interferences)

- LightSquared was a company that planned to deploy a 4G LTE wireless broadband communications network
- Hybrid terrestrial-satellite coverage across US.
- GNSS community raised serious interference concerns, which prevented deployment.



Types of Interferences (Intentional jamming)

- Achieved by using devices that can generate powerful signals in the GNSS band.
- A big class of jammers belong to the personal privacy devices (PPD) that are used as in-car jammers to avoid a vehicle being tracked (e.g. road tolling, fleet control, etc.)
- Effective ranges in the order from a few tens of meters to kilometers.
- Although illegal to sell jammers (in US and many countries in EU), they can be purchased online for few tens of dollars.
- Several jamming incidents have been reported involving the disruption of GNSS services in local harbors and airport traffic control management.

Types of Interferences (Unint./int. interferences)

- A useful model is to assume that the interference decreases the effective carrier-to-noise density ratio:

$$\frac{C}{N_{0,\text{eff}}} = \frac{C \int_{-B/2}^{B/2} X(f)df}{N_0 \int_{-B/2}^{B/2} X(f)df + C_I \int_{-B/2}^{B/2} X(f)I(f)df}$$

  where
  - $X(f)$ and $I(t)$ are the spectrum of the desired and interfering signals, respectively;
  - B is the receiver's frontend bandwidth;
  - C, C_I, and N_0 are the received signal, interference, and noise powers.
  - Model assumes that amplifiers, filters and mixers operate in their linear region.
- The higher the jamming power and the better the interfering signal matches the satellite signal, the larger the increase of the noise.

Types of Interferences (Unint./int. interferences)

- The effects can be summarized as:
  - denial of acquisition and false signal detection,
  - loss of tracking,
  - increased pseudorange errors,
  - high demodulation error rates, and
  - continuous cycle slips.
- We'll get back to this later.

Types of Interferences (Intentional interferences)

- Several papers have addressed the problem of characterizing the jamming signal $i(t)$.
- From the analysis, it emerged that most jammers used in a civil context broadcast frequency modulated signals with an almost periodic behavior.
- Deviations from a perfectly periodic behavior are due to drifts in the local oscillators used for the signal generation.
- The signal center frequency varies according to a periodic pattern that, in most cases, corresponds to a saw-tooth function.

Types of Interferences (Intentional interferences)

- A jammer can be generically modeled as

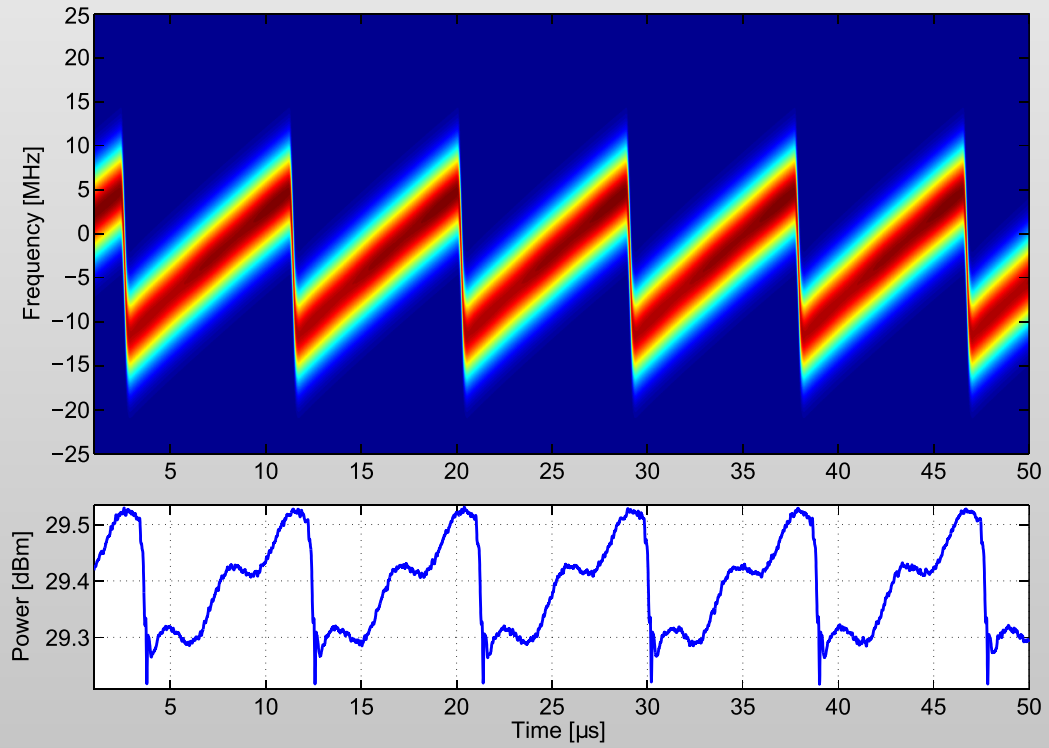
$$i(t) = \sqrt{2C_I}\cos(2\pi(f_{\mathrm{RF}} + f_{\mathrm{I}}(t))t + \varphi_I)$$

where

- $f_{\mathrm{I}}(t)$ is the instantaneous frequency of the jammer,
- defines a practically periodic frequency pattern which is characterized by a sweep range,
- the maximum and minimum values of $f_{\mathrm{I}}(t)$, $f_{\max}$, and $f_{\min}$, play a fundamental role since they determine the spectral overlap between GNSS and jamming signals.

Types of Interferences (Intentional interferences)

- The spectrogram of the signal emitted by a (true) cigarette lighter jammer.
- $f_{\mathrm{I}}(t)$ defines a piecewise linear pattern with a sweep range of 16.7 MHz and a sweep period of about 8.9 μs.



Types of Interferences (Intentional interferences)

- The shorter the sweep period, the more difficult it is to mitigate the impact of the jammer.
- Fast frequency varying signals are more difficult to track.
- Sweep periods are typically around 10 μs whereas sweep ranges are usually in the 10–40 MHz interval.

Types of Interferences (Intentional interferences)

Classification of jammers depending on emitted signals:

Class I the jammer transmits a continuous wave (CW) signal.

$$f_{\mathrm{I}}(t) = f_{\mathrm{I}} \qquad (\mathrm{constant\,jamming\,frequency})$$

Class II single saw-tooth chirp signals; the jammer transmits a frequency-modulated signal with a saw-tooth time-frequency (TF) evolution.

$$f_{\mathrm{I}}(t) = \{\mathrm{Periodic\,saw-tooth}\}$$

Types of Interferences (Intentional interferences)

Classification of jammers depending on emitted signals:

Class III multi-saw-tooth chirp signals; the device transmits a frequency-modulated signal but its TF evolution is more complex and it is determined by the combination of several saw-tooth functions.

$$f_{\mathrm{I}}(t) = \{\mathrm{Periodic\,saw-tooth}\}$$

Class IV chirp with signal frequency bursts; the device transmits a frequency-modulated signal and frequency bursts are used to enlarge the frequency.

$$f_{\mathrm{I}}(t) = \{\mathrm{Frequency\,jumps}\}$$

Types of Interferences (Intentional interferences)

Classification of jammers depending on device characteristics:

Group I cigarette lighter jammers; the device is designed to be plugged into an automotive cigarette lighter with a 12-V power supply.

Group II SubMiniature version A (SMA) battery jammers; the device is powered by a battery and it is connected to an external antenna through an SMA connector.

Group III non-SMA battery jammers; the device is powered by a battery and uses an integrated antenna for transmission.

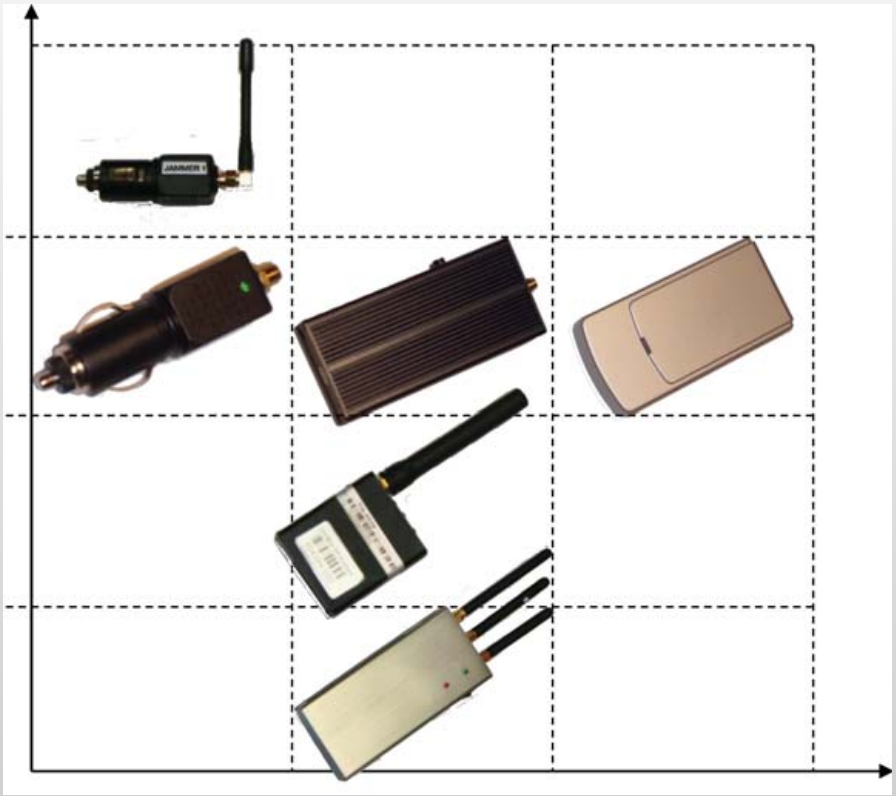
Types of Interferences (Intentional interferences)

Class I: continuous wave signal

Class II: single saw-tooth chirp signal

Class III: multi saw-tooth chirp signal

Class IV: chirp with frequency bursts



Group 1: Cigarette Lighter Jammers

Group 2: SMA – Battery Jammer

Group 3: Non SMA – Battery Jammer

Types of Interferences (Spoofing)

- A jammer can use a number of different signal modulations with high power to affect the availability of the GNSS satellite signals.
- A spoofer attempts to deceive the GNSS user navigation by transmitting signals with the same characteristics as the legitimate GNSS satellite signals.
- A spoofed GNSS receiver will then report a false position and/or timing information from its true one, also depending on the type of the attack accompanied with a confirmed integrity check.
- Although there are no proven records of intentional spoofing attacks, several demonstrations have indicated that spoofing is feasible with todays grade of software defined radios (SDR) and GNSS simulators.

[She12] D. Shepard, J. Bhatti, and T. Humphreys, Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle, GPS World, 2012. [Online]. Available: http://gpsworld.com/drone-hack/, [Accessed: 02-Jan-2016].

Types of Interferences (Spoofing)

- For simplicity, let us focus on a single satellites signal, thus neglecting the contribution of the rest of satellites.
- Realistic assumption, considering that GNSS systems employ spreading codes with a high processing gain and relatively small cross-correlation among satellite codes. Therefore, the influence of other satellites can be considered as Gaussian noise and included in the thermal noise term since those signals are well below the noise floor.
- The signal model is then

$$y(t) = x_\theta(t) + \eta(t)$$

where

$$x_\theta(t) = \sqrt{2C} b(t - \tau(t)) c(t - \tau(t)) \cos(2\pi(f_{\mathrm{RF}} + f_d(t))t + \phi)$$

Types of Interferences (Spoofing)

- Structured interference: a spoofer mimics legitimate GNSS signals but modifies some of its parameters

$$x_{\tilde{\theta}}(t) = \sqrt{2C_S}\tilde{b}(t-\tilde{\tau}(t))c(t-\tilde{\tau}(t))\cos(2\pi(f_{\mathrm{RF}}+\tilde{f}_d(t))t+\tilde{\phi})$$

- A receiver observes a combination of two (very similar) signals:

$$y(t) = \underbrace{x_\theta(t)}_{\text{legitimate signal}} + \underbrace{x_{\tilde{\theta}}(t)}_{\text{spoofer signal}} + \eta(t)$$

- A spoofing attack can involve:
  - Navigation message attack: while matching delay/Doppler to the legitimate signal, this attack aims at modifying navigation data bits.
  - Code level attack: aims at taking over the receiver ultimate PVT solution by substitution of legitimate signal(s)

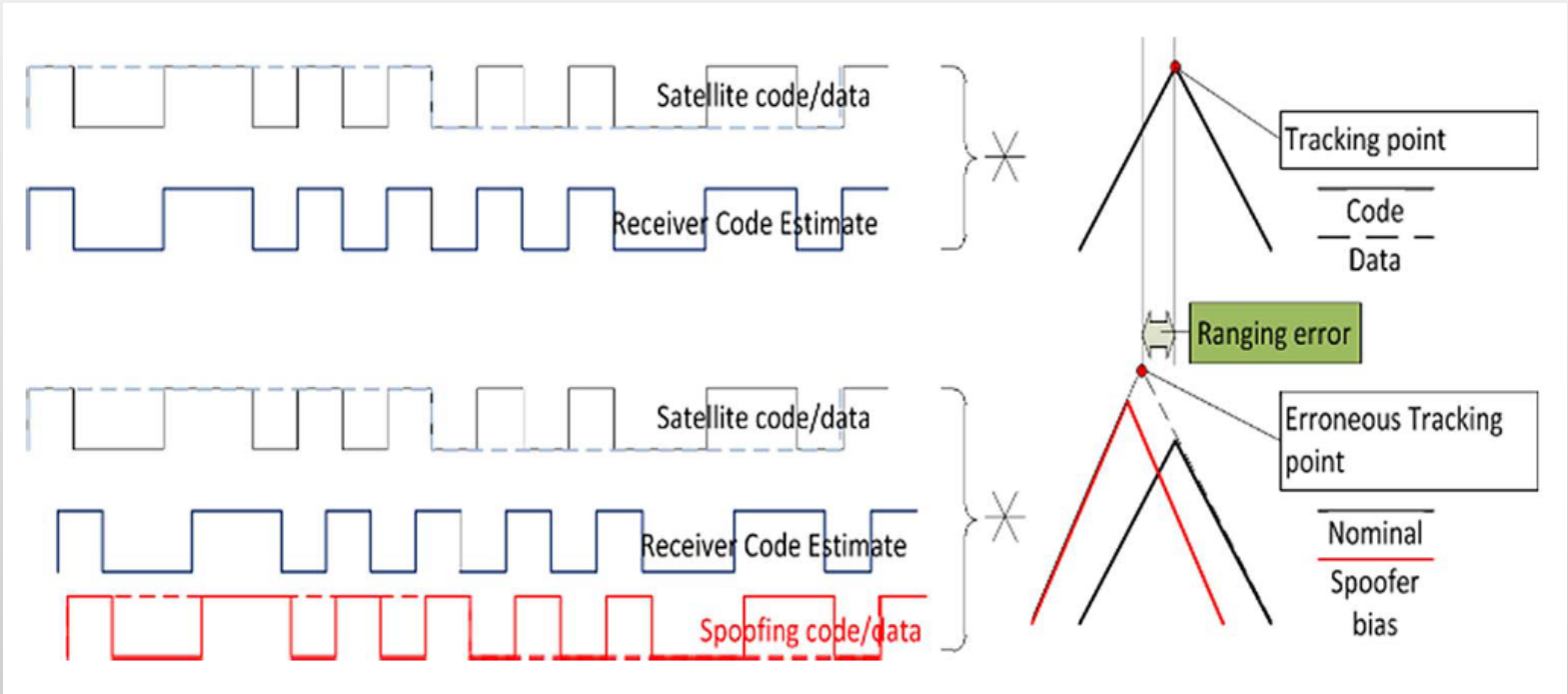
Types of Interferences (Spoofing)

- Navigation message attack: Navigation data involving higher risk.

Navigation data parameter	**Type of impact**
Clock and ephemeris (CED)/ time of ephemeris (ToE) data	Ranging errors (RE), position, velocity and time (PVT) errors
Health	Denial of ranging
User/signal in space ranging accuracy (e.g. URA/ SISA)	Denial of PVT with receiver autonomous integrity monitoring (RAIM)
Galileo system time (GST), coordinated universal time (UTC)	Timing errors
GPS Galileo time offset (GGTO)	Multi space vehicle RE
Data integrity, e.g. cyclic redundancy code (CRC)	Denial of navigation data
Ionospheric corrections	Ranging/PVT errors

Types of Interferences (Spoofing)

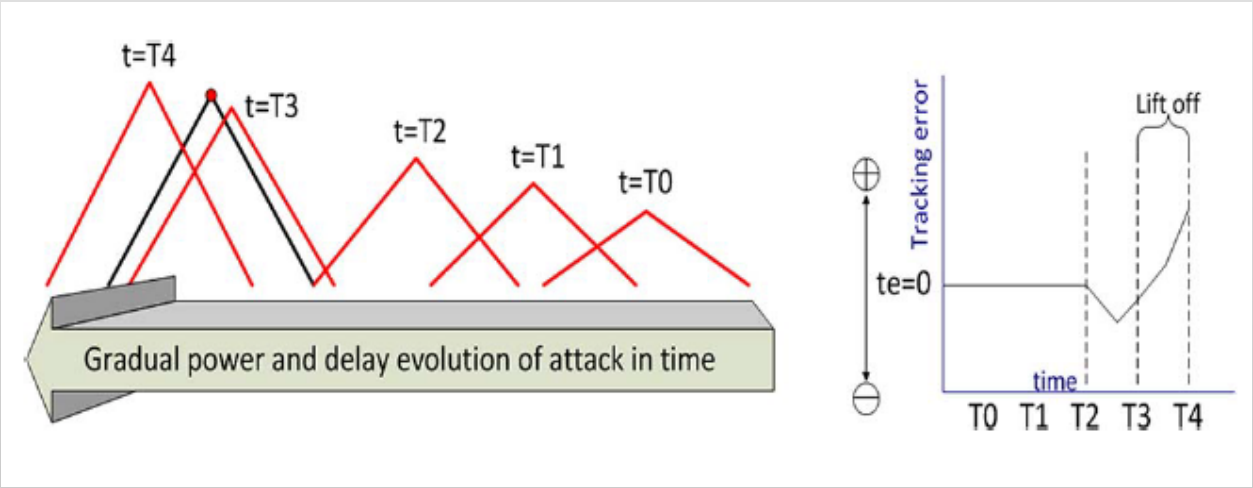
- Code level attack: conceptual illustration



- Authentic tracking point (top) versus spoofed tracking point (bottom)

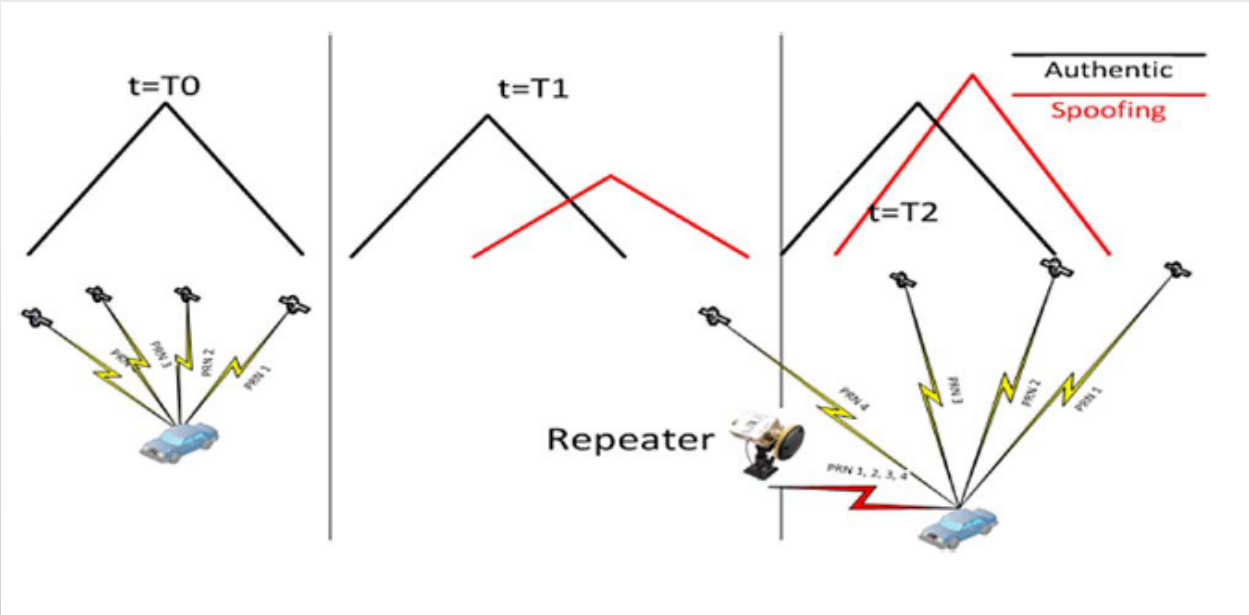
Types of Interferences (Spoofing)

- Code level attack: spoofing cases (I)
  - Lift-off-delay: spoofer approaches the authentic signal with a relative delay and gradually adjusts its power. When aligned, increases power level to take over control of the tracking loops.
  - Lift-off-aligned: similar but spoofer initially aligned to legitimate signal.



Types of Interferences (Spoofing)

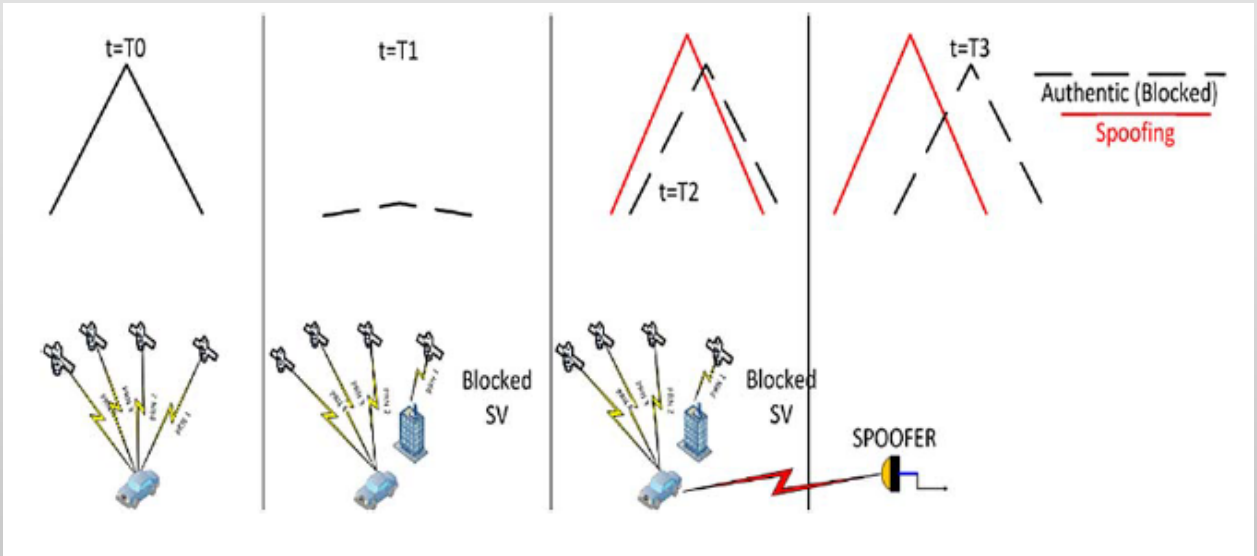
- Code level attack: spoofing cases (II)
  - Meaconing: repeat signal with a different delay and varying power. Simple, but can potentially spoof encrypted signals!



  - Selective delay: spoof specific satellite(s) using directional antennas.

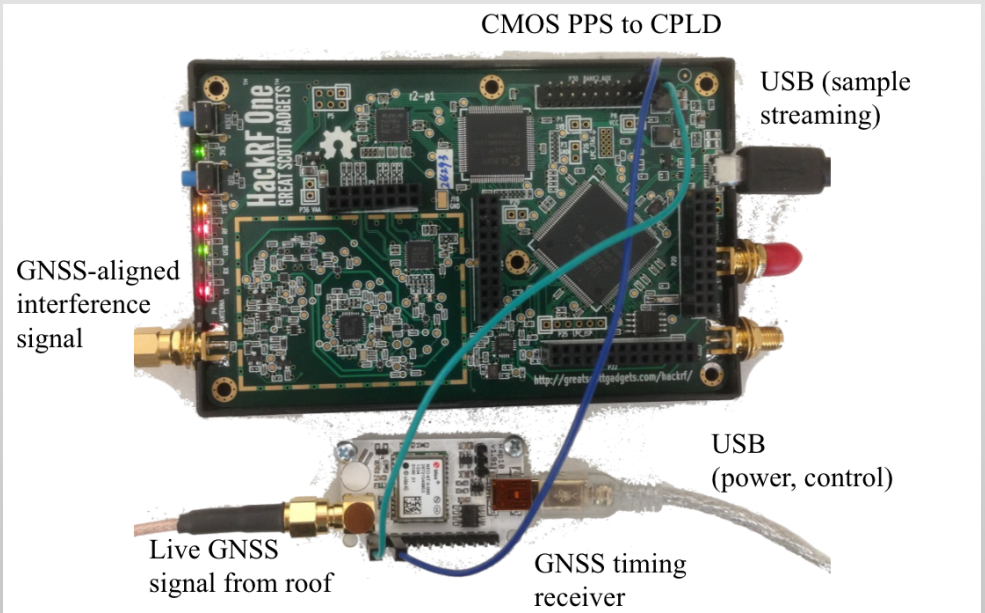
Types of Interferences (Spoofing)

- Code level attack: spoofing cases (III)
  - Non-line-of-sight spoofing: supersede signals from obstructed satellites.
  - Jam-and-Spoof: force the receiver into acquisition (jamming till loss of lock) and supersede legitimate signals.



Types of Interferences (Spoofing)

- Compared to jammers, the spoofer attack is more sophisticated.
- However, with the advent of SDR and GNSS signal simulators, spoofing is doable.
- Potential impact of a spoofing attach is extremely high since the aim is not to disrupt GNSS service but to supersede it.



[Cur17] J. Curran, M. Bavaro, P. Closas, and M. Navarro, "On the Threat of Systematic Jamming of GNSS," in InsideGNSS magazine, July/August 2017.

Types of Interferences (Ionospheric scintillation)

- Primarily, we care about ionospheric scintillation, perturbing carrier-phase observations in Polar and Equatorial regions.
- The ionosphere is a region of the upper atmosphere, from about 85 km to 600 km altitude, that is ionized by solar radiation.
- It constitutes a plasmatic media that causes a group delay of the modulation and a phase advance on the electromagnetic waves that propagate through it.
- The recombination of waves after propagation can be constructive or destructive, and the resulting signal at the receiver antenna may present rapid variations of phase and amplitude.

Types of Interferences (Ionospheric scintillation)

- Particularly challenging in Polar and Equatorial regions.

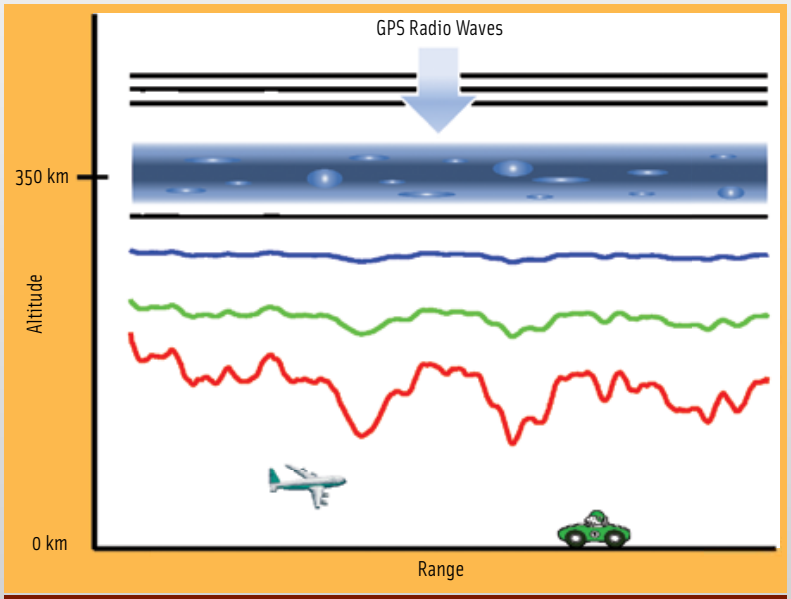


FIGURE 2 Radio wave propagation through a disturbed ionosphere. The horizontal curves represent signal amplitude. Irregularities in the ionosphere introduce phase shifts that become amplitude perturbations as the wave propagates below the ionosphere.

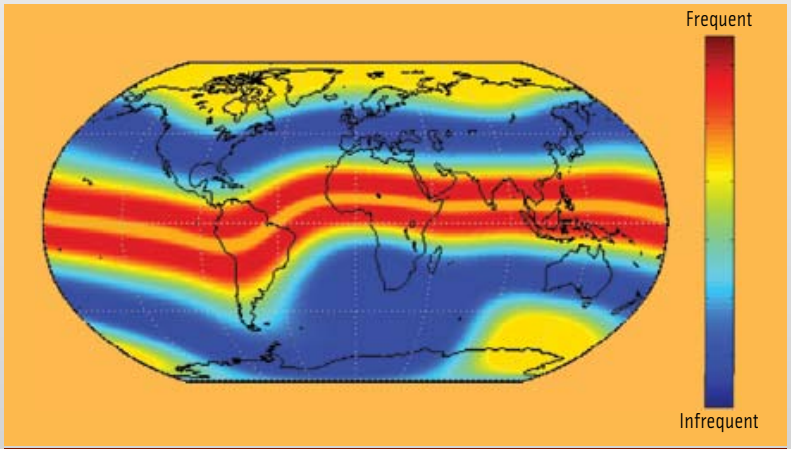
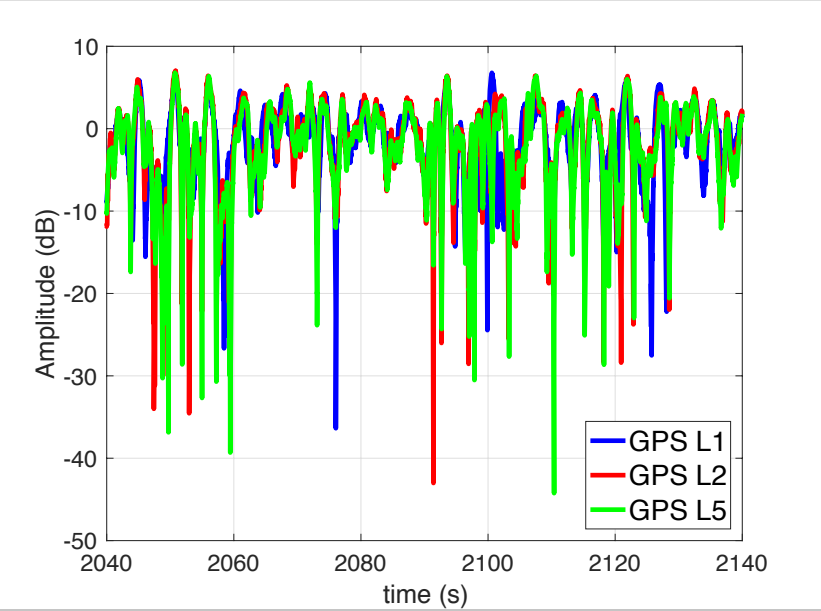


FIGURE 1 Scintillation map showing the frequency of disturbances at solar maximum. Scintillation is most intense and most frequent in two bands surrounding the magnetic equator, up to 100 days per year. At poleward latitudes, it is less frequent and it is least frequent at mid-latitude, a few to ten days per year.

[Kin09] P.M. Kintner, T. Humphreys and J. Hinks, "GNSS and Ionospheric Scintillation. How to survive the next solar maximum", Inside GNSS, July/August 2009.

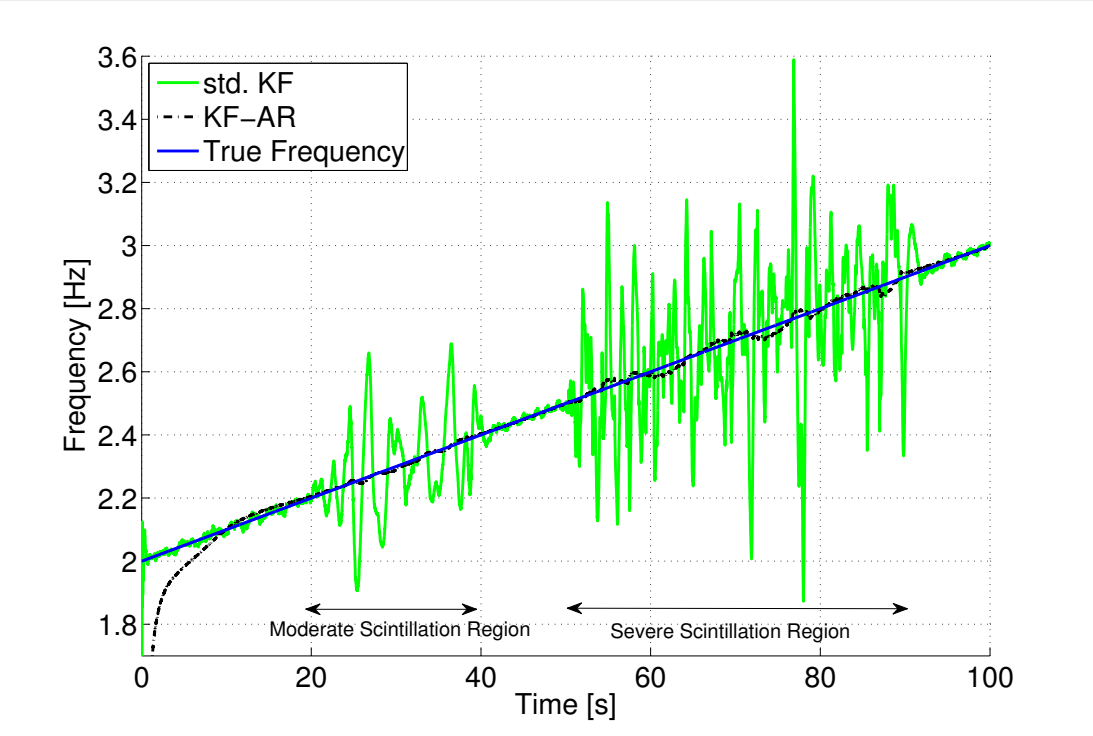
Types of Interferences (Ionospheric scintillation)

- Those amplitude fades and phase changes happen in a simultaneous and random manner, but there exists a correlation between both disturbances (canonical fades).
- That is, the largest amplitude fades are regularly associated with very rapid phase inversions in the processor, which is a very challenging carrier tracking scenario.



Types of Interferences (Ionospheric scintillation)

- May cause loss of lock in the tracking loops depending on intensity.



(Do not pay too much attention to the legend)

[Vil17] J. Vilà-Valls, P. Closas, M. Navarro, C. Fernández-Prades, "Are PLLs Dead? A Tutorial on Kalman Filter-based Techniques for Digital Carrier Synchronization," IEEE Aerospace and Electronic Systems Magazine, to appear 2017

Types of Interferences (Ionospheric scintillation)

- It is useful to have generative models for scintillation interference.
- The most widely used ionosperic scintillation models are:
  - WideBand MODel (WBMOD) provides the global distribution and synoptic behavior of the electron-density irregularities that cause scintillation, and a propagation model that calculates the effects these irregularities will have on a given system.
  - Global Ionospheric Scintillation Model (GISM), based on a phase screen technique driven by the NeQuick electron density climatological model.
  - Cornell Scintillation Model (CSM), based on a statistical model and the proper shaping of the spectrum of the entire complex scintillation signal.

The CSM has been embedded in the so-called Cornell Scintillation Simulation Matlab toolkit, which is available at `http://gps.ece.cornell.edu/tools.php`

Types of Interferences (Ionospheric scintillation)

- The severity of the scintillation is traditionally quantified by two indices:
  - an amplitude scintillation index, denoted S_4;

$$S_4 = \sqrt{\frac{\mathbb{E}({\rho_s}^4) - (\mathbb{E}(\rho_s^2))^2}{(\mathbb{E}(\rho_s^2))^2}} \quad \begin{cases} S_4 \leq 0.3 & (\text{weak}) \\ 0.3 < S_4 \leq 0.6 & (\text{mod.}) \\ 0.6 < S_4 & (\text{sev.}) \end{cases}$$

  - a phase scintillation index, denoted σ_ϕ.
- The indices are computed on a per-signal basis and indicate average intensity of the signal variations over the preceding minute.
- They have been used for some decades and as a result there exist rich databases of historical data for a wide range of observation points.

Types of Interferences (Ionospheric scintillation)

- Scintillation effect can be modeled as a multiplicative channel

$$x_{\tilde{\theta}}(t) = \xi_s(t) x_{\theta}(t)$$

such that $y(t) = x_{\tilde{\theta}}(t) + n(t)$ is the received signal.

- The disturbance caused by ionospheric scintillation is defined as

$$\xi_s(t) = \rho_s(t) e^{j\theta_s(t)},$$

with envelope and phase components, $\rho_s(t)$ and $\theta_s(t)$.

- When simulating scintillation, $\rho_s(t)$ and $\theta_s(t)$ would be generated by the aforementioned generative models (e.g., CSM).

[Vil15] J. Vilà-Valls, P. Closas, C. Fernández-Prades, J. A. López-Salcedo, G. Seco-Granados, "Adaptive GNSS Carrier Tracking under Ionospheric Scintillation: Estimation vs Mitigation," IEEE Communications Letters, Vol. 19, No. 6, pp. 961-964, 2015.

Summary (so far, I)

- Positioning systems are paramount in many applications and services.
- GNSS technology is the *de facto* standard, when available.
- Unintentional or malicious interferences are a real threat.
  - Unintentional interferences
  - Intentional jamming
  - Spoofing
  - Nature-made interferences
- Luckily, interference sources can be classified and modeled mathematically $\Rightarrow$ We can design countermeasures
- Other than those vulnerabilities, GNSS is awesome!

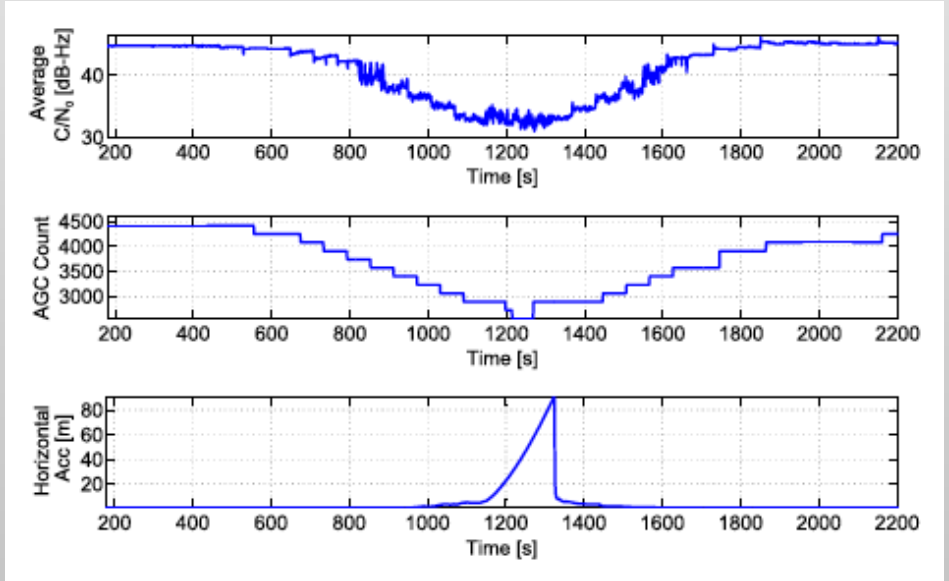
Outline

Jamming impact

- In most cases, the goal of malicious jammers is to totally deny GNSS-based services in a certain geographical area.
- Despite the clear threat posed by a jammer broadcasting a sufficiently strong power, such a scenario is highly detectable.
- Intermediate power values turn out to be the most dangerous cases, since sometimes they might be severe enough to significantly decrease the receiver performance, but not severe enough to make the receiver lose lock or to prevent the acquisition of satellite signals.

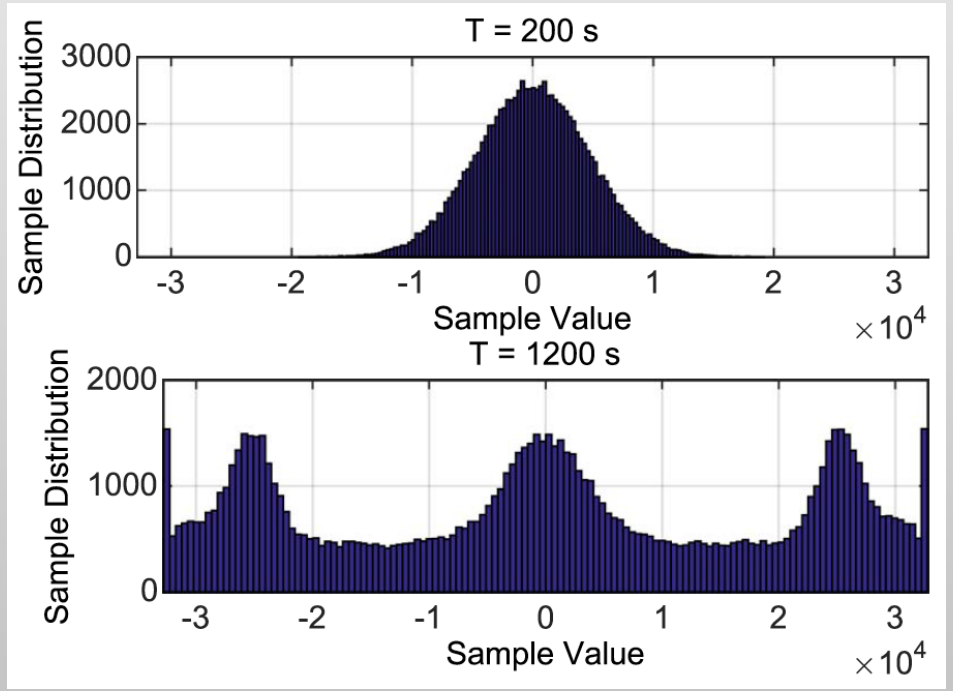
Jamming impact

- Impact of a jamming signal on a high-sensitivity GNSS receiver. Different metrics sensitive to the jamming signal are provided.
- A cigarette lighter jammer was used to disturb GNSS signal reception in a controlled environment.
- The power emitted by the jammer was controlled using a variable attenuator and J/N_0 was varied between 55 and 92 dB-Hz.



Jamming impact (Front-end)

- Multibit ADC require automatic gain control (AGC)
- Jamming forces the AGC to reduce the gain (cf. middle plot of prev. slide)
- This maintains the signal within dynamic range of the ADC
- Eventually, this may lead to saturation if jamming power is high



Jamming impact (Acquisition)

- In general, acquisition does not account for interferences.
- The general test is:

$$\begin{aligned} \mathcal{H}_0 &: y[n] = \eta[n] \\ \mathcal{H}_1 &: y[n] = x_{\theta,i}[n] + \eta[n] \end{aligned}$$

  and in the presence of the satellite AND an interference, the received signal is $y[n] = x_{\theta,i}[n] + i[n] + \eta[n]$.

- The CAF will have the contribution of the desired signal AND the interference:

$$\mathcal{C}_i(\tau, f_d) = \frac{\mathbf{y}\mathbf{c}_i^\top}{N}$$

Jamming impact (Acquisition)

- By virtue of the spreading properties of the used PRN codes, an uncorrelated interference can be considered white noise at the output of the correlation process.

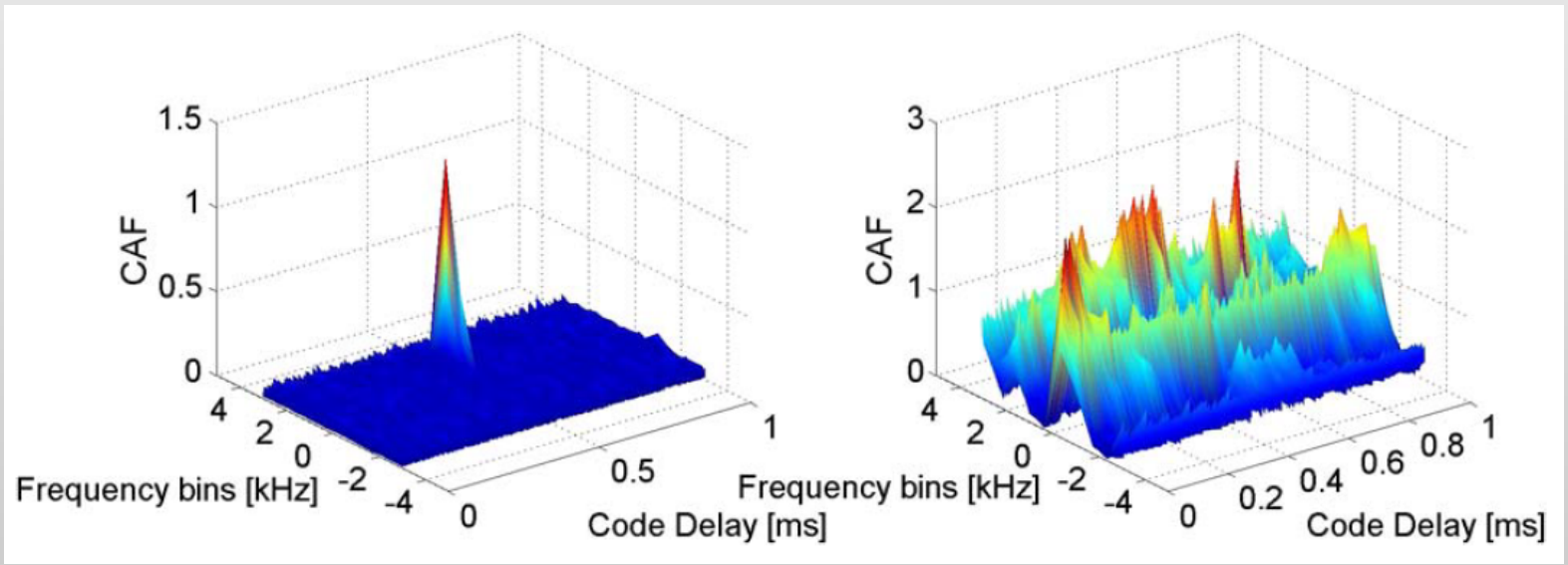
$$\begin{aligned} \mathcal{C}_i(\tau, f_d) &\propto \mathbf{y}\mathbf{c}_i^\top \\ &= \mathbf{x}_{\theta,i}\mathbf{c}_i^\top + \underbrace{\mathbf{i}\mathbf{c}_i^\top + \boldsymbol{\eta}\mathbf{c}_i^\top}_{\tilde{\boldsymbol{\eta}} \approx \text{ colored noise}} \end{aligned}$$

since $\mathbf{i}\mathbf{c}_i^\top$ results in spreading the interference.

- Main effect is to decrease the $\frac{C}{N_{0,\text{eff}}}$

Jamming impact (Acquisition)

- GPS L1 C/A acquisition search without interference (left) and with an in-band CW interference at -130 dBW (right)



Spoofing impact (Acquisition)

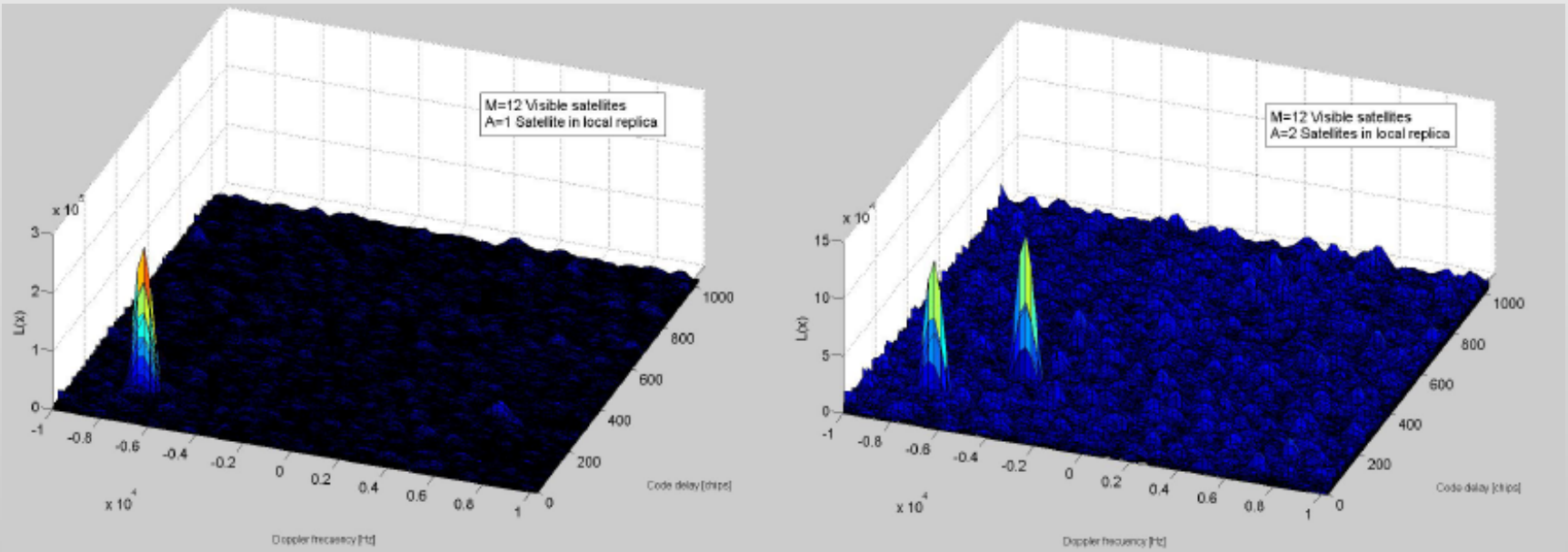
- For correlated interferences, the CAF will reflect the correlation between $\mathbf{c}$ and the interference.
- This is the case of spoofing, which is no longer random noise when correlated:

$$\begin{aligned} \mathcal{C}_i(\tau, f_d) &\propto \mathbf{y}\mathbf{c}_i^\top \\ &= \mathbf{x}_{\theta,i}\mathbf{c}_i^\top + \mathbf{x}_{\tilde{\theta},i}\mathbf{c}_i^\top + \underbrace{\boldsymbol{\eta}\mathbf{c}_i^\top}_{\tilde{\boldsymbol{\eta}} \approx \text{ colored noise}} \end{aligned}$$

since $\mathbf{x}_{\tilde{\theta},i}\mathbf{c}_i^\top$ results in a correlation peak when the local code is aligned in (τ, f_d) to the spoofing signal.

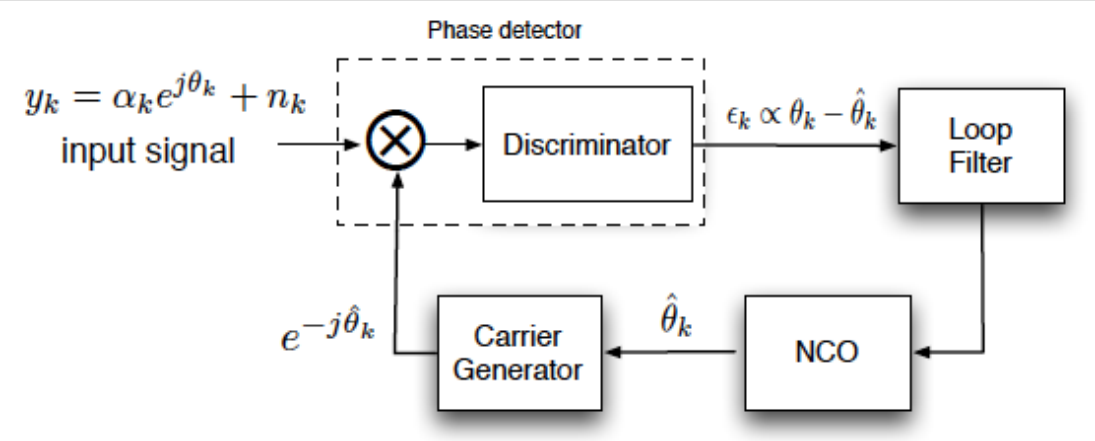
Spoofing impact (Acquisition)

- GPS L1 C/A acquisition search without spofer (left) and with a spoofing signal with similar power levels (right)



Jamming impact (Tracking)

- Interference can affect tracking loops if turned on once signal is acquired.
- Under nominal conditions, the discriminator output should go to zero.
- Discriminator output is a good metric to assess the impact of a jamming interference on tracking loops.



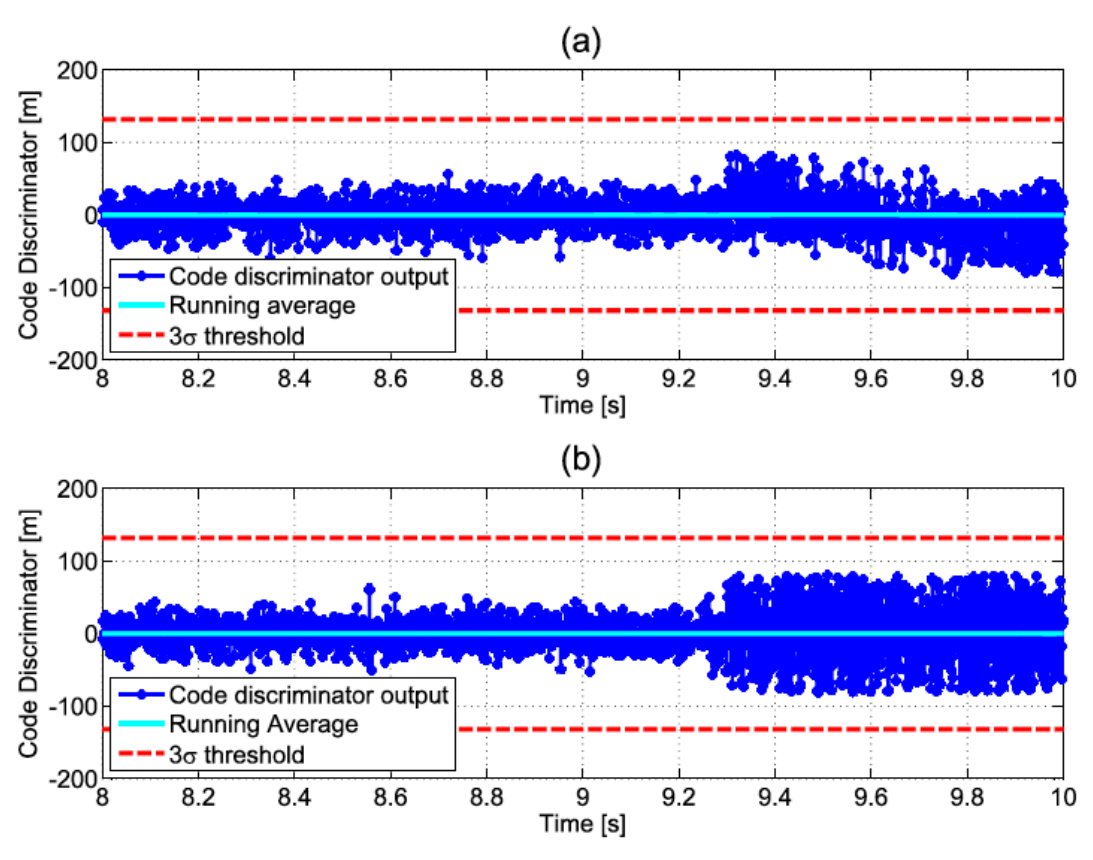
Jamming impact (Tracking)

- Interference can affect tracking loops if turned on once signal is acquired.
- Under nominal conditions, the discriminator output should go to zero.
- Discriminator output is a good metric to assess the impact of a jamming interference on tracking loops.
- Two experiments:
  (a) In-band CW jammer (-130 dBW)
  (b) In-band saw-tooth jammer (-130 dBW), sweeping range of 16.7 MHz centered at L1, and sweep rate of 8.9μs

  in both, the jammer is turned on at instant 9.3 sec.

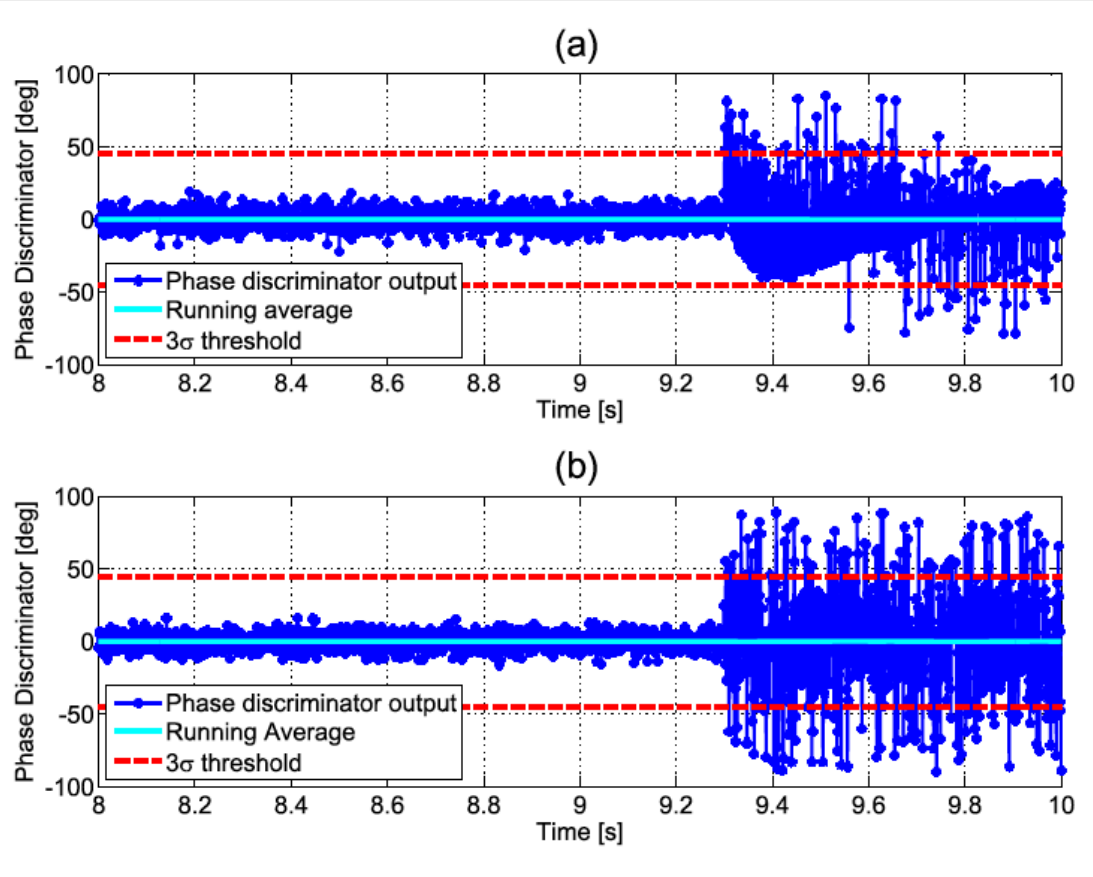
Jamming impact (Tracking)

- Impact on code discriminator output (DLL)



Jamming impact (Tracking)

- Impact on carrier discriminator output (PLL)



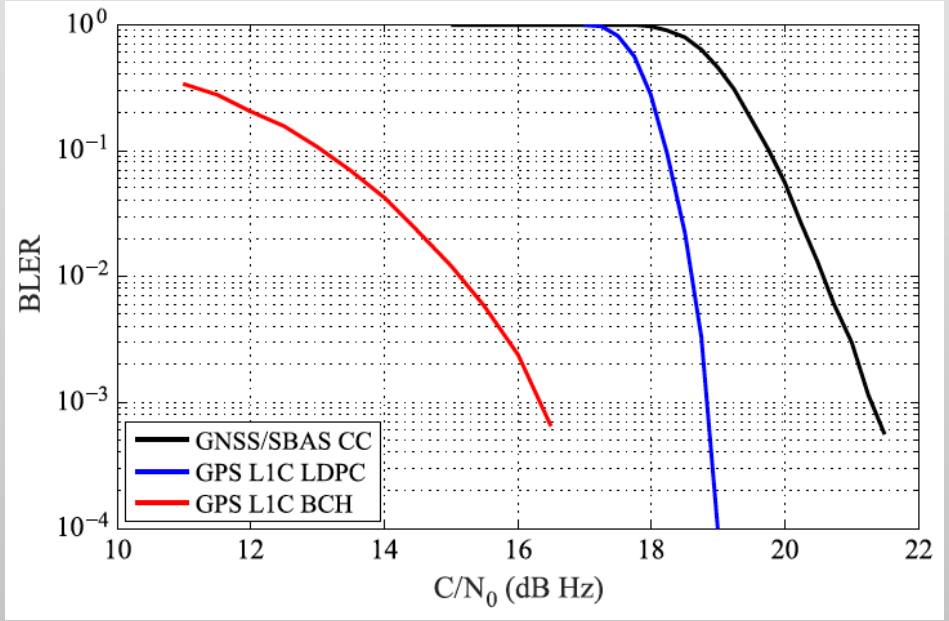
Jamming impact (Decoding)

- Early GNSS signals carried an uncoded navigation message (e.g. GPS L1 C/A)
- The benefits of error correcting codes for GNSS have been recognized and all modern GNSS signals employ forward-error correction (FEC).

System	Signal	Message	Coding
GPS	L1 C/A	LNAV	none
	L1C	CNAV-2	block: BCH & LDPC
	L2C	CNAV	½-rate convolutional
	L5	CNAV	½-rate convolutional
Galileo	E1-B	INAV	½-rate convolutional
	E6-B	CNAV	½-rate convolutional
	E5a	FNAV	½-rate convolutional
	E5b	INAV	½-rate convolutional
SBAS	L1	SBAS	½-rate convolutional

Jamming impact (Decoding)

- Early GNSS signals carried an uncoded navigation message (e.g. GPS L1 C/A)
- The benefits of error correcting codes for GNSS have been recognized and all modern GNSS signals employ forward-error correction (FEC).

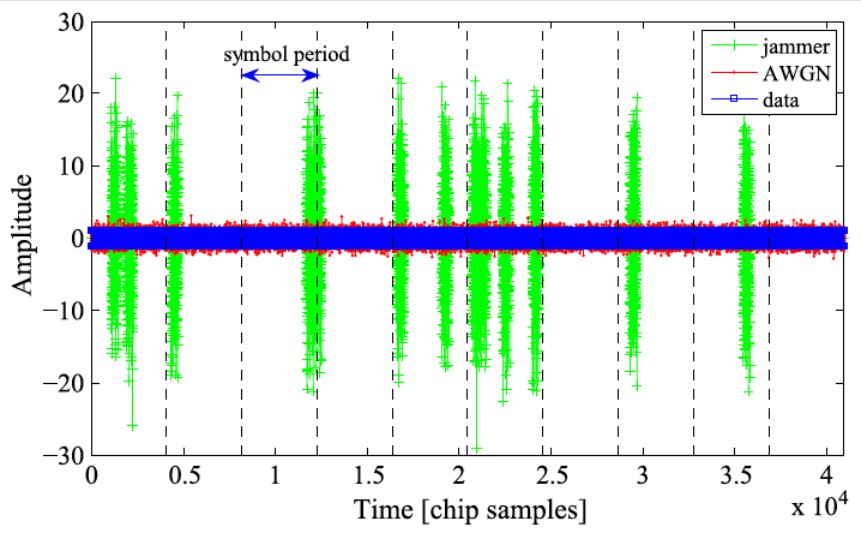


FEC Scheme	Required for BLER = 10^{-3}	
	E_b/N_0 (dB)	C/N_0 (dB-Hz)
GNSS/SBAS CC	4.31	21.30
GPS L1C LDPC	1.85	18.84
GPS L1C BCH	3.95	16.33

Jamming impact (Decoding)

- In the presence of jamming (e.g. pulsed), coding gain can provide additional robustness
- Studies show that soft-decoding schemes can provide enhance performance.

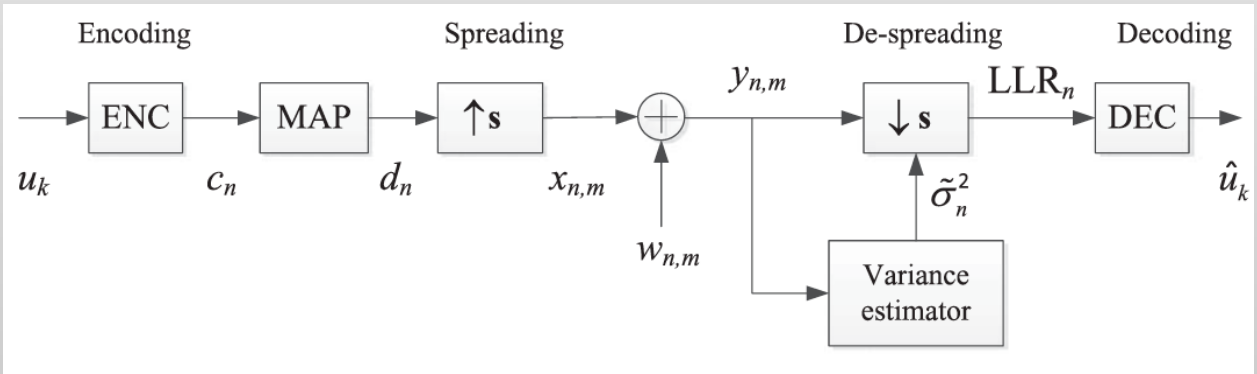
[Cur16] J. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding Aspects of Secure GNSS Receivers," in Proceedings of the IEEE, vol 104, no 6, pp 1271–1287, June 2016.



Jamming impact (Decoding)

- In the presence of jamming (e.g. pulsed), coding gain can provide additional robustness
- Studies show that soft-decoding schemes can provide enhance performance.

[Cur16] J. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding Aspects of Secure GNSS Receivers," in Proceedings of the IEEE, vol 104, no 6, pp 1271–1287, June 2016.

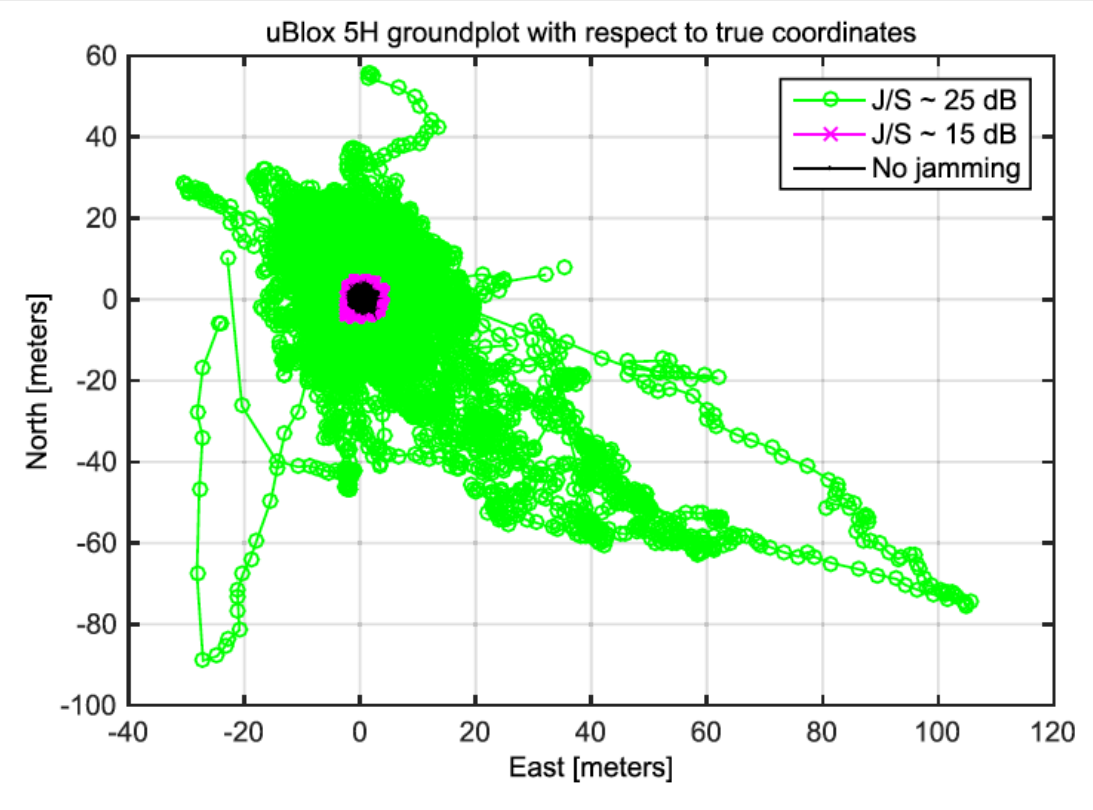


Jamming impact (PVT)

- Given that the receiver is not disrupted, it can provide a PVT solution.
- This PVT would be degraded due to noisy (jammed-)pseudoranges.
- Formally characterizing such deterioration is, in general, hard due to the nonlinearities induced by the jammer.
- For the sake of example, an experiment is shown where
  - A u-Blox 5H receiver is jammed with an in-band CW.
  - C_I/N_0 of 15 dB and 25 dB were tested.
  - 24 hours long.

Jamming impact (PVT)

- Position results around the true coordinates (error < 129.3 m)



Summary (so far, II)

- Overview of baseband signal processing blocks of a GNSS receiver.
- Interferences might affect at different stages of the receiver
  - Front-end elements (filters, amplifiers, AGC, or ADC)
  - Acquisition (jamming: DoS , spoofing: supersede)
  - Tracking (code/carrier loops: loss-of-lock)
  - Decoding (coding gain, soft-decoding)
  - PVT

Outline

Countermeasures

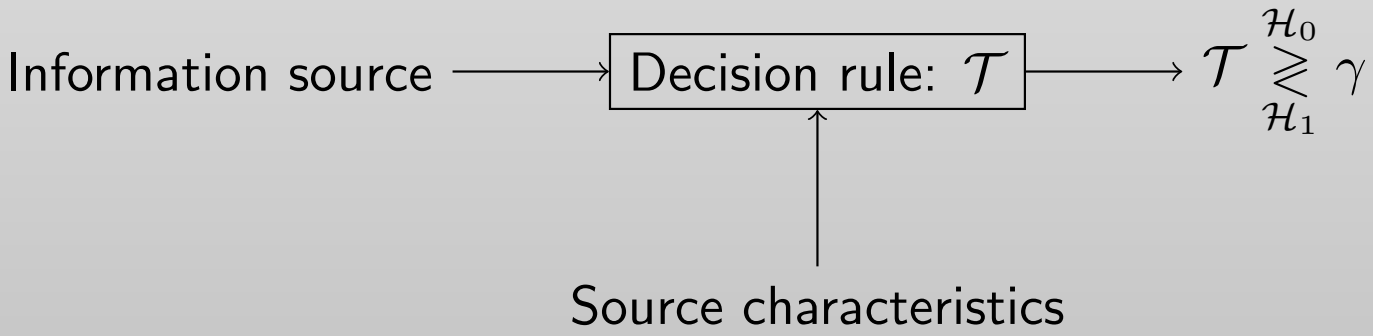
- Detection and mitigation are typically implemented together.
- Spread spectrum modulations provide intrinsic jamming rejection: use mitigation only when necessary!
- Detection: is about revealing whether an interference is present or not ($\Rightarrow$ Hypothesis testing)
- Mitigation: removing the contribution of the interference, possibly using a parametric model ($\Rightarrow$ Estimation problem)

Interference detection

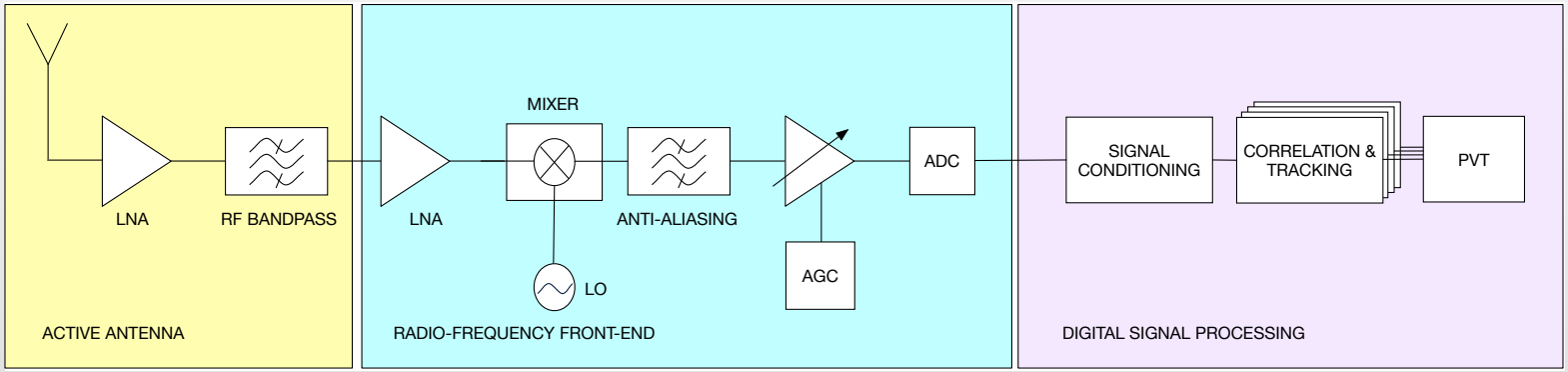
- The detection problem can be generally formulated as:

$$\begin{aligned} \mathcal{H}_0 &: \text{no interference} \\ \mathcal{H}_1 &: \text{interference is present} \end{aligned}$$

- The hypothesis testing is then characterized by
  - The source of information or measurements used.
  - The characteristics of the source to distinguish between hypothesis.
- Almost any signal in the receiver can be considered to build the test!

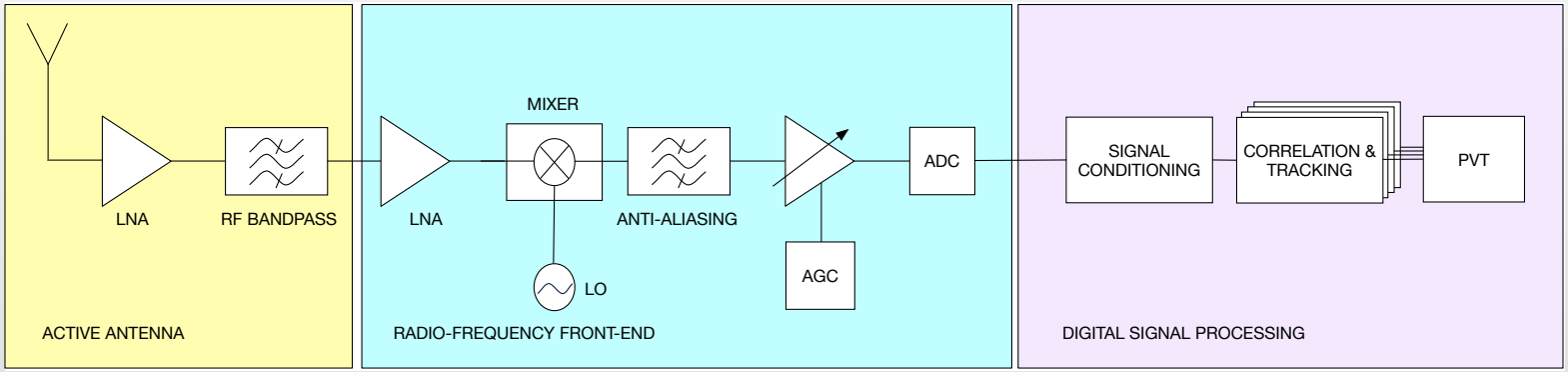


Interference detection



- RF front-end countermeasures such as:
  - AGC gain time series: AGC gain variations can indicate the presence of disturbing signals.
  - Distribution of the samples at the ADC output: deviation from normality.
  - Increased sample variance (high number of samples represented with the highest/lowest levels of the quantization function)

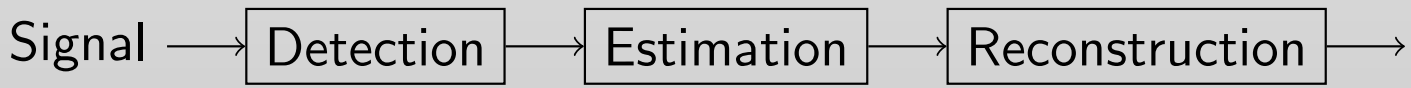
Interference detection



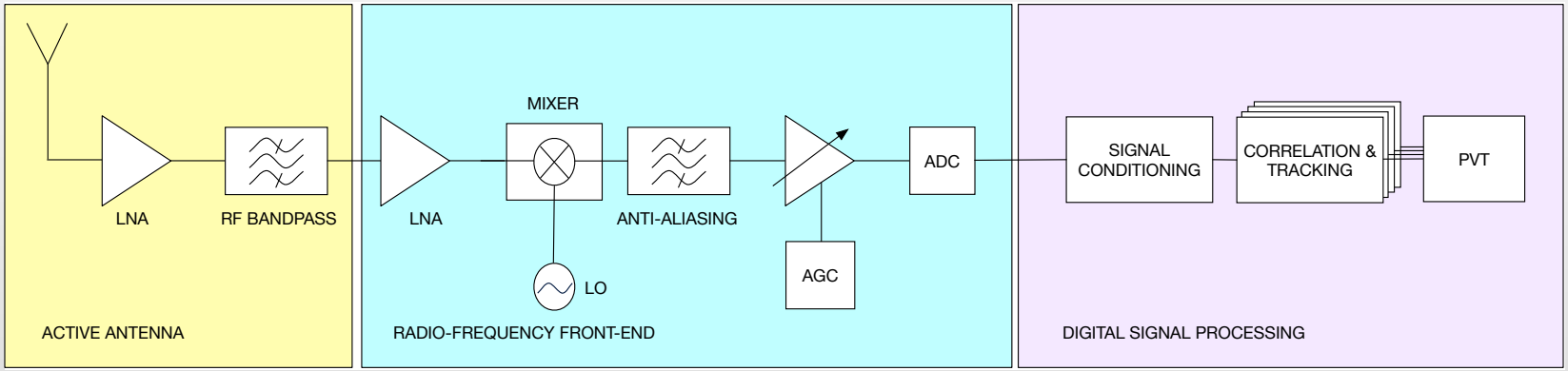
- DSP countermeasures such as:
  - Pre-correlation techniques (sample level):
    - Departure from Gaussianity of ADC samples,
    - Time-frequency analysis (FFT, windowed FFT, Wavelet transform)
  - Post-correlation techniques (lower rate):
    - C/N_0,
    - discriminator outputs,
    - correlator's spectral analysis,
    - exploit observables (pseudoranges and Doppler), or
    - PVT

Interference mitigation

- A mitigation technique has an impact on the desired signal
  - C/N_0 degradation.
  - Biased measurements.
- Adopt mitigation techniques only if detection techniques raise an alarm.
- Besides the parameters of the desired signal ($\boldsymbol{\theta}$), we need to estimate the parameters of the interference so we can mitigate/cancel it.

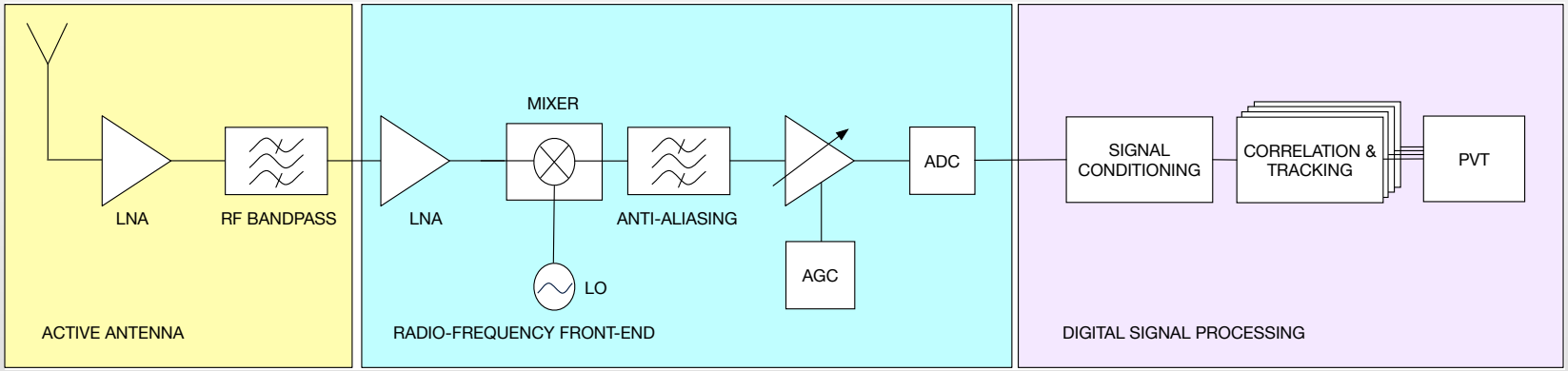


Interference mitigation



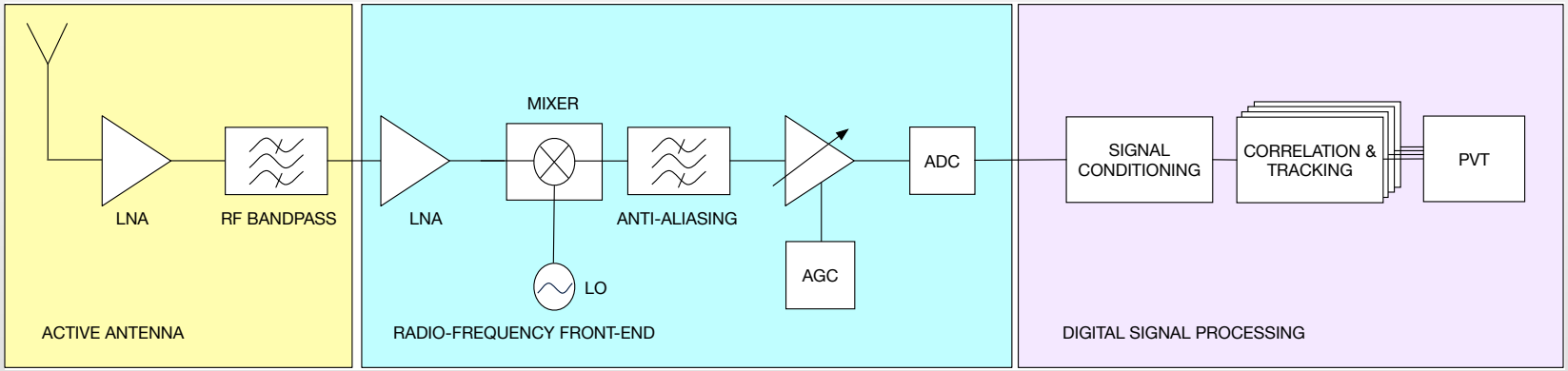
- Antenna countermeasures such as:
  - appropriate reception pattern,
  - sharp out-of-band filtering, or
  - high-compression point of LNA.

Interference mitigation



- RF front-end countermeasures such as:
  - high-dynamic range mixing,
  - multilevel ADC (> 8 bits),
  - short relaxation times of AGC, or
  - interference early detection.

Interference mitigation



- DSP countermeasures such as:
  - Pre-correlation techniques (sample level):
    - pulse blanking (for pulsed interferences),
    - (adaptive) notch filtering (for CW interferences),
    - Robust statistics.
  - Post-correlation techniques (lower rate):
    - robust design of tracking loops,
    - inertial coupling,
    - data fusion, or
    - network aiding.

Interference mitigation (Notch filtering)

- A linear filter whose transfer function attenuates only a single frequency, while leaving all the other signal components unchanged.
- The ideal notch filter is such that its frequency response is (Fourier transform)

$$H(f) = \begin{cases} 0 & , \text{if } f = f_I \\ 1 & , \text{otherwise} \end{cases}$$

- Particularly suited to mitigate CW interferences.
- Need to estimate the frequency f_I of the CW jammer, $\hat{f}_I = f_I + \epsilon_f$.

Interference mitigation (Notch filtering)

- A notch filter has transfer function (in Laplace transform)

$$H(s) = \frac{s^2 + \omega_0^2}{s^2 + \beta s + \omega_0^2}$$

  where
  - $\omega_0 = 2\pi f_I$ is the central frequency to be rejected and
  - $\beta = \frac{\omega_0}{\mathcal{Q}}$, with $\mathcal{Q}$ the quality factor (high $\mathcal{Q}$, implies a narrower null).
  - $H(f) = H(s)|_{s=j2\pi f}$ is the frequency response.

- $\hat{f}_I$ is constantly tracked in order to track the interference frequency.
  - Adaptation criteria: minimization of the signal energy at the output of the filter, $\mathbb{E}\{|y[n] * h[n]|^2\}$.
  - Adaptation algorithm: least mean squares (LMS)
  - Fast sweep rates challenge the tracking method.
  - Frequency jumps causes transients.
- Several notch filters can be cascaded to remove multiple CW jammers.

Summary (so far, III)

- Countermeasures can be implemented at many stages of the GNSS receiver.
  - Antenna
  - RF front-end
  - DSP
- Two basic (inter-related) processes
  - Detection
  - Mitigation
- Important to bear in mind: GNSS is a *closed* system that, once designed cannot be changed. Only the receiver part is modifiable.

Outline

Gaussian assumption

- **Classical GNSS signal processing** is based on the Gaussian assumption for the samples at the output of the RF front-end.
- The receiver design is then approach from a **Least Squares** perspective, which turns out to be optimal when the assumptions hold. For instance the derivation of the CAF:

$$\begin{aligned}\left\{\hat{\tau},\hat{f}_d,\hat{\phi}\right\} &= \arg\min_{\tau,f_d,\phi} J\left(\tau,f_d,\phi\right)\\ &= \arg\min_{\tau,f_d,\phi}\sum_{n=0}^{N-1}\left|y[n]-Ac\left(nT_s-\tau\right)\mathrm{e}^{j2\pi f_d nT_s+j\phi}\right|^2\end{aligned}$$

where we omitted the dependence on i, the satellite index, for convenience.

Gaussian assumption

- It is possible to show that the minimization process can be restated as

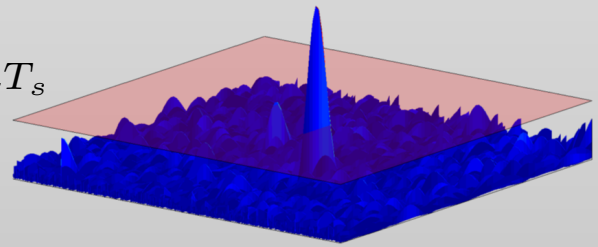
$$\left\{\hat{\tau}, \hat{f}_d\right\} = \arg\max_{\tau, f_d} |\mathcal{C}(\tau, f_d)|$$

$$\hat{\phi} = \angle \mathcal{C}(\hat{\tau}, \hat{f}_d)$$

where

$$\mathcal{C}(\tau, f_d) = \sum_{n=0}^{N-1} y[n] c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}$$

- Acquisition/Tracking are implementations of the optimal estimator in the LS sense.
- Maximization of the CAF:



Gaussian assumption and interferences

- In the presence of interference, the signal at the input of a GNSS receiver in a one-path additive channel can be modeled as:

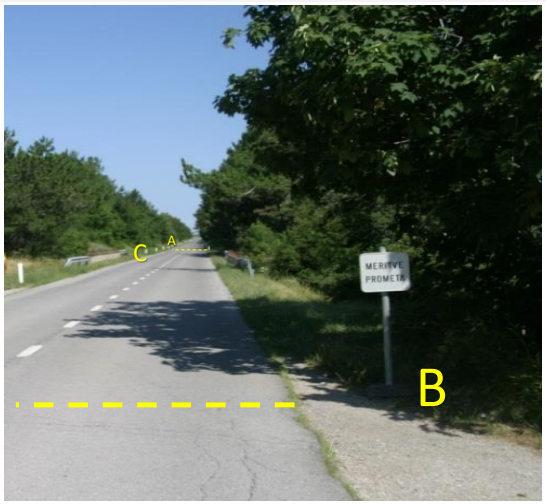
$$y(t) = \sqrt{2C} b\left(t-\tau\right) c\left(t-\tau\right) \cos\left(2\pi(f_{RF}+f_d)t+\phi\right) + \eta(t) + i(t)$$

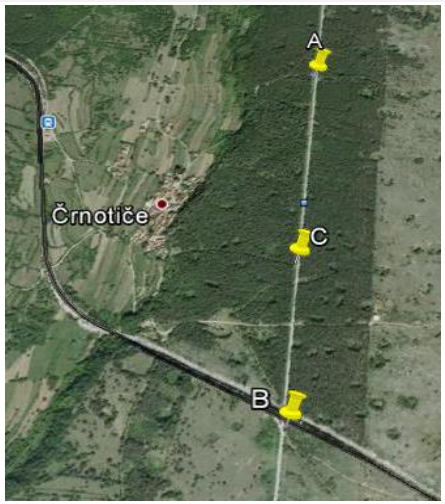
- After down-conversion and sampling, becomes:

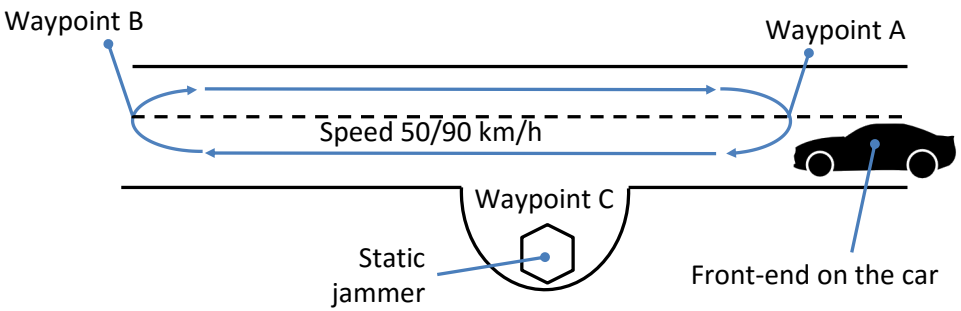
$$y[n] = \sqrt{C} \tilde{b}\left(nT_s-\tau\right) \tilde{c}\left(nT_s-\tau\right) \mathrm{e}^{j2\pi f_d n T_s + j\phi} + \eta_{BB}[n] + i_{BB}[n]$$

- The notation $x[n] = x(nT_s)$ is used to denote a discrete-time sequence sampled at the frequency $f_s = \frac{1}{T_s}$.
- The index "BB" is used to denote a filtered signal down-converted to base-band. The symbol $\tilde{\cdot}$ is used to indicate the impact of the front-end filter on the useful signal components.

An experiment with interferences







- Experiment performed at JRC, Ispra.
- Jammer swept over a large bandwidth, ~ 9 dBm.
- J/N$= 25$ dB at C.
- Narrowband front-end: Realtek RTL2832u.
- $f_s = 2.048$ MHz and 8 bits.

[Bor16] D. Borio, "Swept GNSS jamming mitigation through pulse blanking" in Proc. of the European Navigation Conference (ENC), May 2016, pp. 18. doi:10.1109/EURONAV.2016.7530549

An experiment with interferences

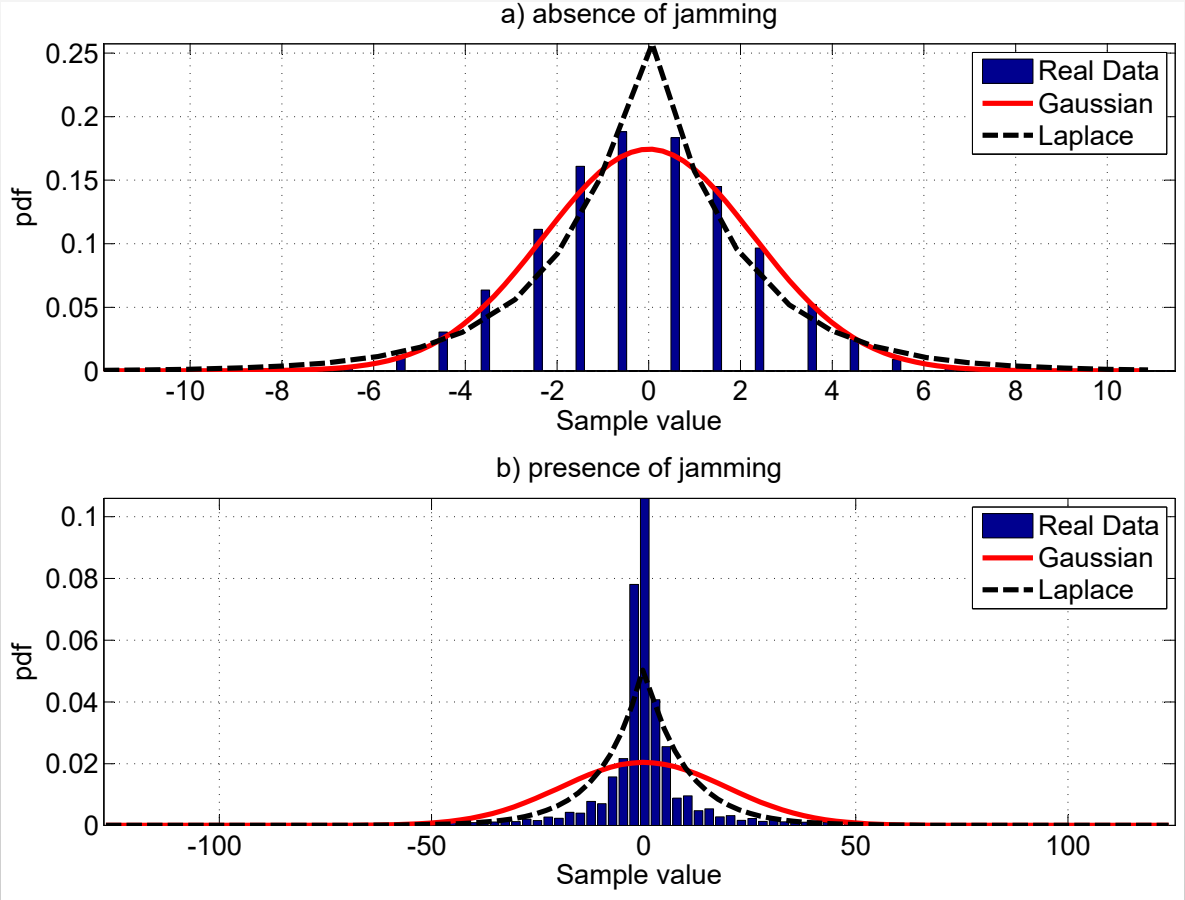


Figure: Empirical distribution of GNSS signal samples collected in the absence (upper part) and in the presence of jamming (lower part) and comparison with the Gaussian and Laplace distributions. Real data.

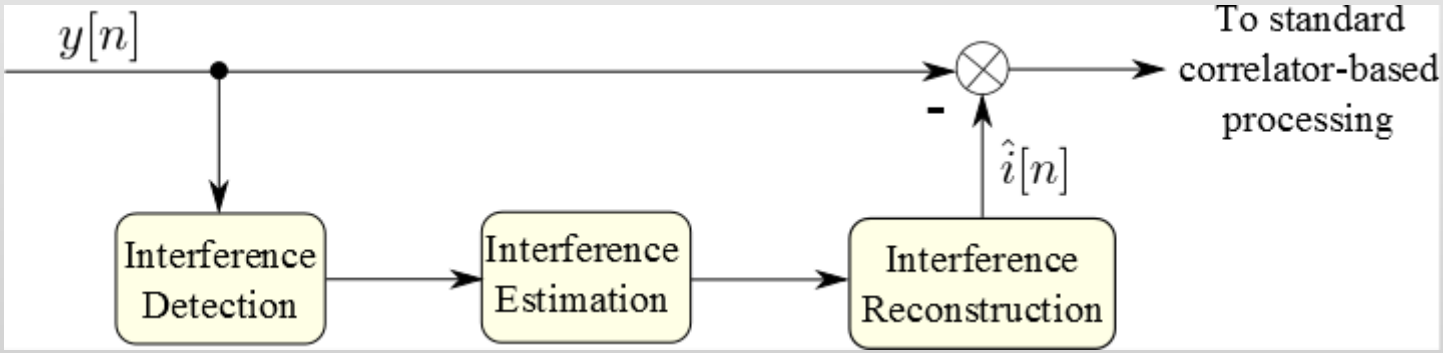
Gaussian assumption and interferences

- The Gaussian assumption is **not adequate** to model the signal in the presence of jamming signals.
- Heavy-tailed distributions can better capture the statistical nature of signals affected by pulsed interference. These distributions assign larger probabilities to the occurrence of outliers and better describe the joint PDF of $\eta_{BB}[n]$ and $i_{BB}[n]$.
- Main objective: reformulate the LS problem yielding to a robust version of the CAF for anti-jamming.

[Bor17b] Borio, D., Closas, P. (2017). A fresh look at GNSS anti-jamming. Inside GNSS, 12, 54-61.

Interference Cancellation

- A standard anti-jamming technique that *cleans* the data by
  1. **Detecting** $i_{BB}[n]$
  2. **Reconstructing** $\hat{i}_{BB}[n]$ and substracting it from $y[n]$



Interference Cancellation

- A standard anti-jamming technique that *cleans* the data by
  1. **Detecting** $i_{BB}[n]$
  2. **Reconstructing** $\hat{i}_{BB}[n]$ and substracting it from $y[n]$
- Pulse Blanking (PB) is a popular IC method for pulsed interference mitigation.
- At a glance, PB detects the presence of interference by identifying abnormally large values in the pre-correlation samples. This can be easily achieved by comparing to a predefined threshold T_{PB}. Then, the interfered samples are set to zero such that they are not used throughout the receiver:

$$\hat{i}_{BB}[n] = \begin{cases} y[n] & \text{if } |y[n]| \geq T_{\text{PB}} \\ 0 & \text{otherwise} \end{cases}$$

Interference Cancellation

- IC considers a modified cost-function:

$$J_{IC}\left(\tau, f_d, \phi\right) = \sum_{n=0}^{N-1} \left| y[n] - \hat{i}_{BB}[n] - Ac\left(nT_s - \tau\right) \mathrm{e}^{j2\pi f_d n T_s + j\phi} \right|^2$$

where $\hat{i}_{BB}[n]$ is the reconstructed interference term. In a similar way, the CAF is generalized as

$$\mathcal{C}_{IC}(\tau, f_d) = \sum_{n=0}^{N-1} (y[n] - \hat{i}_{BB}[n]) c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}.$$

- The main limitation of IC-based approaches is that they have to be able to estimate the interfering term, $i_{BB}[n]$:
  - A parametric model for $i_{BB}[n]$ is usually required.
  - Usually perform poorly when the interference term does not follow the model assumption made for its reconstruction.

Interference Cancellation

- Back to PB, we can conveniently express the CAF as:

$$\mathcal{C}_{\mathrm{PB}}(\tau, f_d) = \sum_{n=0}^{N-1} \psi_{\mathrm{PB}}(y[n]) c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s} \ ,$$

  where

$$\psi_{\mathrm{PB}}(y[n]) = \begin{cases} y[n] & \text{if } |y[n]| < T_{\mathrm{PB}} \\ 0 & \text{otherwise} \end{cases}$$

  is a non-linear function on the samples.

- PB can be seen as a pre-processing of the data, resulting on a robust CAF.

- We'll see soon how this connects to robust statistics...

Robust signal processing

- When the IC principle is used, the interfering term is treated as a signal component whose parameters should be estimated.
- A different approach for the design of interference mitigation techniques can be derived from the theory of robust statistics.
- In this case, the receiver does not try to estimate the jamming signal but adopts processing strategies which can produce *reasonable results* even in the presence of interference.
- Two options:
  1. **Interference Cancellation**: deterministic models for the interference.
  2. **Robust statistics**: models tolerants to errors.

Robust signal processing

- An alternative to IC is provided by the **M-estimation** approach. The 'M' in 'M-estimator' stands for ML since the functional form of this type of approaches derives from that of ML estimators.
- The main idea behind M-estimators is that the squares in cost functions as that in the LS cost function should be replaced by less rapidly increasing functions of the residuals:

$$J_\rho\left(\tau, f_d, \phi\right) = \sum_{n=0}^{N-1} \rho\Big(y[n] - Ac\left(nT_s - \tau\right) \mathrm{e}^{j2\pi f_d n T_s + j\phi}\Big)$$

where $\rho(\cdot)$ is a positive real (non-linear) function of complex argument, and

$$\left\{\hat{\tau}, \hat{f}_d, \hat{\phi}\right\} = \arg \min_{\tau, f_d, \phi} J_\rho\left(\tau, f_d, \phi\right)$$

Robust signal processing

- In the presence of interference, $r[n] = y[n] - Ac\left(nT_s - \tau\right) \mathrm{e}^{j2\pi f_d nT_s + j\phi}$, assume large values that can be significantly amplified by the square in the LS function.
- The cost function $J(\cdot)$ can be significantly biased, preventing the estimation of the actual signal parameters.
- The role of $\rho(\cdot)$ is to reduce the impact of large residuals on the overall cost function $J_\rho\left(\tau, f_d, \phi\right)$. In particular, $\rho(\cdot)$ can clip or down-weight large residuals.
- This type of approach is effective only if there exist a significant number of samples not affected by interference. For instance, if the interfering signal is pulsed. The interference term, $i_{BB}[n]$ has to behave as an outlier and a sufficient number of clean samples has to be available (**Outliers** $<<$ **Inliers**).

Robust signal processing

- Two key ideas in robust statistics:
  1. In nominal conditions, performance should be close to optimal. When interference is not present, residuals with low amplitudes are obtained. Through $\rho(\cdot)$, they should provide a significant contribution to the evaluation of $J_\rho(\tau, f_d, \phi)$ reflecting the actual signal properties. Concept of Loss of Efficiency.
  2. In the presence of outliers, the estimation should not breakdown. When interference is present, the residuals are significantly attenuated by $\rho(\cdot)$ only marginally impacting the computation of $J_\rho(\tau, f_d, \varphi)$. However, if $i_{BB}[n]$ impacts the majority of the samples, then $J_\rho(\tau, f_d, \varphi)$ will be significantly biased. Concept of Breakdown Point.

Robust CAF

- The generalized cost function

$$J_\rho(\tau, f_d, \phi) = \sum_{n=0}^{N-1} \rho\Big(y[n] - Ac(nT_s - \tau)\, e^{j2\pi f_d n T_s + j\phi}\Big)$$

can be further manipulated considering:

- $\rho(z)$ is a real positive function of complex argument $z = z_I + jz_Q$.
- $\rho(z) \triangleq \rho(z_I, z_Q)$ is a real positive function of two real arguments.
- $\Delta z = \Delta z_I + j\Delta z_Q$ is a small $\mathbb{C}$ increment.
- Regard $y[n]$ as z.
- Regard $Ac(nT_s - \tau)\, e^{j2\pi f_d n T_s + j\phi}$ as Δz.
- Then, we have $\rho(z - \Delta z)$ in $J_\rho(\tau, f_d, \phi)$ above.

Robust CAF

- We can approximate $\rho(z-\Delta z)$ as

$$\begin{aligned}\rho(z-\Delta z) &= \rho(z_I-\Delta z_I, z_Q-\Delta z_Q)\\ &\approx \rho(z)-\frac{\partial\rho(z)}{\partial z_I}\Delta z_I-\frac{\partial\rho(z)}{\partial z_Q}\Delta z_Q\\ &= \rho(z)-\mathrm{Re}\left\{\psi(z)\Delta z^*\right\}\end{aligned}$$

with

$$\psi(z)=\psi_I(z)+j\psi_Q(z)=\frac{\partial\rho(z)}{\partial z_I}+j\frac{\partial\rho(z)}{\partial z_Q}$$

Robust CAF

- Using that result, the generalized cost function is

$$\begin{aligned} J_\rho(\tau, f_d, \phi) &= \sum_{n=0}^{N-1} \rho\Big(y[n] - Ac(nT_s - \tau)\, \mathrm{e}^{j2\pi f_d n T_s + j\phi}\Big) \\ &\approx \sum_{n=0}^{N-1} \rho(y[n]) - \mathrm{Re}\left\{\psi(y[n]) Ac(nT_s - \tau)\, \mathrm{e}^{-j2\pi f_d n T_s - j\phi}\right\} \end{aligned}$$

such that

$$\begin{aligned} \left\{\hat{\tau}, \hat{f}_d, \hat{\phi}\right\} &= \arg\min_{\tau, f_d, \phi} J_\rho(\tau, f_d, \phi) \\ &= \arg\max_{\tau, f_d, \phi} \mathrm{Re}\left\{\sum_{n=0}^{N-1} \psi(y[n]) c(nT_s - \tau)\, \mathrm{e}^{-j2\pi f_d n T_s - j\phi}\right\} \end{aligned}$$

Robust CAF

- The resulting robust estimation problem involves optimizing the so-called Robust CAF

$$\left\{\hat{\tau}, \hat{f}_d\right\} = \arg\max_{\tau, f_d} |\mathcal{C}_\rho(\tau, f_d)|$$

$$\hat{\phi} = \angle \mathcal{C}_\rho(\hat{\tau}, \hat{f}_d)$$

where

$$\mathcal{C}_\rho(\tau, f_d) = \sum_{n=0}^{N-1} \psi(y[n]) c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}$$

- Remember our earlier formulation of the Pulse Blanking method?

Robust GNSS signal processing

- Different approaches exist for the design of $\rho(\cdot)$, yielding to different $\psi(\cdot)$ functions.
- A ML-type approach is to use $\rho(z) = -\log\left(f(z)\right)$, where $f(z)$ is the PDF of a complex random variable with possibly heavy tails. For instance **Cauchy** [Bor17a] or **Laplace** [Bor18a] distributions.
- Another approach is to use functions from robust statistics, for instance **Huber**'s nonlinearity [Bor18b].

[Bor17a] Borio, D. (2017). Myriad non-linearity for GNSS robust signal processing. IET Radar, Sonar and Navigation, 11(10), 1467-1476.
[Bor18a] Borio, D., Closas, P. (2018). Complex signum non-linearity for robust GNSS signal processing. IET Radar Sonar and Navigation, 12(8) 900-909.
[Bor18b] Borio, D., Li, H., Closas, P. (2018). Huber's non-linearity for GNSS interference mitigation. Sensors, 18(7), 2217.

Myriad non-linearity

- The myriad non-linearity is obtained considering the **Cauchy** distribution

$$f(z) = \frac{\sqrt{K}}{2\pi(K + |z|^2)^{3/2}}$$

where K is a linearity parameter.

- Then

$$\rho(z) = -\log\left(f(z)\right) = \frac{3}{2}\log(K + |z|^2) + \frac{1}{2}\log\left(\frac{4\pi^2}{K}\right)$$

which results in

$$\psi(z) = \frac{3z}{K + |z|^2}$$

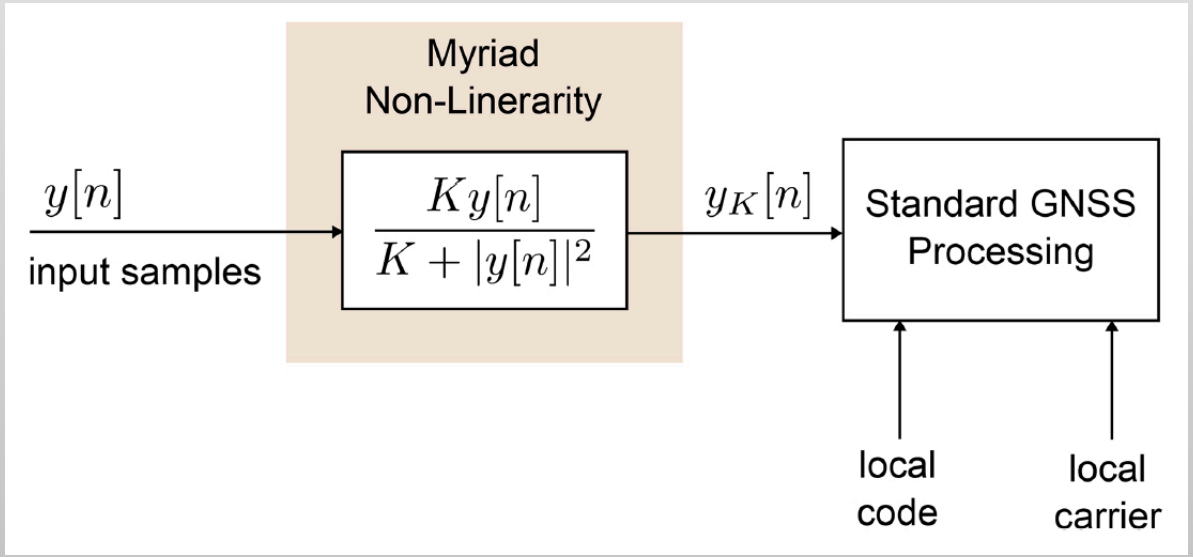
Myriad non-linearity

- In practice, the scaled version

$$\psi(z) = \frac{Kz}{K + |z|^2} \quad : \mathbb{C} \mapsto \mathbb{C}$$

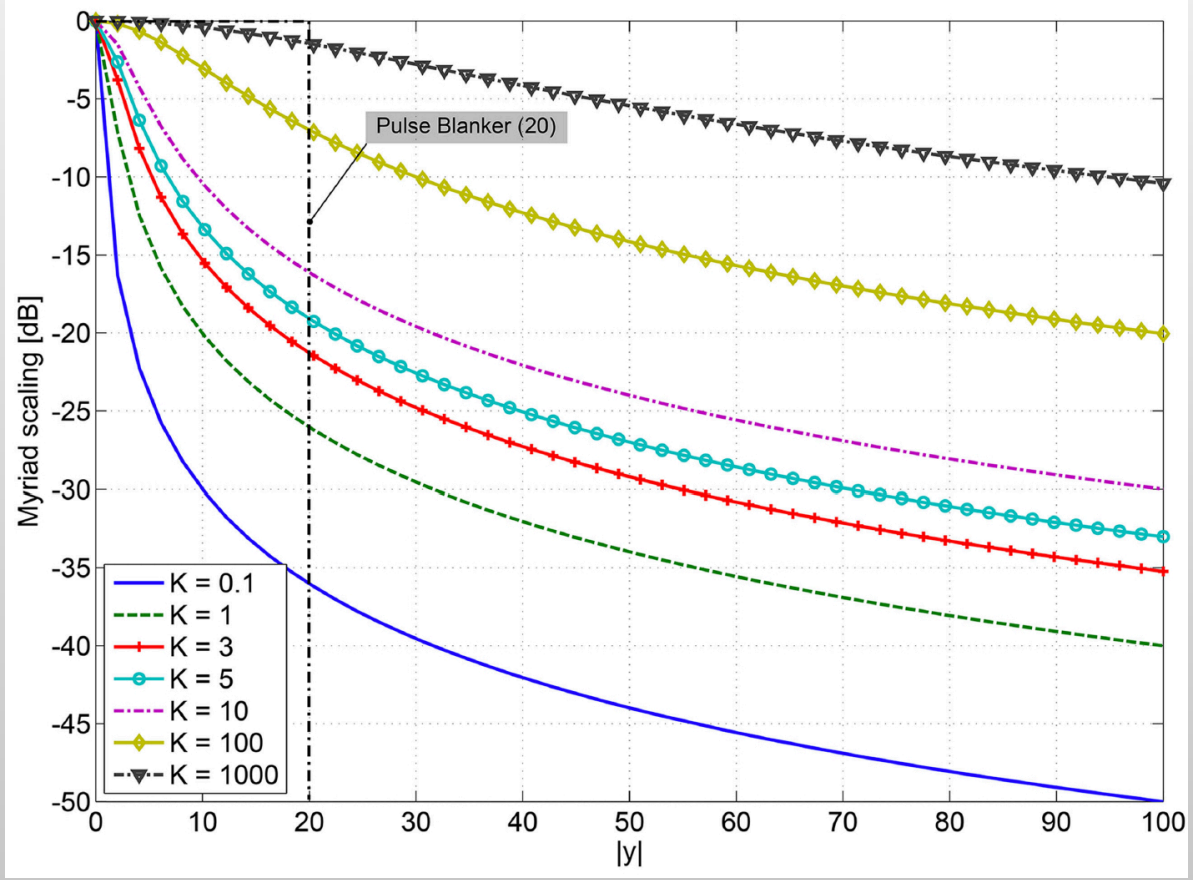
  is used instead.

- Linearity parameter $K \to \infty \Rightarrow \psi(z) \to z$.



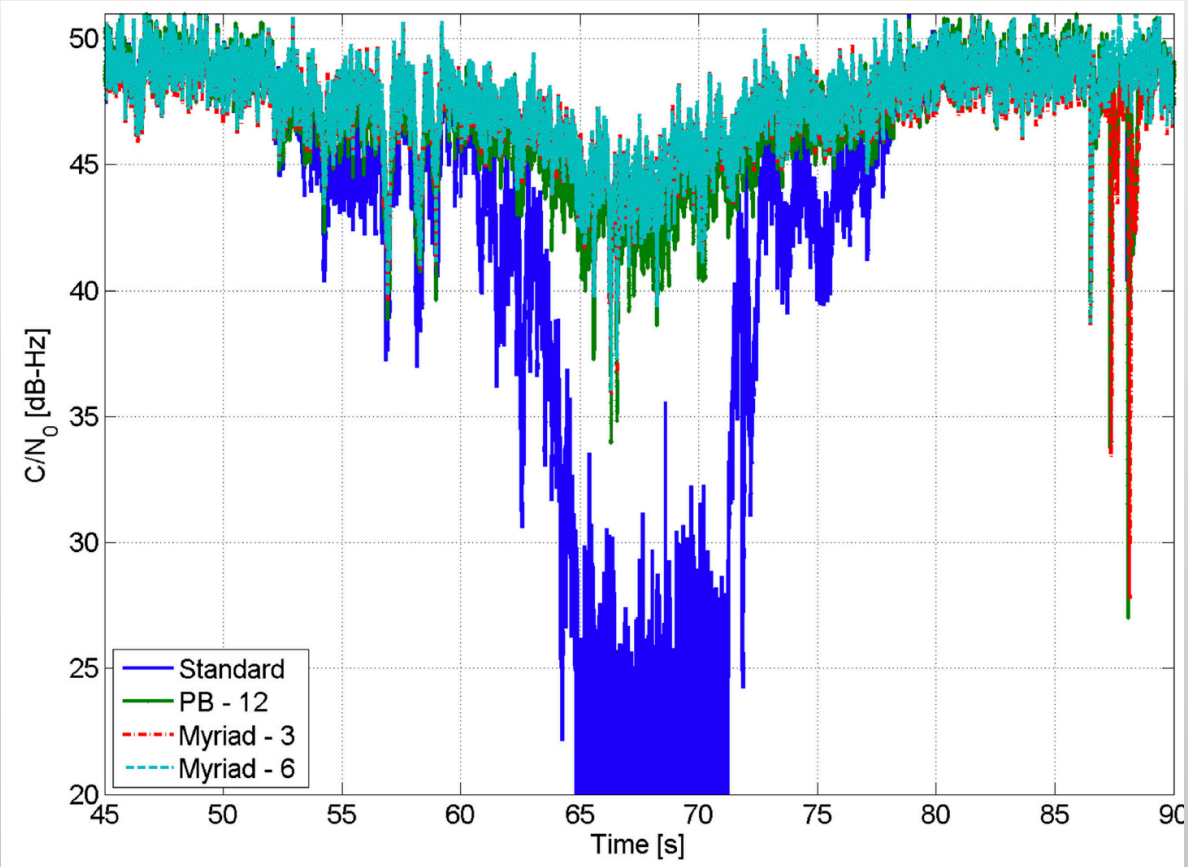
Myriad non-linearity

- It performs a scaling on the input samples $y[n]$ depending on K.



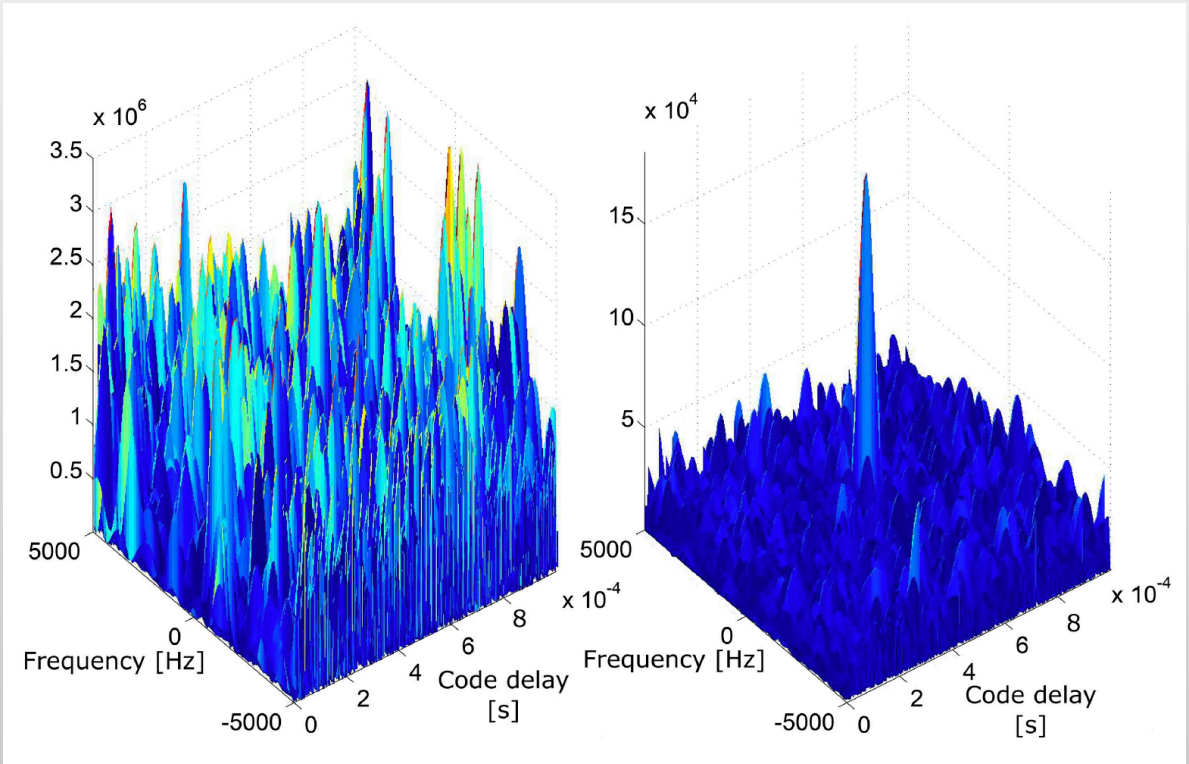
Myriad non-linearity

- Back to the experimental setup, with $K = 6\sigma^2$.



Myriad non-linearity

- Standard CAF and Myriad-based CAF with $K = 6\sigma^2$ under jamming.



Myriad non-linearity

- Myriad non-linearity provides an alternative to PB with a similar computational complexity.
- The samples $y[n]$ are pre-processed in order to reduce the impact of outliers, which is basically a scaling depending on K and $|y[n]|^2$.
- Results are slightly better, depending on the adjustment of K.
- However, there is no free lunch...
- ...when developing robust methods, one needs to evaluate the **loss of efficiency** under nominal conditions.
- In our case, the degradation of the robust method when there are no interference signals.

Loss of efficiency

- Under the assumption of Gaussian input noise, standard GNSS signal processing should be the most efficient estimator for the signal parameters.
- This loss is expressed in terms of coherent output signal-to-noise power ratio which is one of the main performance indicators used in GNSS to measure of the *quality* of the CAFs:

$$L_0 = \frac{\mathrm{SNR}_{\mathrm{out},\rho}}{\mathrm{SNR}_{\mathrm{out}}}$$

- In general, we have that $0 < L_0 < 1$ (in linear scale...)

Loss of efficiency

- Where SNR_{out} is defined as

$$\text{SNR}_{\text{out}} = \max_{\tau, f_d} \frac{\left|\mathbb{E}\left[\mathcal{C}(\tau, f_d)\right]\right|^2}{\frac{1}{2}\text{Var}\left[\mathcal{C}(\tau, f_d)\right]},$$

and when standard processing is adopted, it is possible to show that

$$\text{SNR}_{\text{out}} = 2\frac{C}{N_0}T_c$$

if $B_{Rx} \approx \frac{f_s}{2}$ is assumed and T_c denotes the coherent integration time.

[Bet01] Betz, J.W., "Effect of partial-band interference on receiver estimation of C/N_0: Theory" Proc. of the National Technical Meeting of The Institute of Navigation, Long Beach, CA, January 2001, pp. 81782828
[Bet00] Betz, J.W.: "Effect of narrowband interference on GPS code tracking accuracy" Proc. of the National Technical Meeting of The Institute of Navigation, Anaheim,CA, January 2000, pp. 1627

Loss of efficiency (Myriad non-linearity)

- Similarly, $\mathrm{SNR}_{\mathrm{out},\rho}$ is defined as

$$\mathrm{SNR}_{\mathrm{out},\rho} = \max_{\tau, f_d} \frac{\left|\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right]\right|^2}{\frac{1}{2}\mathsf{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right]},$$

  which requires some tedious calculations to compute the moments of $\mathcal{C}_\rho(\tau, f_d)$.

- The first moment

$$\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right] = \sum_{n=0}^{N-1} \mathbb{E}\left[\psi(y[n])\right] c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}.$$

  which under the weak signal assumption

$$\mathbb{E}\left[\psi(y[n])\right] \approx \mathbb{E}\left[y[n]\right] \frac{K}{2\sigma^2}\left[1 - \frac{K}{2\sigma^2}\mathrm{e}^{K/2\sigma^2}\mathsf{E}_1\left(\frac{K}{2\sigma^2}\right)\right]$$

Loss of efficiency (Myriad non-linearity)

- Similarly, $\mathsf{SNR}_{\mathrm{out},\rho}$ is defined as

$$\mathsf{SNR}_{\mathrm{out},\rho} = \max_{\tau, f_d} \frac{\left|\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right]\right|^2}{\frac{1}{2}\mathsf{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right]},$$

  which requires some tedious calculations to compute the moments of $\mathcal{C}_\rho(\tau, f_d)$.

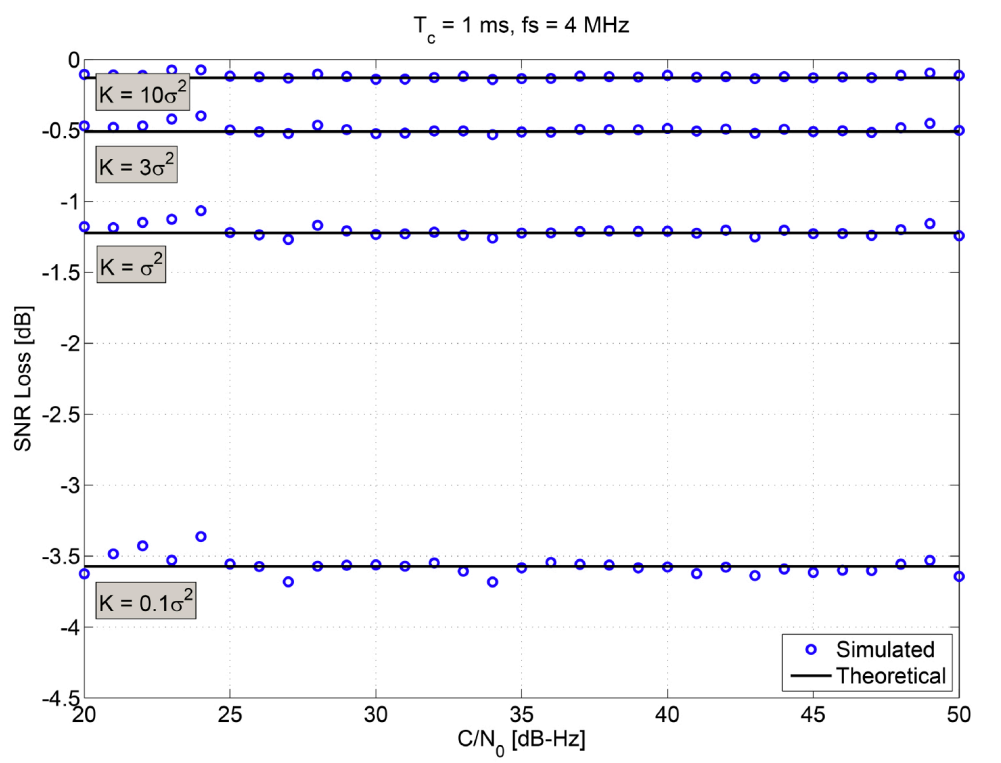
- The second moment

$$\mathsf{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right] = N\mathsf{Var}\left[\psi(y[n])\right] = N\left[\mathbb{E}\left[\left|\psi(y[n])\right|^2\right] - \left|\mathbb{E}\left[\psi(y[n])\right]\right|^2\right]$$

  where

$$\mathbb{E}\left[\left|\psi(y[n])\right|^2\right] \approx \frac{K}{2\sigma^2}\left[\left(1 + \frac{K}{2\sigma^2}\right)\mathrm{e}^{K/2\sigma^2}\mathsf{E}_1\left(\frac{K}{2\sigma^2}\right) - 1\right]$$

Loss of efficiency (Myriad non-linearity)



$$L_0\left(\frac{K}{2\sigma^2}\right) = \frac{\left[1-\frac{K}{2\sigma^2}e^{K/2\sigma^2}E_1\left(\frac{K}{2\sigma^2}\right)\right]^2}{\left(1+\frac{K}{2\sigma^2}\right)e^{K/2\sigma^2}E_1\left(\frac{K}{2\sigma^2}\right)-1}$$

- L_0 does not depend on C/N_0.
- Small K values $\Rightarrow$ higher loss.
- $K > 3\sigma^2 \Rightarrow L_0 < 0.5$ dB.

Complex signum non-linearity

- The complex signum non-linearity is obtained considering the **Laplace** distribution (for complex random variables...)
- If $z \in \mathbb{R}$, the univariate Laplace pdf is

$$f(z) = \frac{1}{2\lambda} \exp\left\{-\frac{1}{\lambda}|z-\mu|\right\}$$

that leads to (for $\mu = 0$) the minimization of the sum of Least Absolute Deviations (LADs)

$$\rho(z) = |z|$$

known as the *sign non-linearity*.

Complex signum non-linearity

- If $z \in \mathbb{C}$, the univariate Laplace pdf is expressed as

$$f(z) = \frac{1}{2\pi\lambda^2} \mathrm{K}_0 \left(\frac{1}{\lambda} |z - \mu| \right)$$

where $\mathrm{K}_0(\cdot)$ is the modified Bessel function of the second kind and order zero.

- It can be shown that this also leads to (for $\mu = 0$ and using an asymptotic expansion of $\mathrm{K}_0(\cdot)$) the minimization of the sum of LADs

$$\rho(z) \approx |z|$$

whose complex gradient is

$$\psi(z) = \mathrm{csign}(z) = \begin{cases} z/|z| & z \neq 0 \\ 0 & z = 0 \end{cases} .$$

Complex signum non-linearity

- $\psi(z)$ is usually referred to as the *complex signum* of z, since it generalizes the concept of sign function to complex numbers.
- For $z \in \mathbb{R}$ we have the usual definition: $\psi(z > 0) = +1$ and $\psi(z < 0) = -1$
- It satisfies

$$z = \text{csign}(z)|z|$$
$$|z| = z\ \text{csign}^*(z)$$

- Intuitively:
  - The complex sign non-linearity acts as an instantaneous AGC where each sample is normalized by its amplitude.
  - Thus, if an outlier is present in the input samples, its amplitude is normalized to 1.
  - The normalization is performed sample by sample whereas the gain provided by the AGC generally varies slowly with time.
  - For this reason, standard AGCs are not suitable for jamming mitigation and are generally used only for detection purposes.

Loss of efficiency (Complex signum non-linearity)

- Recall that the loss of efficiency is defined as the ratio of coherent output SNRs of standard and robust processing:

$$L_0 = \frac{\mathrm{SNR}_{\mathrm{out},\rho}}{\mathrm{SNR}_{\mathrm{out}}}$$

- $\mathrm{SNR}_{\mathrm{out}}$ is obtained as before.
- Similarly, $\mathrm{SNR}_{\mathrm{out},\rho}$ is defined as

$$\mathrm{SNR}_{\mathrm{out},\rho} = \max_{\tau, f_d} \frac{\left|\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right]\right|^2}{\frac{1}{2}\mathrm{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right]},$$

where $\mathcal{C}_\rho(\cdot,\cdot)$ is now the complex signum non-linearity.

Loss of efficiency (Complex signum non-linearity)

- The first moment

$$\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right] = \sum_{n=0}^{N-1} \mathbb{E}\left[\psi(y[n])\right] c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}.$$

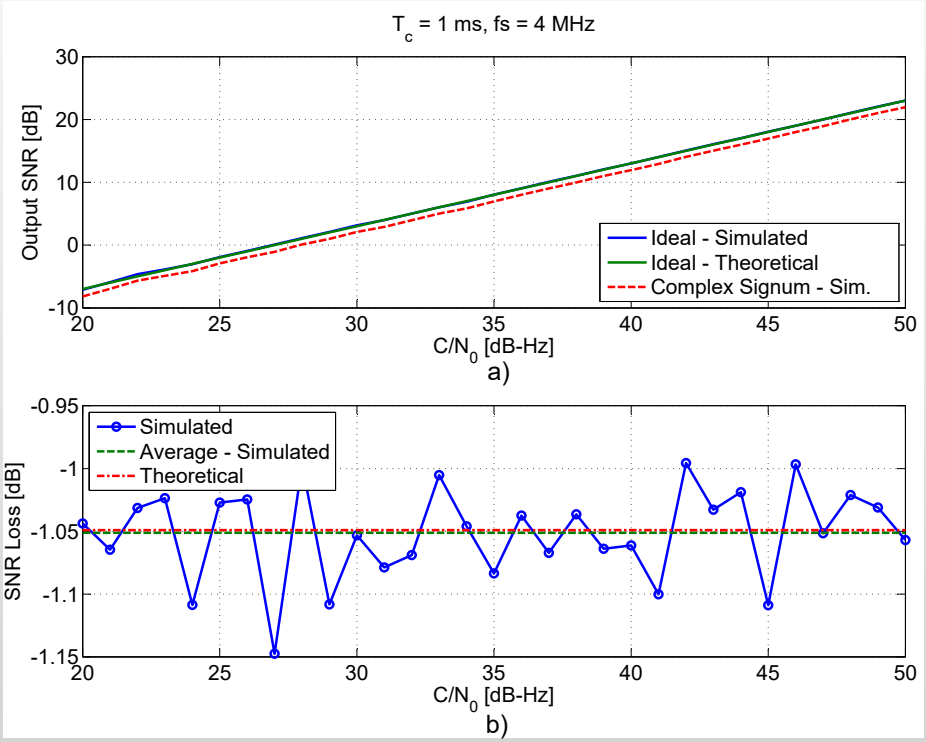
which under the weak signal assumption

$$\mathbb{E}\left[\mathsf{csign}(y[n])\right] \approx \sqrt{\frac{\pi}{2}} \frac{\mathbb{E}\left[y[n]\right]}{2\sigma}$$

- The second moment

$$\begin{aligned} \mathsf{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right] &= N\mathsf{Var}\left[\psi(y[n])\right] = N\left[\mathbb{E}\left[\left|\psi(y[n])\right|^2\right] - \left|\mathbb{E}\left[\psi(y[n])\right]\right|^2\right] \\ &= N\left[1 - \frac{\pi}{2}\frac{C}{4\sigma^2}\right] \approx N \end{aligned}$$

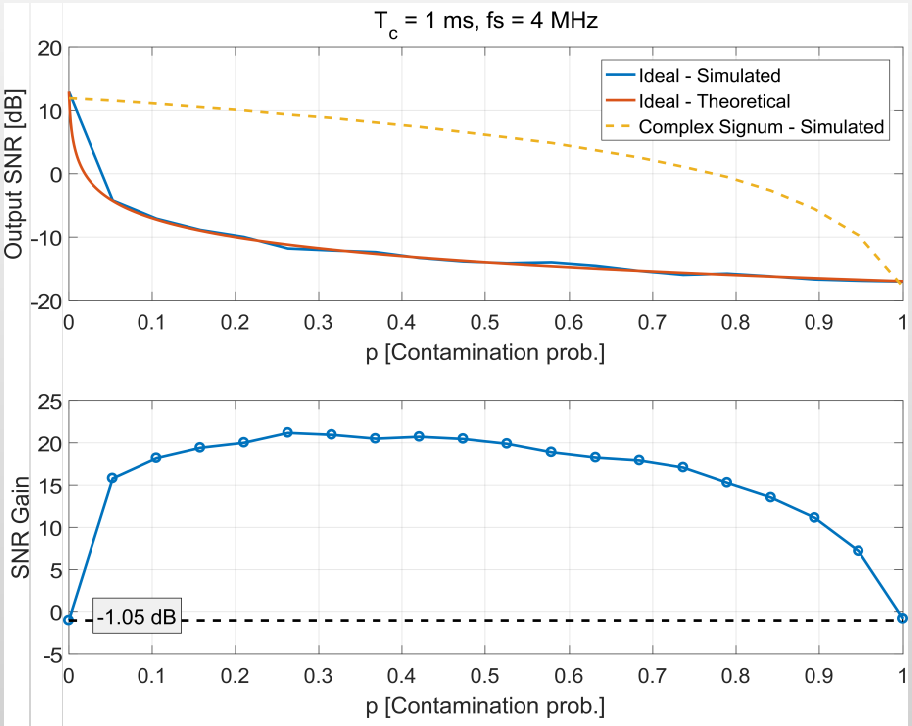
Loss of efficiency (Complex signum non-linearity)



$$L_0 = \frac{\pi}{4} \rightarrow -1.049 \text{ dB}$$

- L_0 is constant.
- a) Coherent output SNR as a function of the input C/N_0: simulation and theoretical results.
- b) Loss of efficiency caused by the complex sign non-linearity.

Loss of efficiency (Complex signum non-linearity)

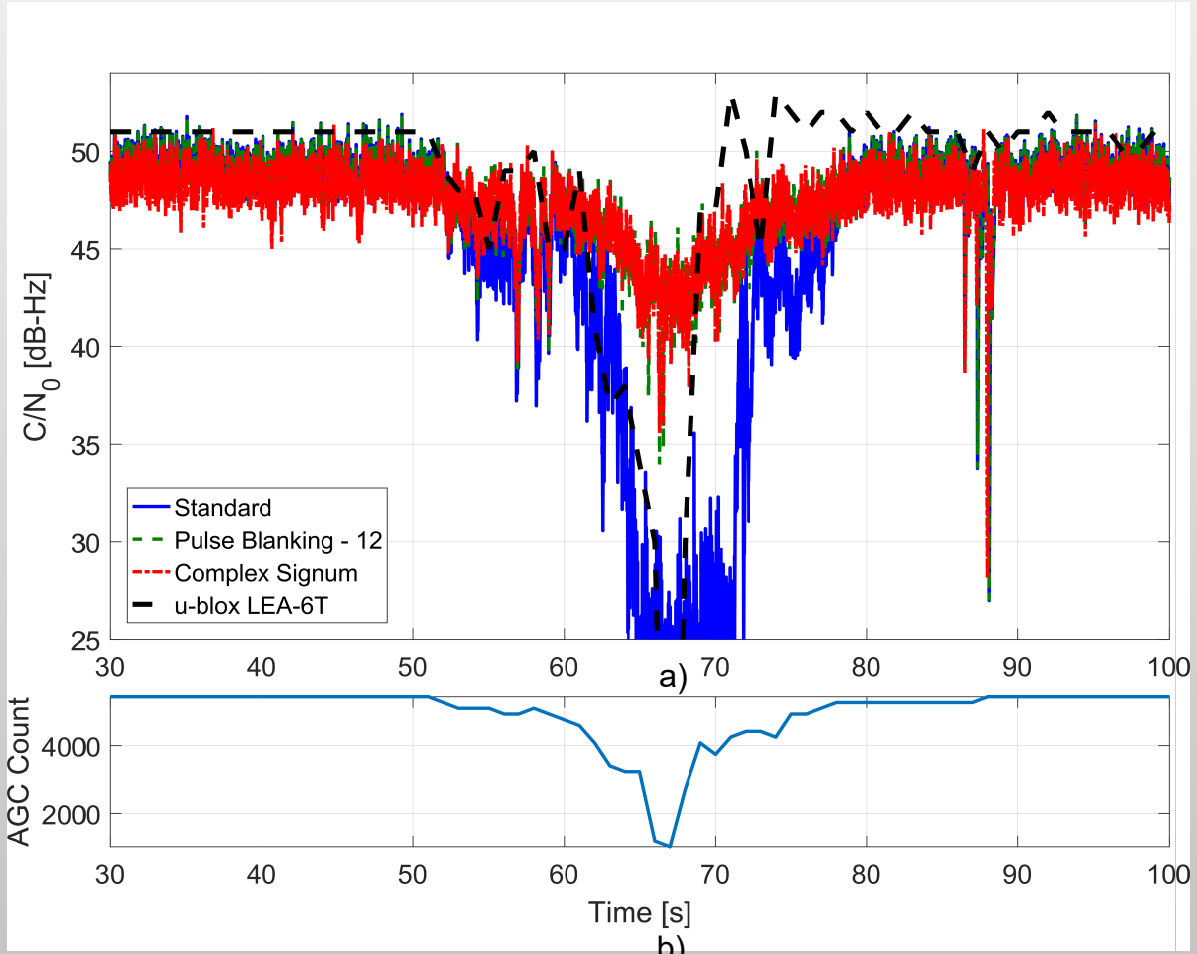


$$L_0 = \frac{\pi}{4} \rightarrow -1.049 \text{ dB}$$

- L_0 is constant.
- Coherent output SNR computed in the presence of pulsed interference as a function of the contamination probability, p.
- a) Comparison between standard and complex signum non-linearity.
- b) Gain obtained using the complex signum non-linearity.

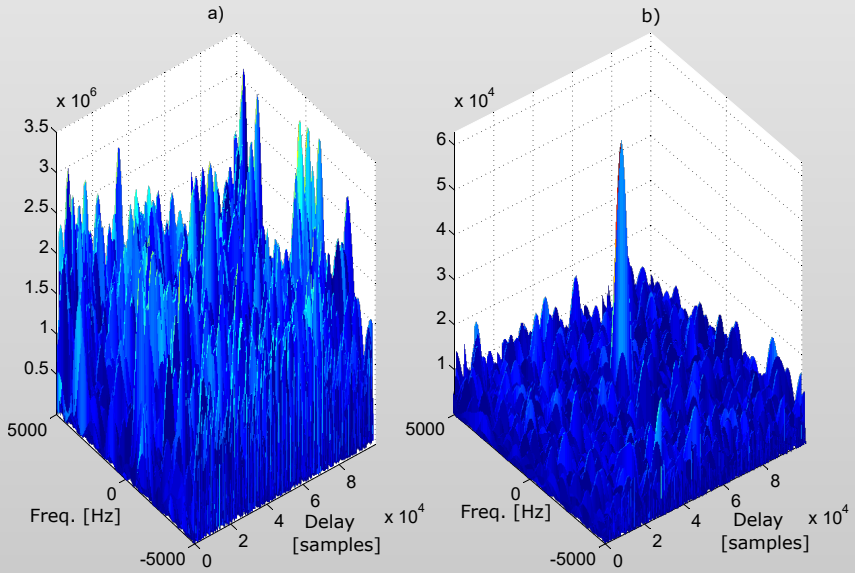
Complex signum non-linearity

- Back to the experimental setup. AGC values recorded with a u-blox LEA-6T receiver.



Complex signum non-linearity

- The main advantage of the complex signum non-linearity is that it does not require adjustment of any parameter.
- For instance, it does not require estimation of the noise power.



Robust Interference Mitigation (RIM)

- RIM is the general name for the robust CAF processing (Myriad, Complex signum, Huber, etc.)
- It can also be applied on transformed domains (TD), where the 'jammer is sparse'.
- Transform $\mathbf{T}_1$ produces the TD samples:

$$Y[k] = \mathbf{T}_1(y[n])$$

- Signal is processed through the non-linearity:

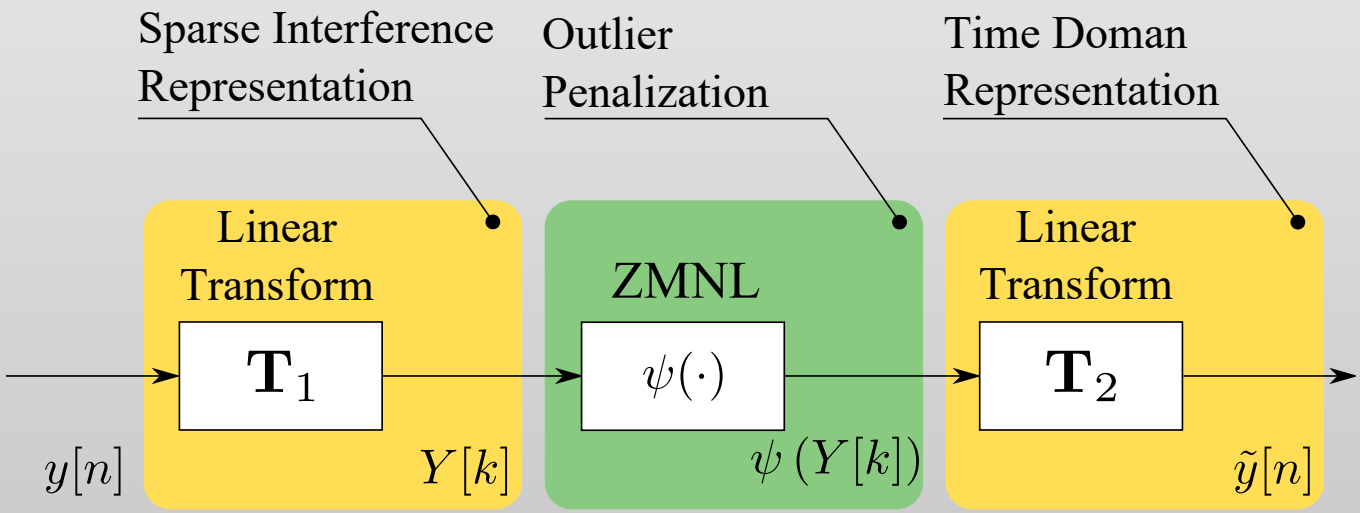
$$Y_\psi[k] = \psi(Y[k])$$

- ...and back to time domain:

$$\tilde{y}[n] = \mathbf{T}_2(Y_\psi[k])$$

Robust Interference Mitigation (RIM)

- RIM is the general name for the robust CAF processing (Myriad, Complex signum, Huber, etc.)
- It can also be applied on transformed domains (TD), where the 'jammer is sparse'.



Robust Interference Mitigation (RIM)

- RIM is the general name for the robust CAF processing (Myriad, Complex signum, Huber, etc.)
- It can also be applied on transformed domains (TD), where the 'jammer is sparse'.
- $\mathbf{T}_1$ and $\mathbf{T}_2$ are inverse operators such that $\mathbf{T}_1 \circ \mathbf{T}_2 = \mathbf{I}$.
- If $\mathbf{T}_1$ and $\mathbf{T}_2$ are identity operators, we end up performing RIM in the time domain.
- If $\mathbf{T}_1$ and $\mathbf{T}_2$ can be represented as invertible square matrices, they are orthogonal projection operators that change the signal representation basis. Here we consider only **orthonormal transformations that preserve power relationships**.

Transformed domain RIM

- Cost function $J(\tau, f_d, \varphi)$ can be interpreted as a norm and can be rewritten in vector form by introducing the following vectors

$$\mathbf{y} = \begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[N-1] \end{bmatrix} \quad \text{and} \quad \mathbf{s}(\tau, f_d) = \begin{bmatrix} c\left(-\tau\right) \\ c\left(T_s - \tau\right) \mathrm{e}^{j2\pi f_d T_s} \\ \vdots \\ c\left((N-1)T_s - \tau\right) \mathrm{e}^{j2\pi f_d (N-1) T_s} \end{bmatrix}$$

such that

$$\begin{aligned} J(\tau, f_d, \phi) &= \left\| \mathbf{y} - A\mathbf{s}(\tau, f_d) e^{j\phi} \right\|^2 \\ &= \left(\mathbf{y} - A\mathbf{s}(\tau, f_d) e^{j\phi}\right)^H \left(\mathbf{y} - A\mathbf{s}(\tau, f_d) e^{j\phi}\right) = \mathbf{r}^H \mathbf{r} \end{aligned}$$

[Bor19a] Borio, D., Closas, P. Robust transform domain signal processing for GNSS. NAVIGATION. 2019; 66: 305-323.

Transformed domain RIM

- The cost function can be expressed in a TD by introducing a norm-preserving matrix, $\mathbf{Q}$:

$$\begin{aligned} J(\tau, f_d, \phi) &= \mathbf{r}^H \mathbf{Q}^H \mathbf{Q} \mathbf{r} = (\mathbf{Q}\mathbf{r})^H \mathbf{Q}\mathbf{r} \\ &= \left\| \mathbf{Q}\mathbf{y} - \mathbf{Q} A \mathbf{s}(\tau, f_d) e^{j\phi} \right\|^2 \\ &= \left\| \mathbf{Y} - A \mathbf{S}(\tau, f_d) e^{j\phi} \right\|^2 \end{aligned}$$

  which is obtained under the assumption that

$$\mathbf{Q}^H \mathbf{Q} = \mathbf{I} \, .$$

- We assume that $\mathbf{Q}$ is a square matrix and that its rows define a new base for $\mathbf{y}$ and for $\mathbf{s}(\tau, f_d)$. Examples of such matrices are those defining the DFT and the Hadamard transform.

- The result is an expression of Parseval's theorem, which states that norms are preserved under unitary transformations.

- The cost function can be rewritten as

$$J\left(\tau, f_d, \varphi\right) = \sum_{k=0}^{N-1} \left| Y[k] - AS_{\tau, f_d}[k] e^{j\varphi} \right|^2$$

- For which now we know that a 'more robust version' exist

$$\begin{aligned} J_{TD}(\tau, f_d, \varphi) &= \sum_{k=0}^{N-1} \rho \left(Y[k] - AS_{\tau, f_d}[k] e^{j\varphi} \right) \\ &\approx \sum_{k=0}^{N-1} \rho \left(Y[k] \right) - A\Re \left\{ C_\rho^{TD} \left(\tau, f_d \right) e^{-j\varphi} \right\} \end{aligned}$$

with

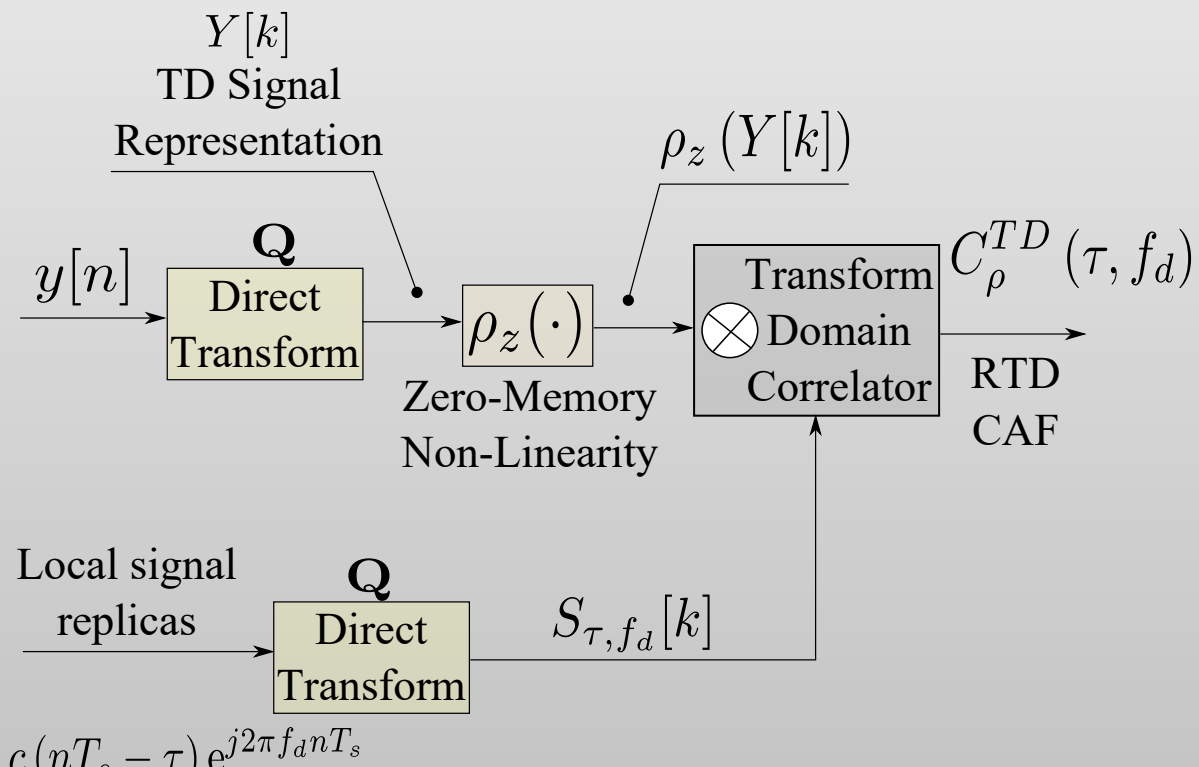
$$\mathcal{C}_\rho^{TD}(\tau, f_d) = \sum_{k=0}^{N-1} \psi \left(Y[k] \right) S_{\tau, f_d}^*[k]$$

Transformed domain RIM

- The estimation problem is then

$$\left\{\hat{\tau}, \hat{f}_d\right\} = \arg\max_{\tau, f_d} \left| C_\rho^{TD}\left(\tau, f_d\right)\right|$$

$$\hat{\varphi} = \angle\, C_\rho^{TD}(\hat{\tau}, \hat{f}_d).$$



Transformed domain RIM

- Implementation as a pre-correlation processing: applied only once!

$$\mathbf{Y}_\rho = \begin{bmatrix} \rho_z(Y[0]) \\ \rho_z(Y[1]) \\ \vdots \\ \rho_z(Y[N-1]) \end{bmatrix},$$

it is possible to express (1) as

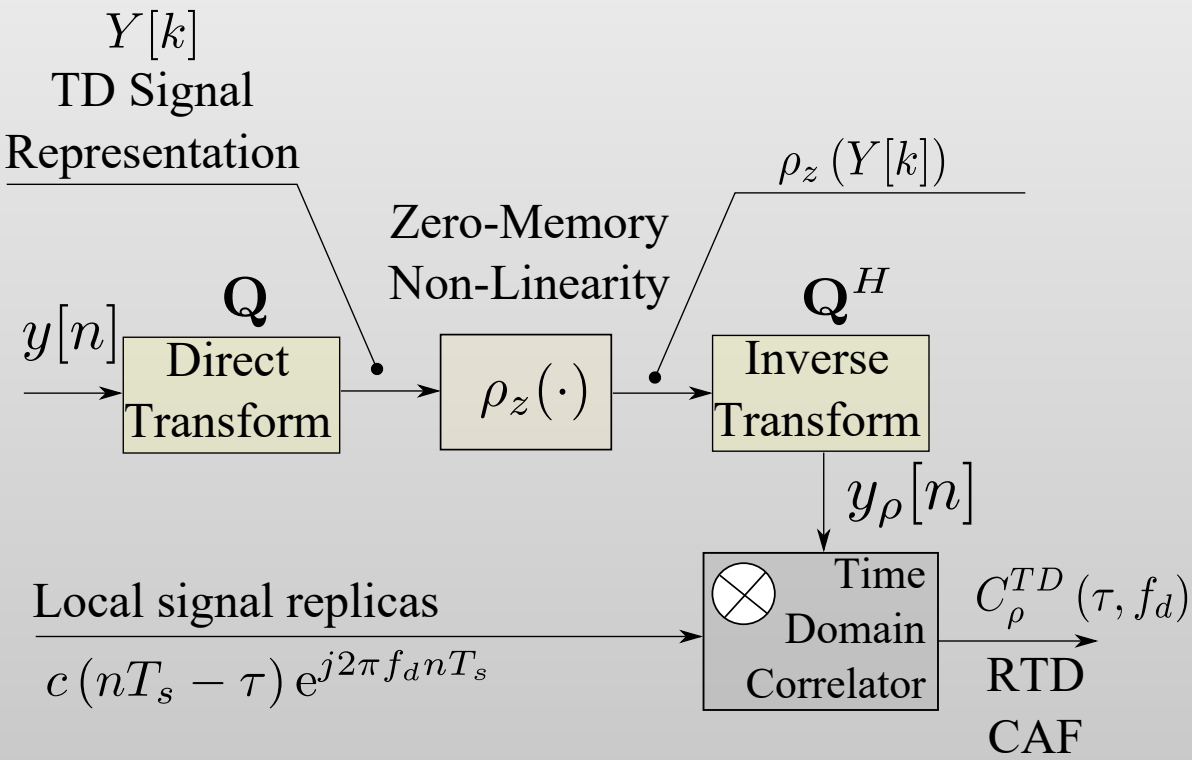
$$C_\rho^{TD}(\tau, f_d) = \sum_{k=0}^{N-1} \psi\left(Y[k]\right) S^*_{\tau,f_d}[k] = \mathbf{S}^H(\tau, f_d)\mathbf{Y}_\rho.$$

The transformation defined by $\mathbf{Q}$ is norm-preserving and thus,

$$\begin{aligned} C_\rho^{TD}(\tau, f_d) &= \mathbf{S}^H(\tau, f_d)\mathbf{Y}_\rho = \mathbf{S}^H(\tau, f_d)\mathbf{Q}\mathbf{Q}^H\mathbf{Y}_\rho \\ &= \left[\mathbf{Q}^H\mathbf{S}(\tau, f_d)\right]^H \left[\mathbf{Q}^H\mathbf{Y}_\rho\right] = \mathbf{s}^H(\tau, f_d)\mathbf{y}_\rho \end{aligned}$$

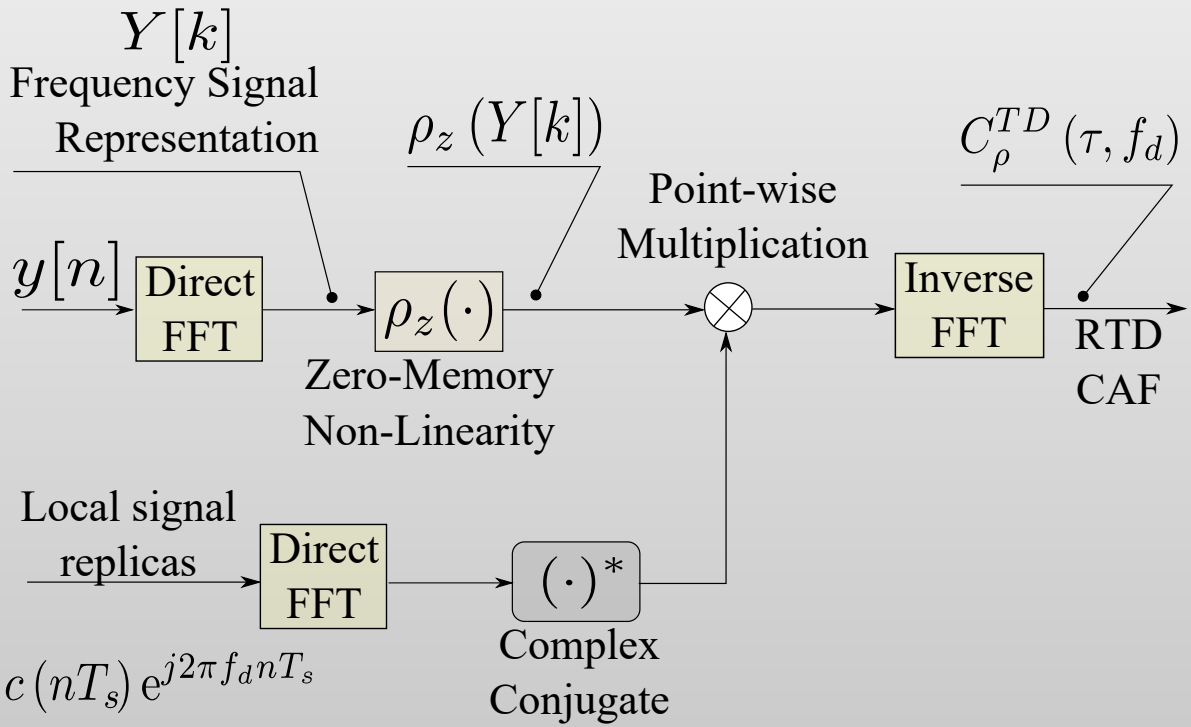
Transformed domain RIM

- Implementation as a pre-correlation processing: applied only once!



Transformed domain RIM

- FFT-based implementation: reuse efficient structures.



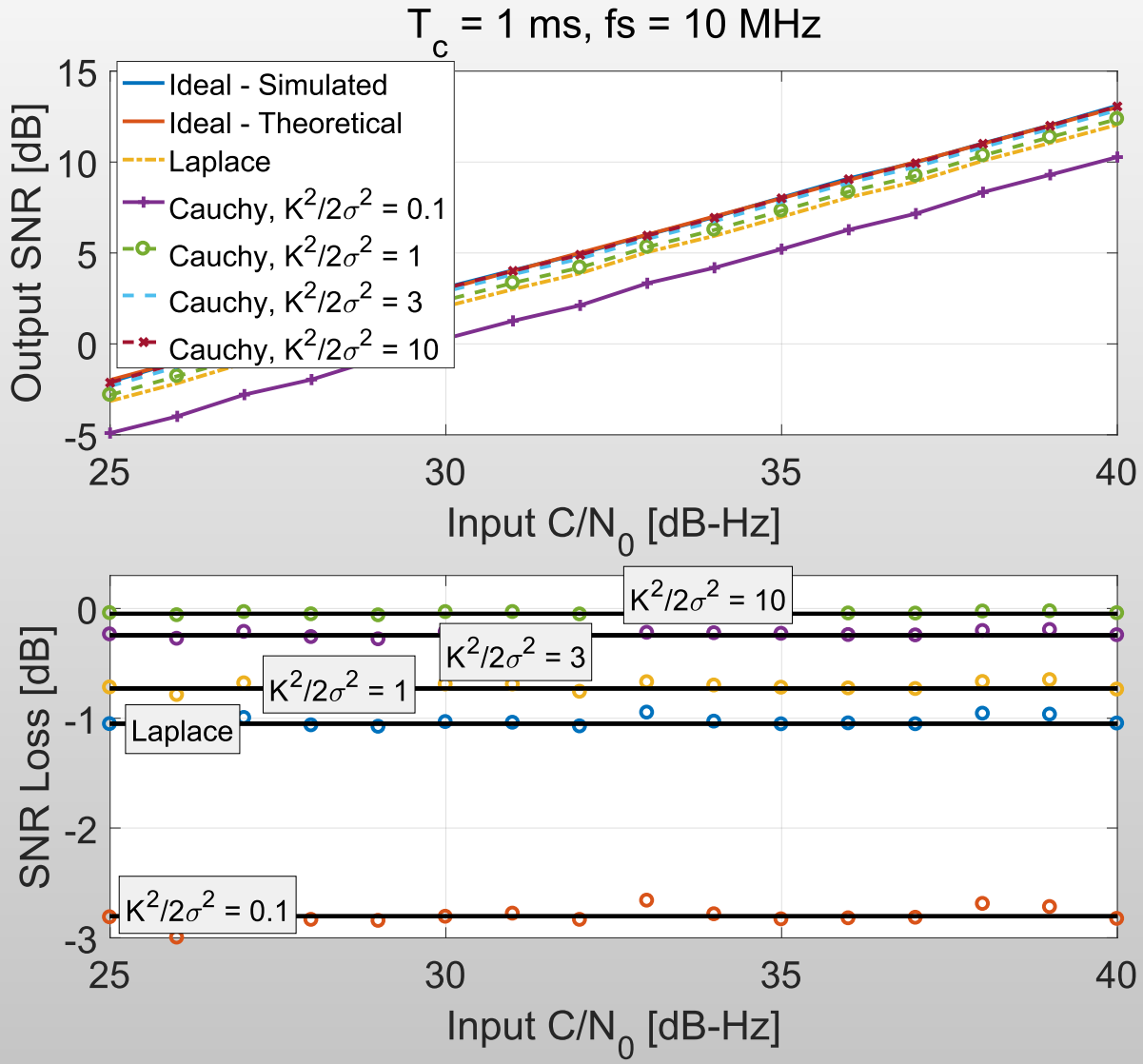
Transformed Domain RIM's loss of efficiency

- Loss of efficiency analysis is the same as for time domain processing, thanks to the *convenient choice* of the transformation $\mathbf{Q}$.
- Since $\mathbf{Q}$ defines an orthonormal basis that preserves noise and signal power relationships, we have that:

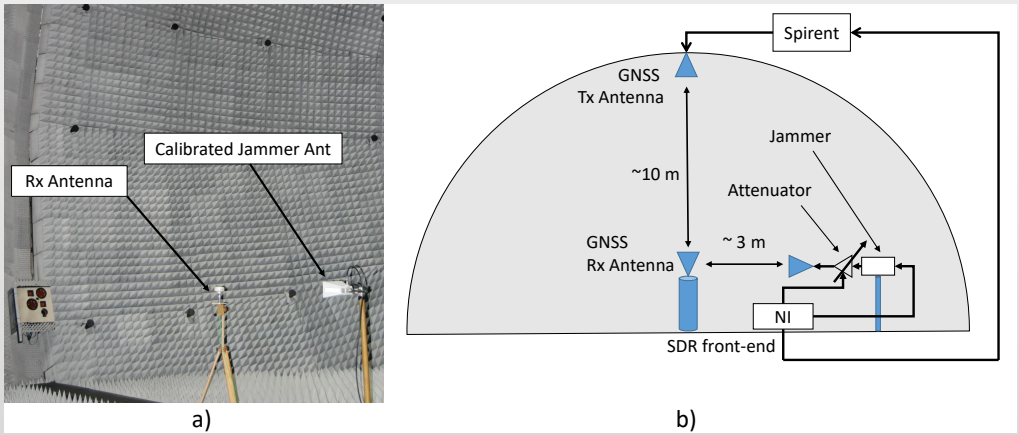
$$L_0 = L_0^{TD}$$

regardless of the transformation $\rho(\cdot)$.

Transformed Domain RIM's loss of efficiency



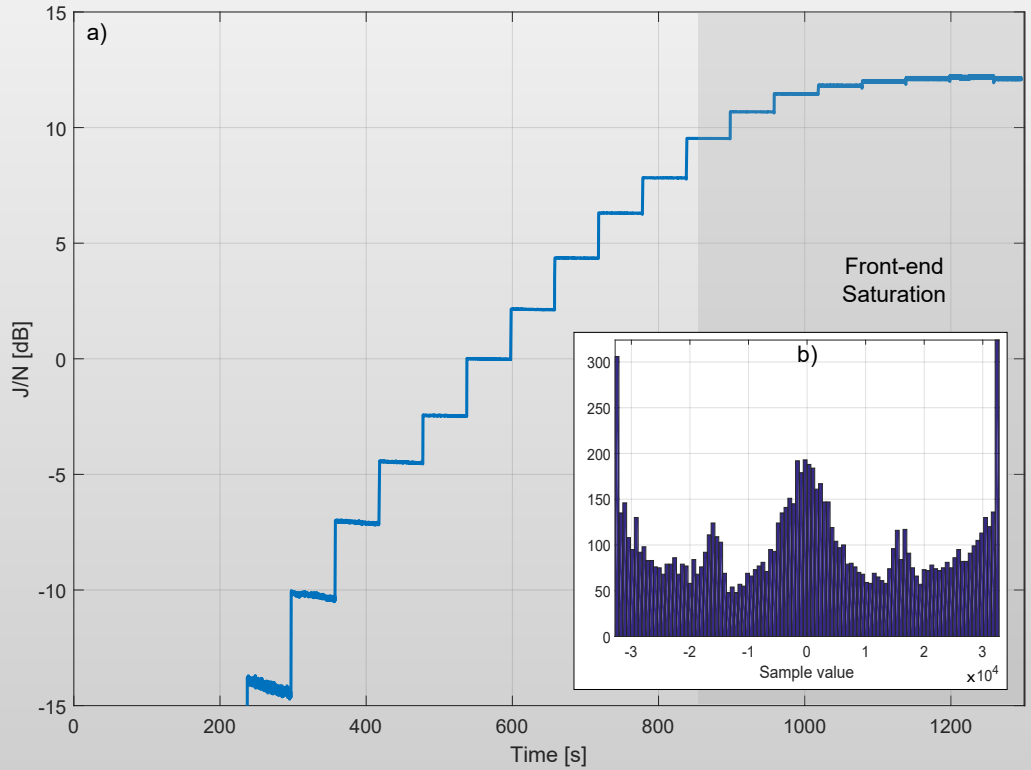
RIM's experimental results



- Experiment performed at JRC, Ispra.
- Jammer swept over 12 MHz in 9μs.
- Incremental attenuation from 81 to 45 dB.
- $f_s = 10$ MHz and 16 bits.

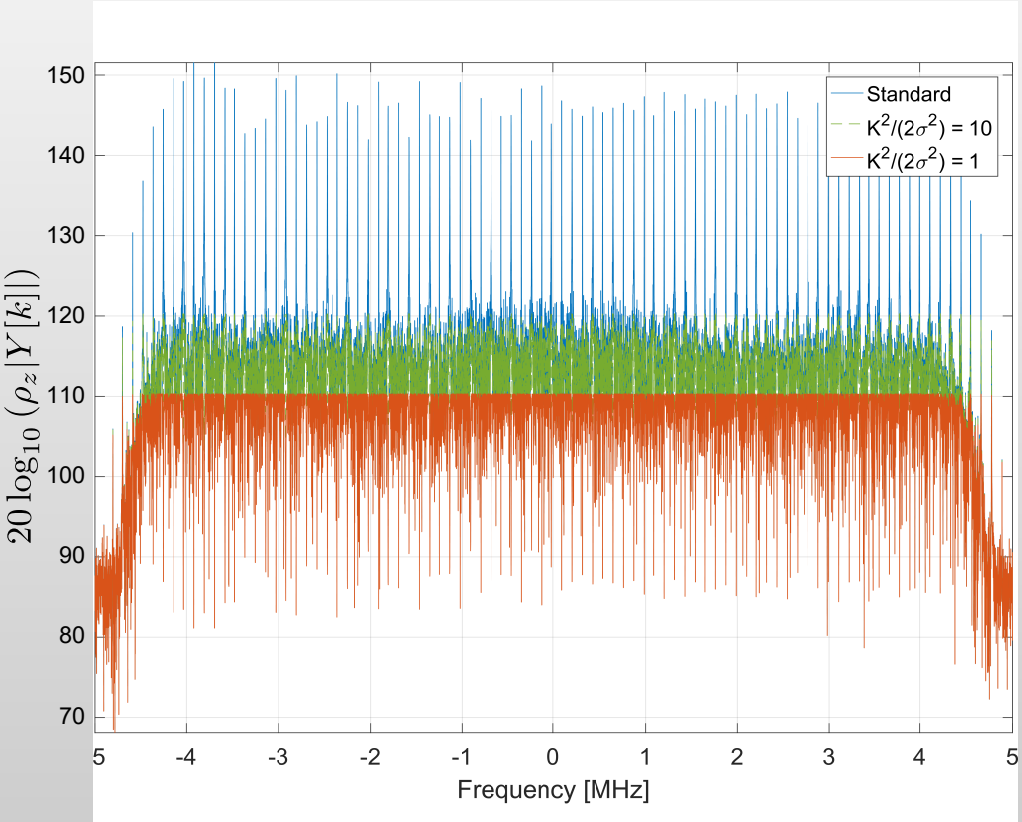
[Bor12] D. Borio, C. ODriscoll, and J. Fortuny, "GNSS jammers: Effects and countermeasures," in Proc.of the 6th ESA Workshop on Satellite Navigation Technologies (Navitec), Dec. 2012, pp. 1-7.

RIM's experimental results



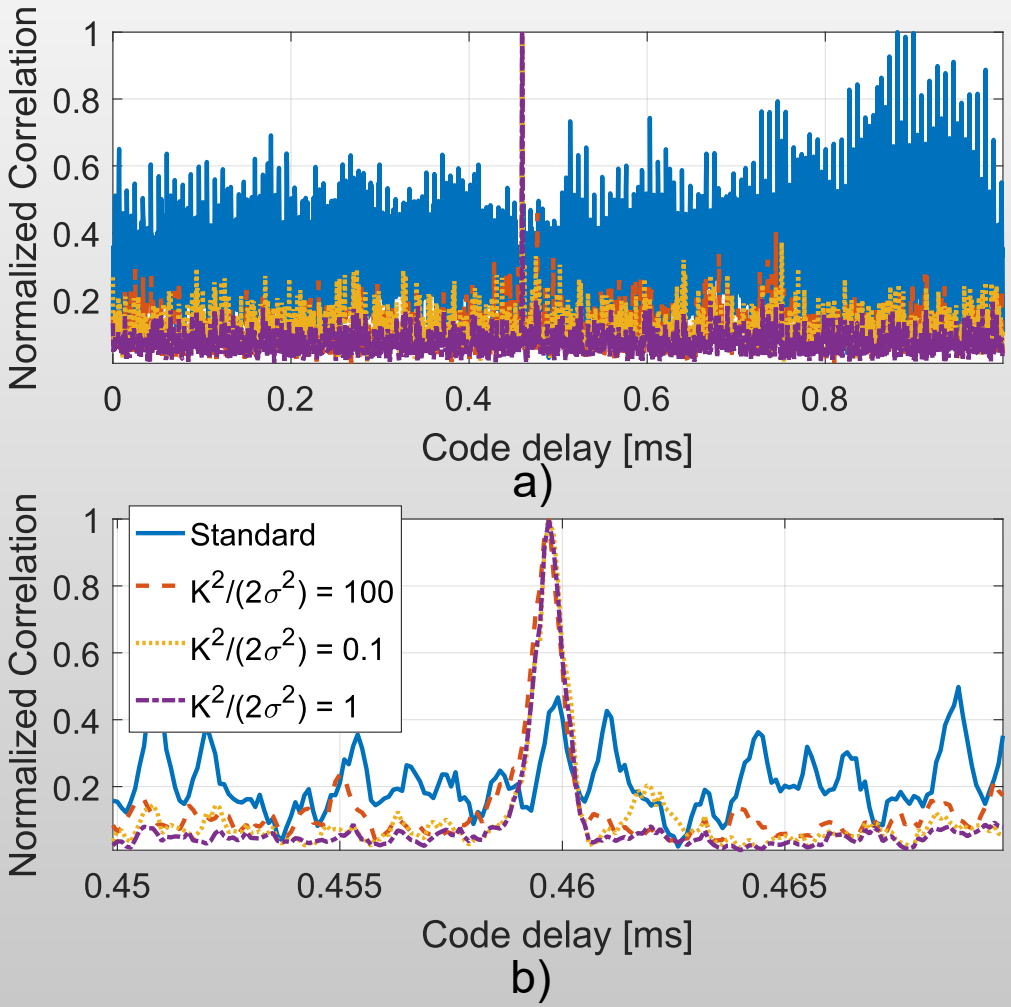
- Experiment performed at JRC, Ispra.
- Jammer swept over 12 MHz in 9μs.
- Incremental attenuation from 81 to 45 dB.
- $f_s = 10$ MHz and 16 bits.

RIM's experimental results



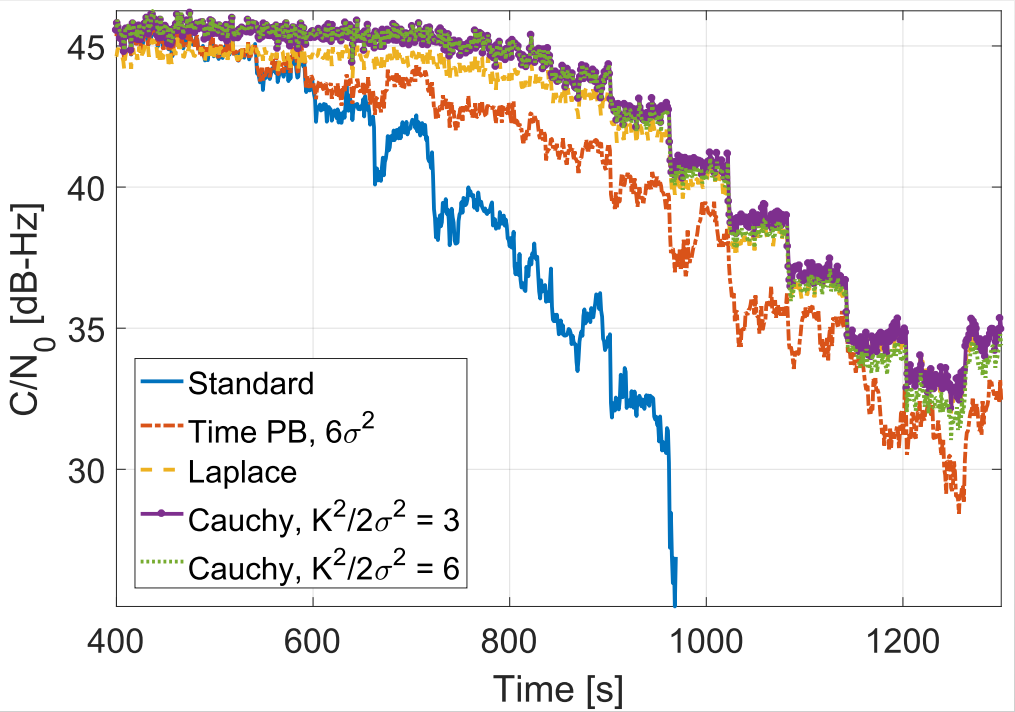
- Experiment performed at JRC, Ispra.
- Jammer swept over 12 MHz in 9μs.
- Incremental attenuation from 81 to 45 dB.
- $f_s = 10$ MHz and 16 bits.

RIM's experimental results



- Experiment performed at JRC, Ispra.
- Jammer swept over 12 MHz in 9μs.
- Incremental attenuation from 81 to 45 dB.
- $f_s = 10$ MHz and 16 bits.

RIM's experimental results



- Experiment performed at JRC, Ispra.
- Jammer swept over 12 MHz in 9μs.
- Incremental attenuation from 81 to 45 dB.
- $f_s = 10$ MHz and 16 bits.

Huber's non-linearity

- So far, we only considered Cauchy and Laplace distributions to generate $\rho(\cdot)$, but many other options are possible.
- In the field of robust statistics, Huber function is one popular option when it comes to developing robust estimation methods.
- The function is defined as

$$\rho(z) = \begin{cases} \frac{1}{2}z^2 & \text{for } |z| \leq T_h \\ T_h|z| - \frac{1}{2}T_h^2 & \text{for } |z| > T_h \end{cases}$$

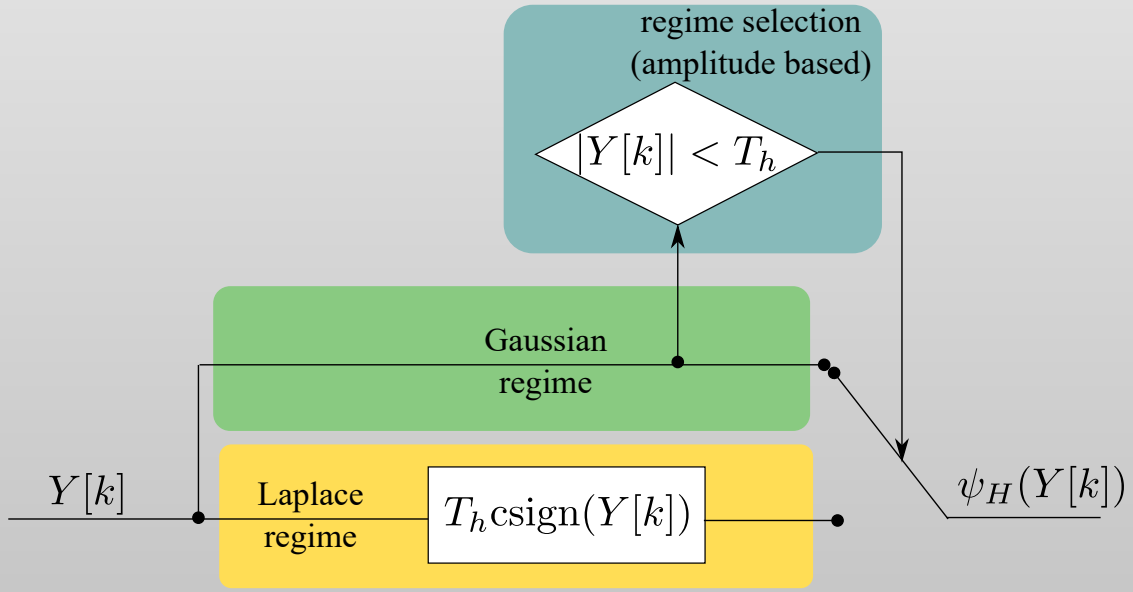
where T_h is a decision threshold.

Huber's non-linearity

- The resulting Huber non-linearity applied to the data is

$$\psi(y[n]) = \begin{cases} y[n] & \text{for } |y[n]| \leq T_h \\ T_h \text{ csign}(y[n]) & \text{for } |y[n]| > T_h \end{cases}$$

- Not based on a distribution $f(\cdot)$, but still interpretable...



Loss of efficiency (Huber's non-linearity)

- Recall that the loss of efficiency is defined as the ratio of coherent output SNRs of standard and robust processing:

$$L_0 = \frac{\mathrm{SNR}_{\mathrm{out},\rho}}{\mathrm{SNR}_{\mathrm{out}}}$$

- $\mathrm{SNR}_{\mathrm{out}}$ is obtained as before.
- Similarly, $\mathrm{SNR}_{\mathrm{out},\rho}$ is defined as

$$\mathrm{SNR}_{\mathrm{out},\rho} = \max_{\tau, f_d} \frac{\left|\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right]\right|^2}{\frac{1}{2}\mathrm{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right]},$$

where $\mathcal{C}_\rho(\cdot,\cdot)$ is now the complex signum non-linearity.

Loss of efficiency (Huber's non-linearity)

- The first moment

$$\mathbb{E}\left[\mathcal{C}_\rho(\tau, f_d)\right] = \sum_{n=0}^{N-1} \mathbb{E}\left[\psi(y[n])\right] c\left(nT_s - \tau\right) \mathrm{e}^{-j2\pi f_d n T_s}.$$

  which under the weak signal assumption

$$\mathbb{E}\left[\psi(y[n])\right] = \mathbb{E}\left[y[n]\right] \left(1 - -\frac{T_h^2}{2\sigma^2} + \frac{\sqrt{\pi}}{2} \frac{T_h}{\sqrt{2}\sigma} \mathrm{erfc}\left(\frac{T_h}{\sqrt{2}\sigma}\right)\right)$$

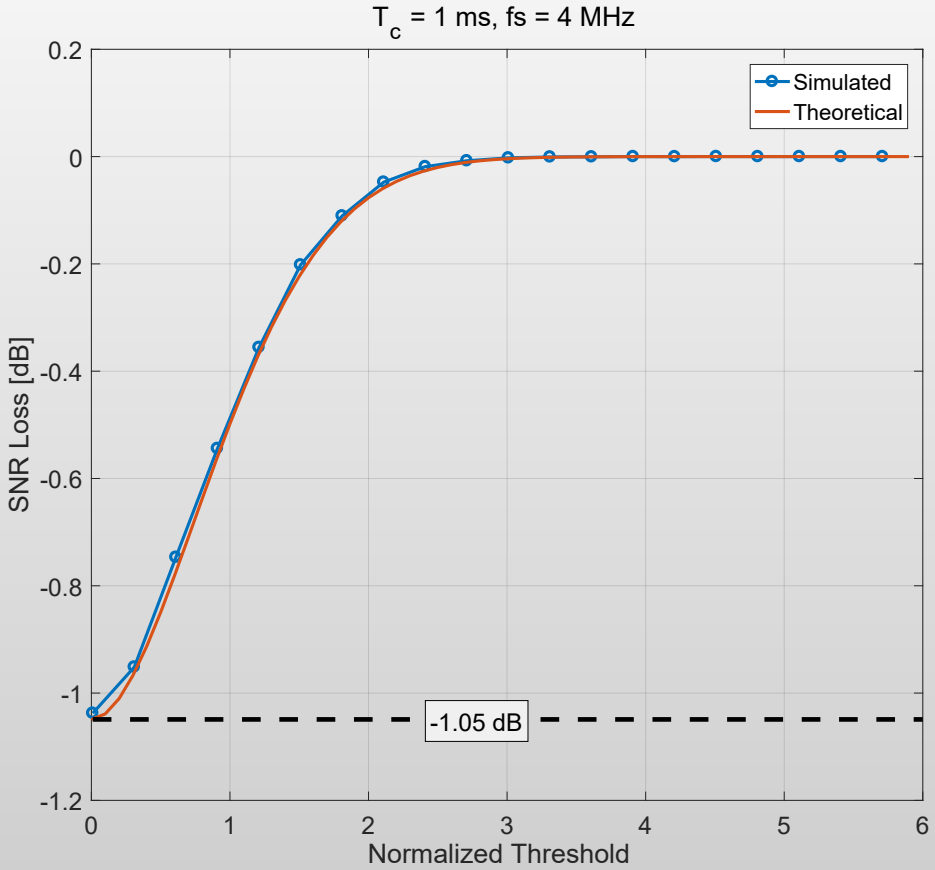
- The second moment

$$\mathrm{Var}\left[\mathcal{C}_\rho(\tau, f_d)\right] = \mathrm{Var}[\mathcal{C}(\tau, f_d)] \left[1 - \mathrm{e}^{-\frac{T_h^2}{2\sigma^2}}\right]$$

- The loss of efficiency results in

$$L_0(T_h) = \frac{\left[1 - \mathrm{e}^{-\frac{T_h^2}{2\sigma^2}} + \frac{T_h}{\sqrt{2}\sigma} \frac{\sqrt{\pi}}{2} \mathrm{erfc}\left(\frac{T_h}{\sqrt{2}\sigma}\right)\right]^2}{1 - \mathrm{e}^{-\frac{T_h^2}{2\sigma^2}}}.$$

Loss of efficiency (Huber's non-linearity)



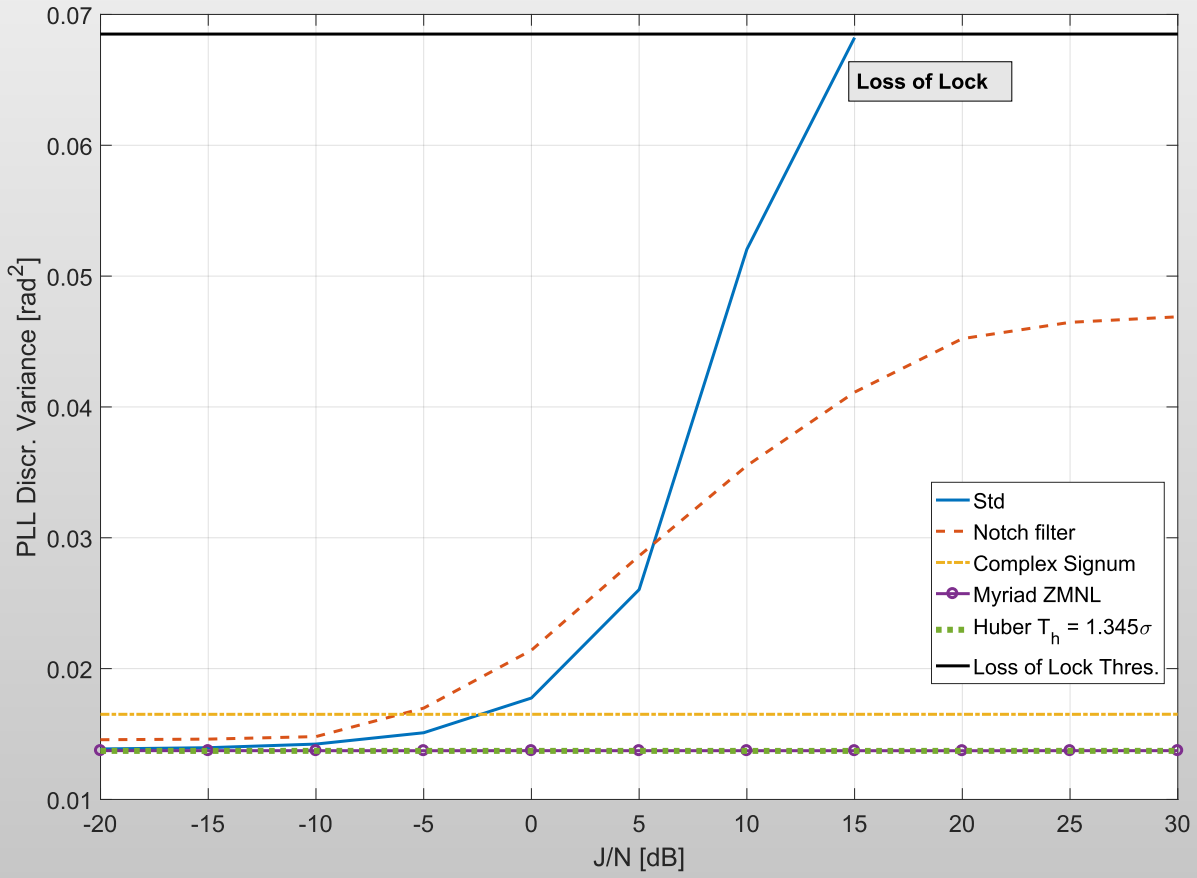
- L_0 depends on the normalized threshold $\frac{T_h}{\sigma}$.
- Gaussian and Laplacian regimes.

$$T_h \to \infty \Rightarrow L_0(T_h) \to 1$$

$$T_h \to 0 \Rightarrow L_0(T_h) \to \frac{\pi}{4}$$

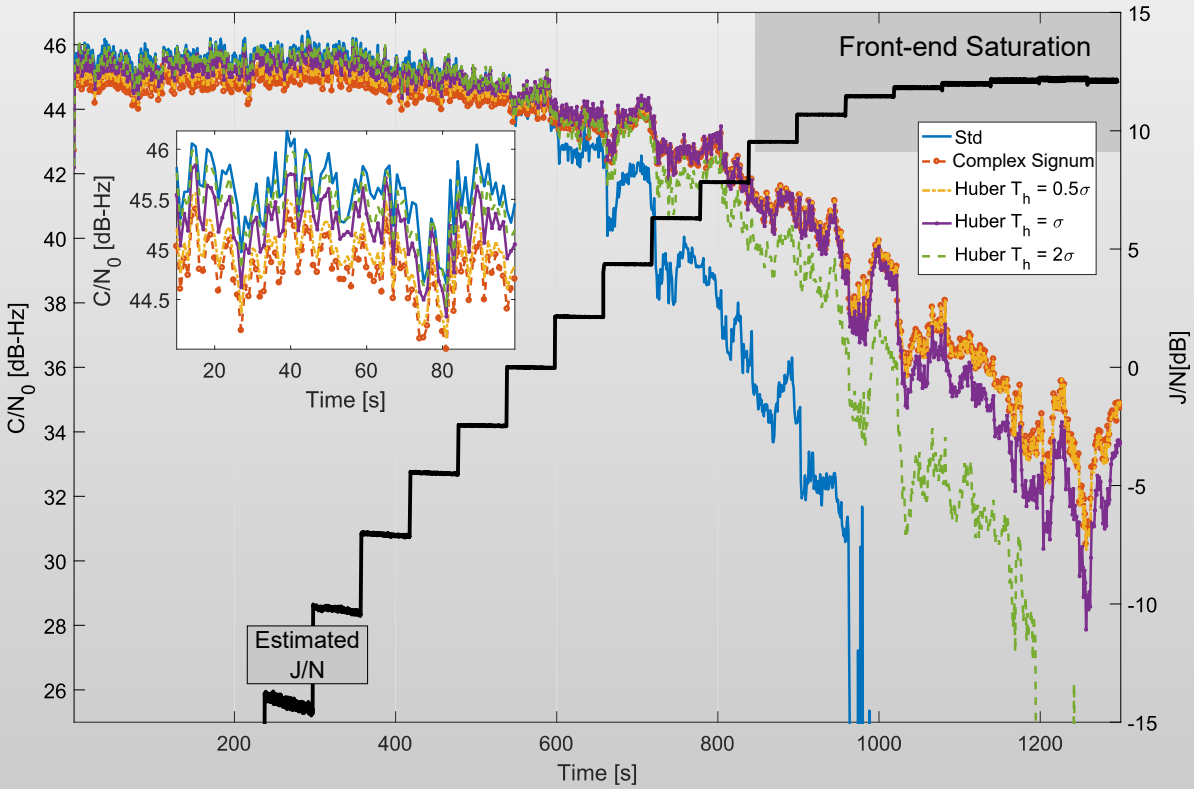
Huber's non-linearity

- Back to the experimental setup: PLL tracking performance (simulated), similar for DLL performance.



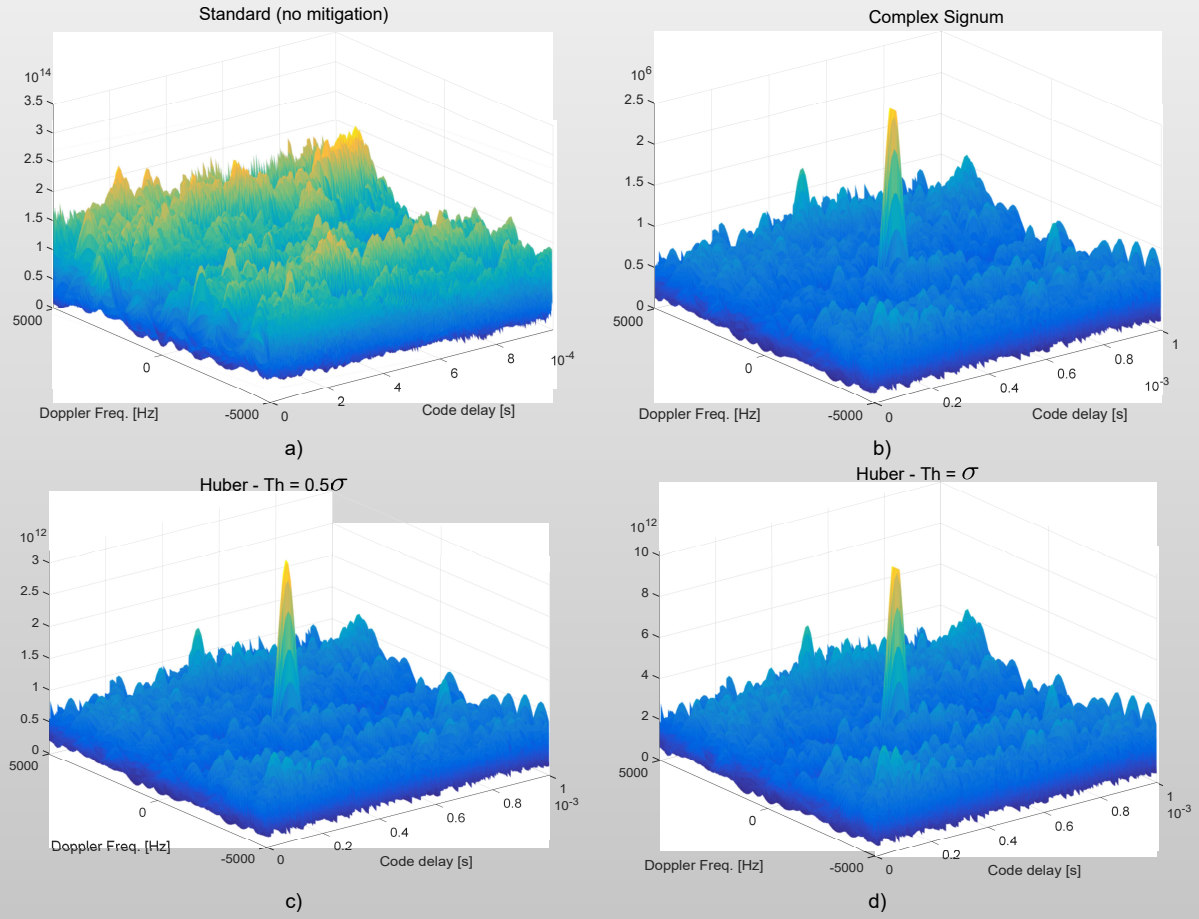
Huber's non-linearity

- Back to the experimental setup: C/N_0 performance (real data)



Huber's non-linearity

- Back to the experimental setup: C/N_0 performance (real data)



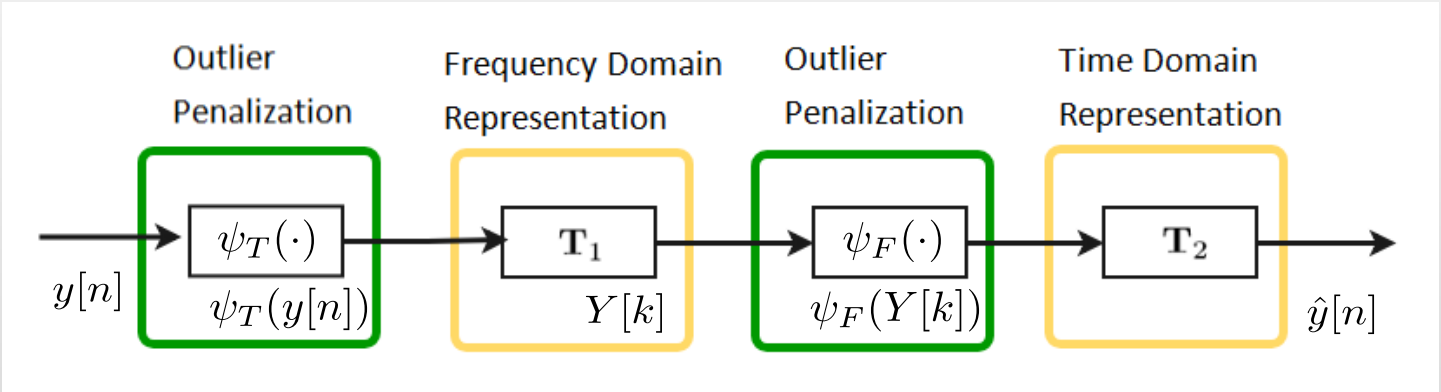
Dual-Domain RIM

- In principle, one does not know the type of interference that the receiver will encounter.
- Some interferences are sparse in time domain (e.g. pulsed interferences) while others in transformed domains (e.g. CW).
- Idea: can RIM be *preventively* applied in both domains? what is the loss of efficiency?
- **Dual-Domain RIM** (DD-RIM) formalizes, precisely, that methodology.

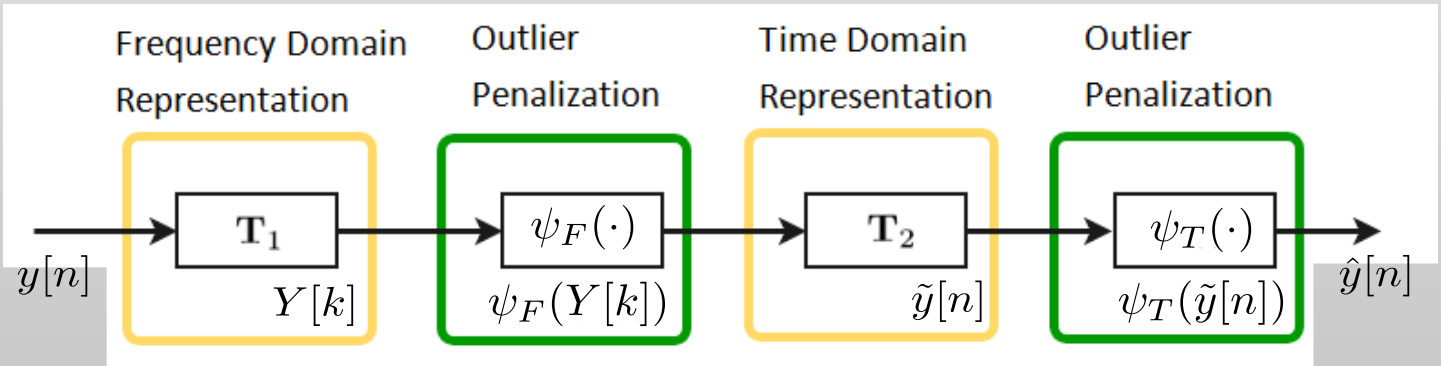
[Li19] H. Li, D. Borio, P. Closas, "Dual-Domain Robust GNSS Interference Mitigation," in Proc. of the ION GNSS+ 2019, 16-20 September 2019, Miami, FL.

Dual-Domain RIM

'time-then-frequency'

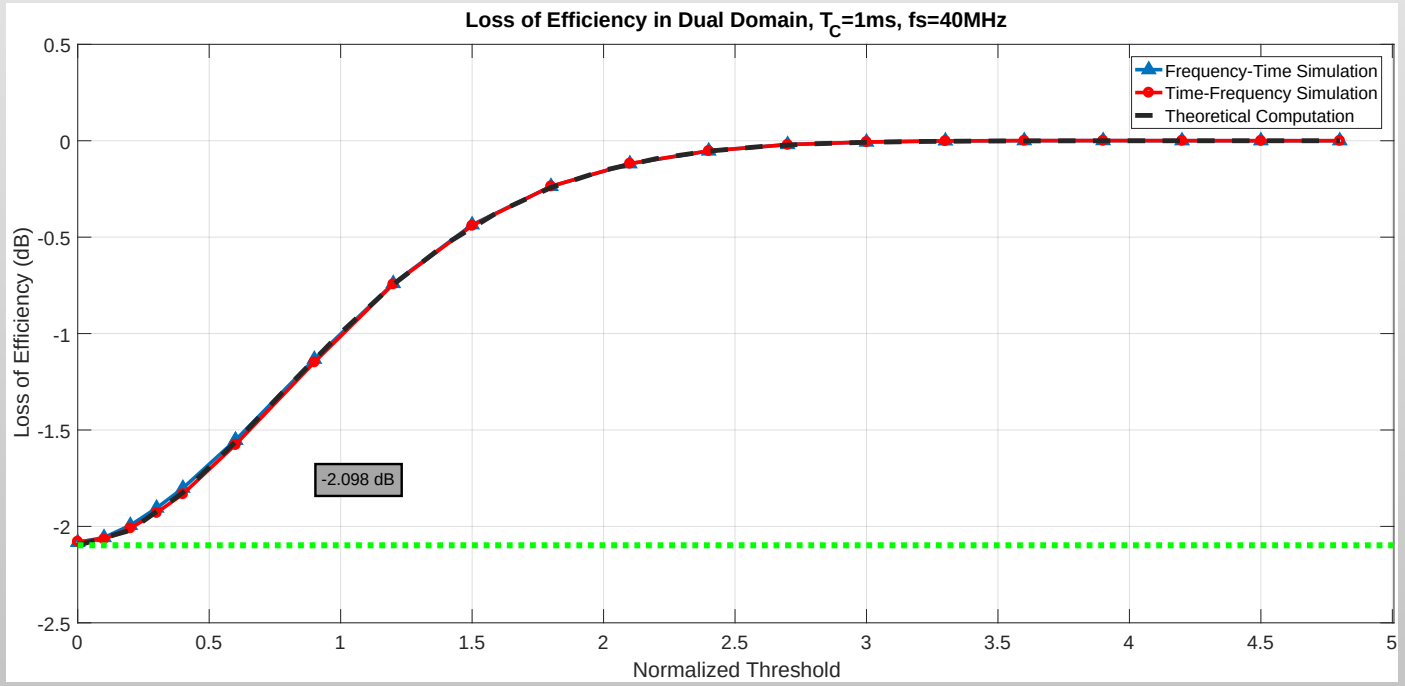


'frequency-then-time'



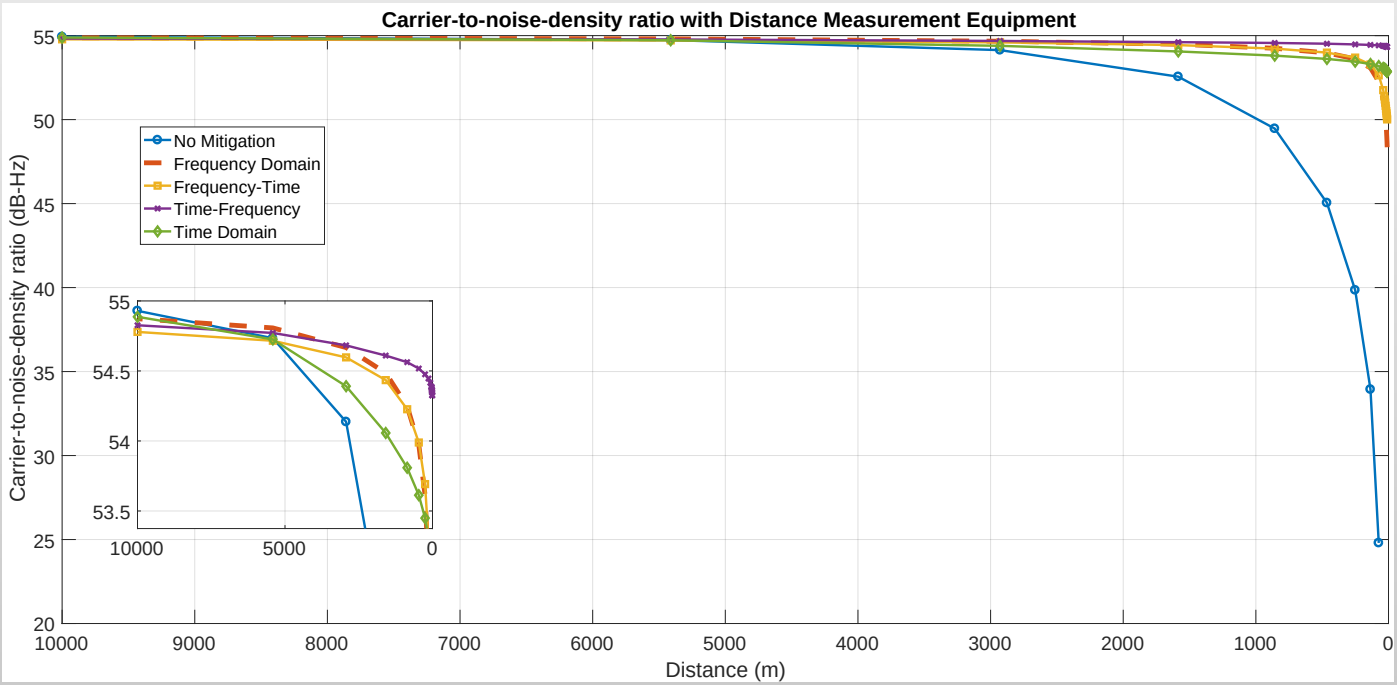
Loss of efficiency (Dual-Domain RIM)

- It can be shown that the loss of efficiency is **twice** the one computed in single-domain RIM. It is also intuitive.
- It can be also shown that the loss of efficiency of 'time-then-frequency' is the same as that of 'frequency-then-time'.
- For instance, for Huber:

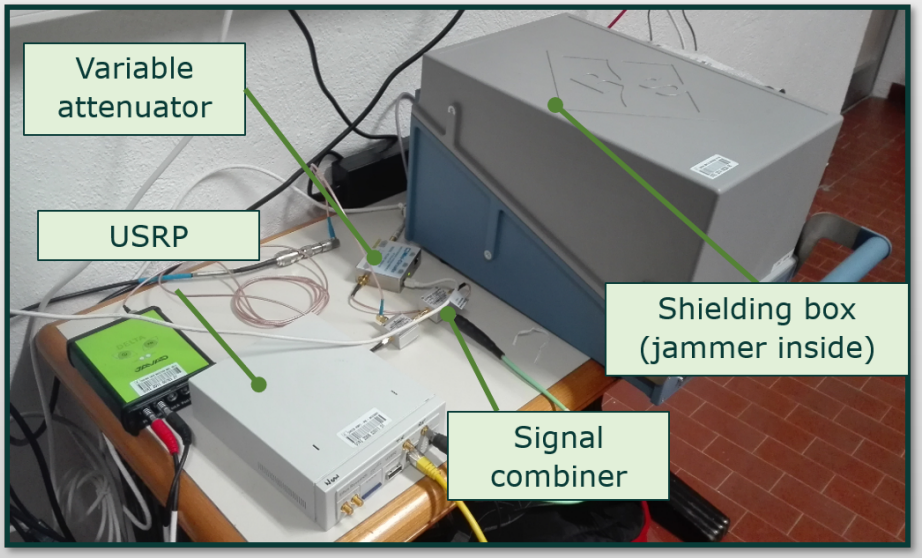


Dual-Domain RIM

- Simulated DME signal (sparse in both time and frequency domains).

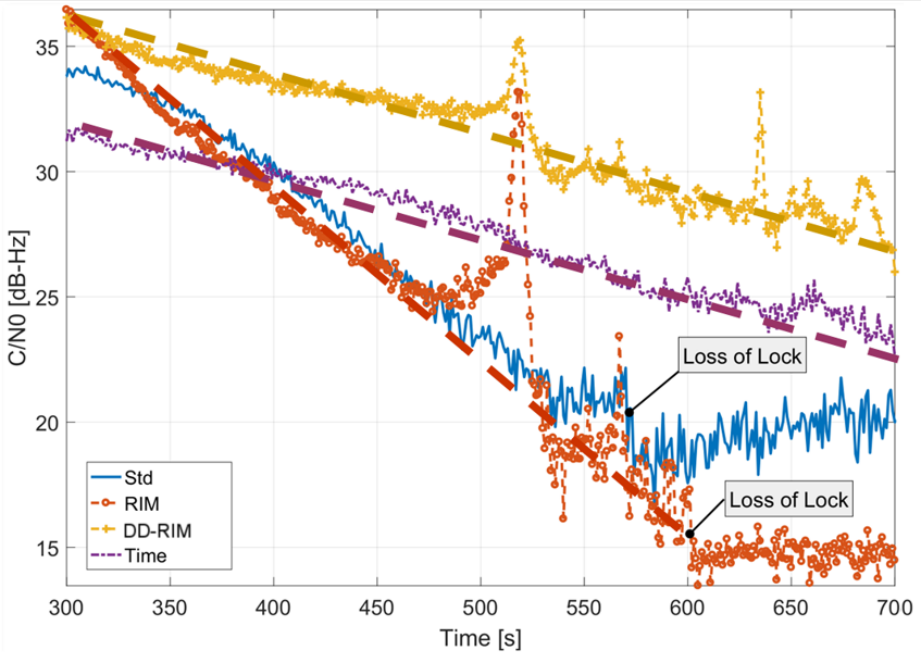


Dual-Domain RIM



- Experiment performed at JRC, Ispra.
- Jammer swept over 15 MHz, ~ 9 dBm.
- Galileo E5b signal (wide-band)
- Narrowband front-end: Realtek RTL2832u.
- $f_s = 2.048$ MHz and 8 bits.

Dual-Domain RIM



- Experiment performed at JRC, Ispra.
- Jammer swept over 15 MHz, ~ 9 dBm.
- Galileo E5b signal (wide-band)
- Narrowband front-end: Realtek RTL2832u.
- $f_s = 2.048$ MHz and 8 bits.

Summary (so far, IV)

- Under jamming interferences, the Gaussian assumption is not satisfied.
- Robust methods can be developed to improve the CAF optimization process.
- A number of techniques are available (and more) for which the loss of efficiency is understood.
- Robust Interference Mitigation (RIM) is an appealing framework that requires less detection/estimation than classic interference mitigation techniques such as those of Interference Cancellation (IC).
- RIM is based on the assumption that the interference is sparse in a certain domain(s), and thus treated as an outlier.
- RIM can be applied in transformed domains.
- RIM can be applied in multiple domains.

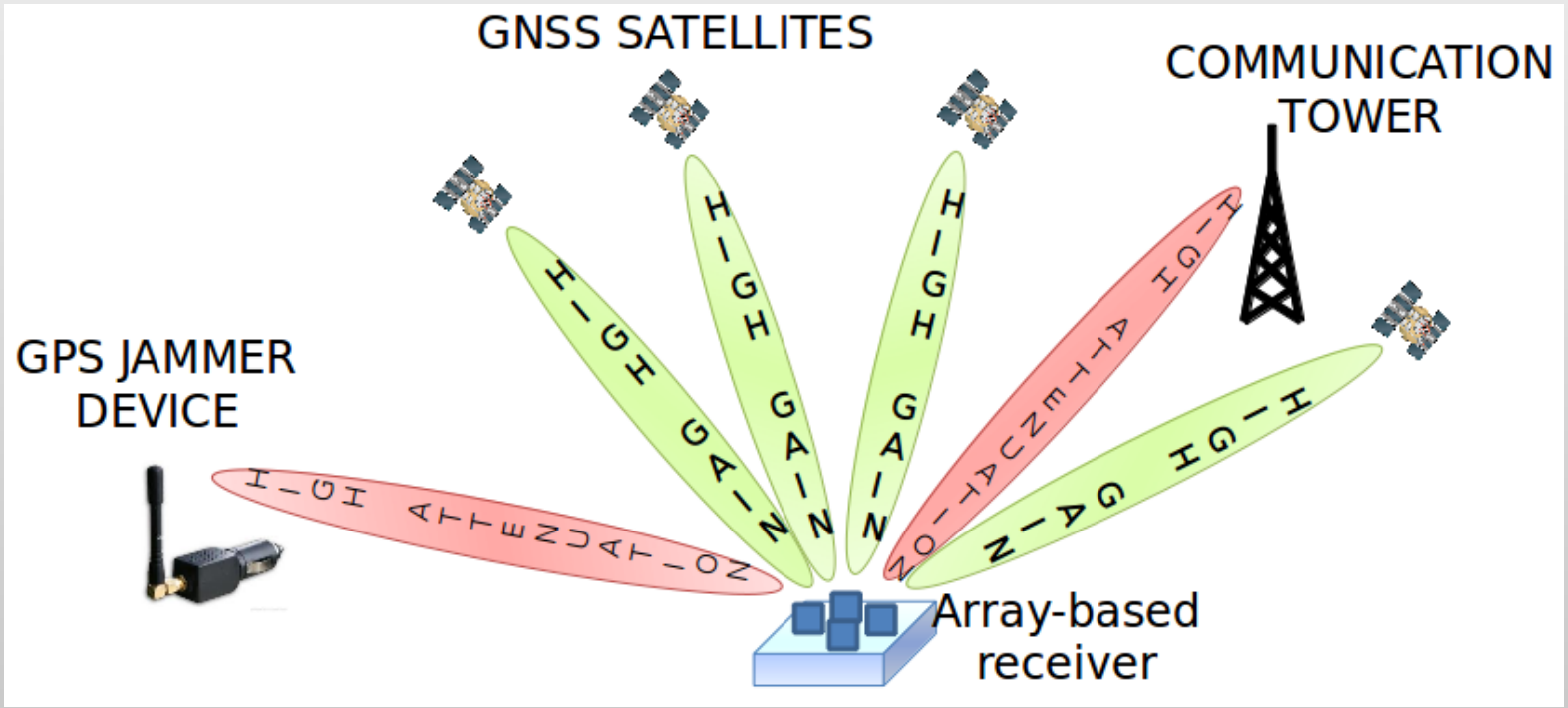
Outline

Introduction

- The previously discussed detection/mitigation techniques are very useful but do not provide robustness against match spectrum and broadband noise jammers, although spread-spectrum provides intrinsic rejection.
- For powerful jamming, this rejection might not be enough to increase the $\frac{C}{N_{0,\text{eff}}}$
- In addition to the detection/mitigation techniques developed for single antenna receivers, one can use multi-antenna frontends to improve $\frac{C}{N_{0,\text{eff}}}$ either decreasing C_I or increasing C.
- Landscape:
  - Mass-market receivers use omnidirectional antennas with no rejection capabilities.
  - Professional receivers have fixed gain patterns to attenuate low elevation RF signals.
  - Advanced receivers can support multi-antenna elements to adapt the gain pattern to the signal, interference, and noise environment.

Introduction

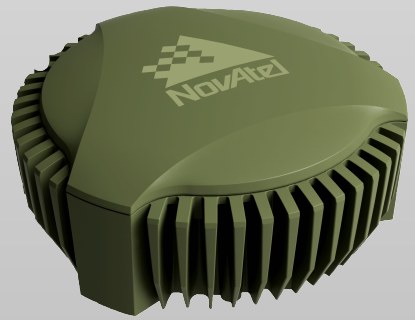
- Steering the beam pattern the receiver can place nulls and/or point to specified directions.



Introduction

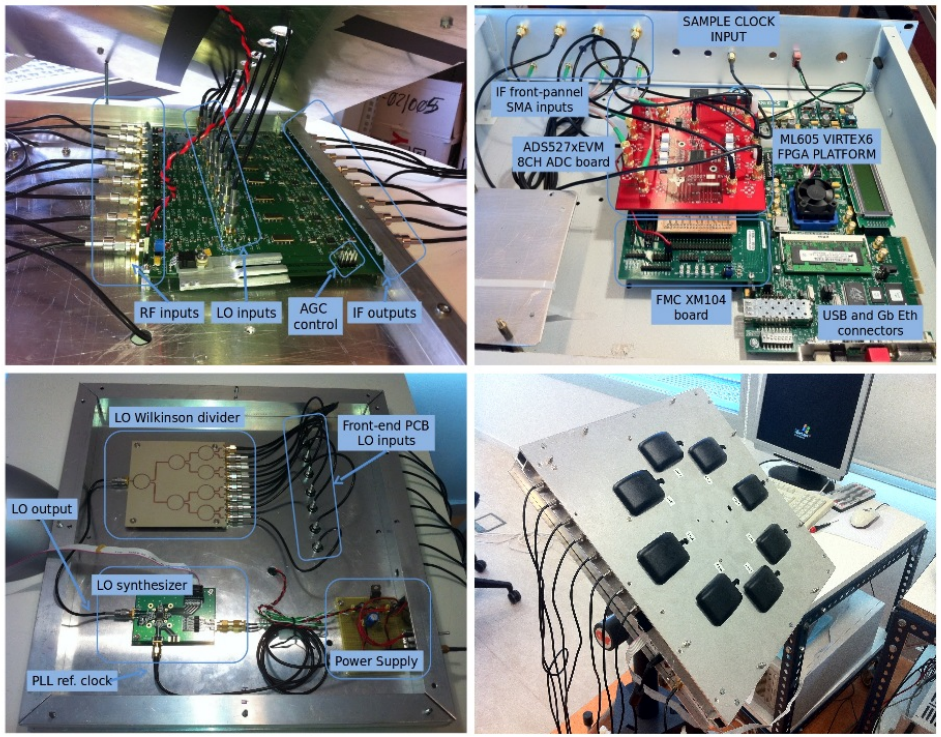
Examples of deployed systems:

- NovAtel-QinetiQ GAJT-700 ML
  - 7 antenna elements,
  - can create up to 6 independent nulls in GPS L1 and L2, and
  - the size of this CRPA is a diameter of 29 cm and a height of 12 cm, weighting 7.5 kg.
- Raytheon's GPS anti-jamming products
  - known as GAS-1, MiniGAS, and Advanced Digital Antenna Production (ADAP) systems
  - GAS-1 is a 7-element adaptable phased-array antenna, and
  - ADAP adds enhanced interference mitigation and dual-frequency beam-forming capabilities.



Introduction

- These systems are targeted to a particular market...
- Several research groups are actively working on the area (with even bulkier prototypes!)



Signal model

- An N–element antenna array receives signals from M satellites, each one with $M(m)$ scaled, time–delayed and Doppler–shifted replicas (multipath), plus interferences and thermal noise. At each antenna, the receiving baseband signal can be modeled as

$$x(t) = \sum_{m=1}^{M} \sum_{p=0}^{M(m)-1} a_{m,p} s_m(t - \tau_{m,p}) e^{j2\pi f_{m,p} t} + \sum_{\ell=1}^{M_I} i_\ell(t) + n(t) \ ,$$

- Each antenna receives a different replica of those signals, with a different phase depending on the array geometry and the direction of arrival (DOA).

Signal model

- The corresponding vector signal model, where each row corresponds to one antenna:

$$\mathbf{x}(t) = \sum_{m=1}^{M} \mathbf{H}_m \mathbf{b}_m(t) + \mathbf{H}_I \mathbf{i}(t) + \mathbf{n}(t) \ ,$$

where:

- $\mathbf{x}(t) \in \mathbb{C}^{N\times 1}$ is the observed signal vector (snapshot),
- $\mathbf{H}_m \in \mathbb{C}^{N\times M(m)}$ is the spatial signature matrix related to array geometry and DOAs of the desired satellite signal m and its corresponding $M(m)$ echoes,
- $\mathbf{b}_m(t) = \begin{bmatrix} a_{m,0} s_m(t-\tau_{m,0}) e^{j2\pi f_{m,0} t} \\ \vdots \\ a_{m,M(m)-1} s_m(t-\tau_{m,M(m)-1}) e^{j2\pi f_{m,M(m)-1} t} \end{bmatrix} \in \mathbb{C}^{M(m)\times 1}$ is the delayed and Doppler–shifted satellite signals envelopes vector, as received in the phase center of the antenna array,

Signal model

- The corresponding vector signal model, where each row corresponds to one antenna:

$$\mathbf{x}(t) = \sum_{m=1}^{M} \mathbf{H}_m \mathbf{b}_m(t) + \mathbf{H}_I \mathbf{i}(t) + \mathbf{n}(t) \ ,$$

where:

- $\mathbf{H}_I \in \mathbb{C}^{N \times M_I}$ is the spatial signature matrix related to array geometry and DOAs of the interferences,
- $\mathbf{i}(t) \in \mathbb{C}^{M_I \times 1}$ are the uncorrelated interferences, as received in the phase center of the antenna array, and
- $\mathbf{n}(t) \in \mathbb{C}^{N \times 1}$ represents additive white Gaussian noise received at each antenna.

Signal model

- The spatial signature matrix $\mathbf{H}$ can be expressed as a function of the scenario geometry and the electrical characteristics of the antenna array:

$$\mathbf{H} = \mathbf{C}\mathbf{G} \ .$$

- Matrix $\mathbf{C} \in \mathbb{C}^{N \times N}$ models RF channels' gain and phase unalignments, as well as cross-coupled terms, which can be measured in a calibration process.
- Matrix $\mathbf{G} \in \mathbb{C}^{N \times M}$ depends on the geometry of the array and on the position of the sources or considered scatterers, and it is uniquely defined for a set of sources emitting from different directions.

Signal model

- Consider a local coordinate system (for example, an east–north–up or $[e, n, u]$ system with origin in a reference point, usually the phase center of the whole array)
- In general, for M sources and N antennas with arbitrary geometry, the time delay of each source caused in each antenna can be computed and expressed in a matrix form

$$\mathbf{G} = e^{j\pi(\mathbf{KR})^\top},$$

where $\mathbf{K} \in \mathbb{R}^{M\times 3}$ is the wavenumber matrix, defined as

$$\mathbf{K} = \begin{pmatrix} \cos(\phi_1)\cos(\theta_1) & \sin(\phi_1)\cos(\phi_1) & \sin(\theta_1) \\ \vdots & \vdots & \vdots \\ \cos(\phi_M)\cos(\theta_M) & \sin(\phi_M)\cos(\phi_M) & \sin(\theta_M) \end{pmatrix},$$

where ϕ_i is the angle of i-th source defined anticlockwise from the e axis on the en plane and θ_i the angle with respect to the en plane.

Signal model

- Consider a local coordinate system (for example, an east–north–up or $[e, n, u]$ system with origin in a reference point, usually the phase center of the whole array)
- In general, for M sources and N antennas with arbitrary geometry, the time delay of each source caused in each antenna can be computed and expressed in a matrix form

$$\mathbf{G} = e^{j\pi(\mathbf{KR})^\top},$$

where the matrix of sensor element positions normalized to units of half wavelengths with respect to the e, n and u axes is

$$\mathbf{R} = \begin{pmatrix} r_{e_1} & \dots & r_{e_N} \\ r_{n_1} & \dots & r_{n_N} \\ r_{u_1} & \dots & r_{u_N} \end{pmatrix} \qquad \in \mathbb{R}^{3\times N}$$

Signal model

Two main modeling assumptions

- Narrowband array assumption:
  - The time required for the signal to propagate along the array is much smaller than the inverse of its bandwidth and, thus, a phase shift can be used to describe the propagation from one antenna to another.
  - For instance, for a navigation signal transmitted with a 20-MHz bandwidth, its inverse is 50 ns, or 15 m in spatial terms. The array is expected to be much smaller, since the carrier's half–wavelength is on the order of 10 cm, so the assumption seems reasonable.
- Narrowband signal assumption:
  - It is assumed that the Doppler effect can be modeled by a frequency shift.
  - Well justified because the bandwidth of the GNSS signals is on the order of few megahertz, and the carrier frequency is between 1 and 2 GHz.

Signal model

- Suppose that K snapshots of the impinging signal are taken with a sampling interval T_s satisfying the Nyquist criterion. Then, the sampled data can be expressed as

$$\mathbf{X}[k] = \sum_{m=1}^{M} \mathbf{H}_m \mathbf{B}_m[k] + \mathbf{H}_I \mathbf{I}[k] + \mathbf{N}[k] \ ,$$

using the following definitions:

- $\mathbf{X}[k] = \begin{pmatrix} \mathbf{x}(t_{k-K+1}) & \cdots & \mathbf{x}(t_k) \end{pmatrix} \in \mathbb{C}^{N\times K}$, referred to as the *spatiotemporal data matrix*, where we used $t_k \equiv k\mathrm{T}_s$,
- $\mathbf{B}_m[k] = \begin{pmatrix} \mathbf{b}_m(t_{k-K+1}) & \cdots & \mathbf{b}_m(t_k) \end{pmatrix} \in \mathbb{C}^{M(m)\times K}$, known as basis function matrices,
- $\mathbf{I}[k] = \begin{pmatrix} \mathbf{i}(t_{k-K+1}) & \cdots & \mathbf{i}(t_k) \end{pmatrix} \in \mathbb{C}^{M_I\times K}$, known as the interference functions matrix, and
- $\mathbf{N}[k] = \begin{pmatrix} \mathbf{n}(t_{k-K+1}) & \cdots & \mathbf{n}(t_k) \end{pmatrix} \in \mathbb{C}^{N\times K}$.

- This is a quite versatile signal model!

Architectures (FRPA vs CRPA)

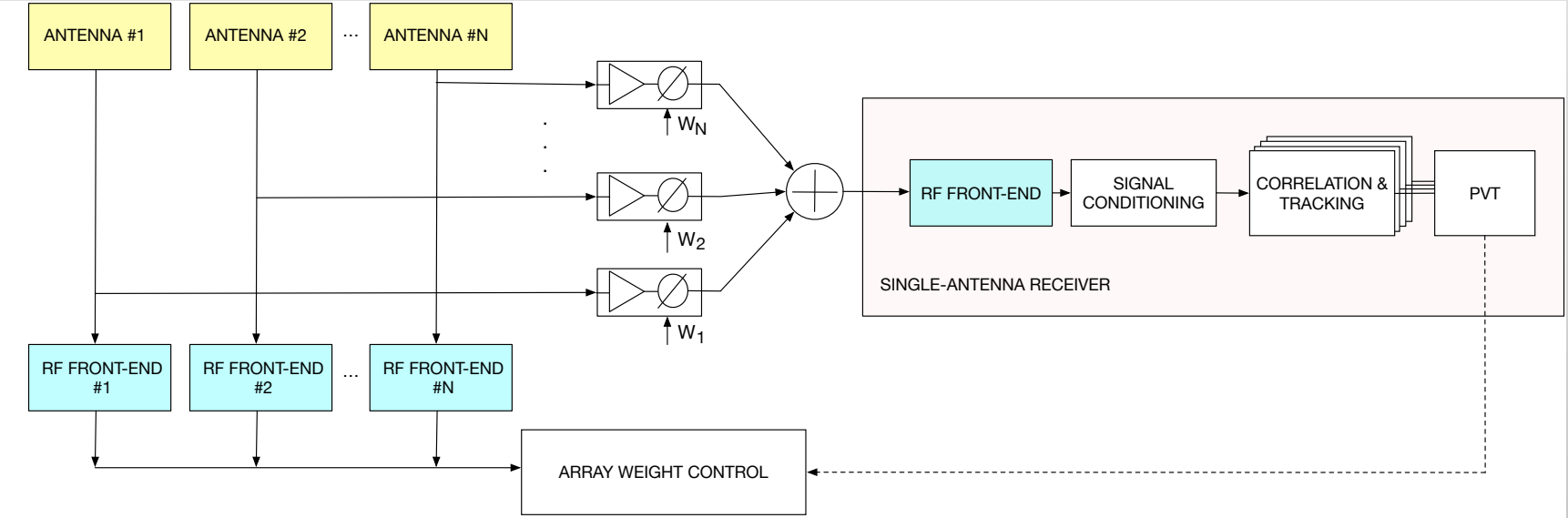
- Fixed reception pattern antenna (FRPA): in single-antenna receivers, FRPA provides
  - a radiation pattern attenuating signals coming from low elevation angles (for instance, a choke-ring antenna)
  - a larger input dynamic range in order to avoid saturation
  - some digital signal processing techniques addressing the presence of those undesired signals, as well as consistency checks.
- Controlled reception pattern antenna (CRPA): in multi-antenna receivers, CRPA provides
  - (adaptive) jamming rejection capabilities.
  - Raytheon's and Novatel's products fall in this category.
- We focus on CRPA in this course.

Architectures (CRPA)

- Controlled reception pattern antenna (CRPA):
  - Several antenna elements whose outputs are controlled in phase and gain, *i.e.*, multiplied by complex weights and combined together in a single output, in order to achieve a gain pattern that can be manipulated electronically.
  - Weights can be stacked in a complex–valued vector $\mathbf{w} \in \mathbb{C}^{N\times 1} = \begin{bmatrix} w_0 & \cdots & w_{N-1} \end{bmatrix}^\top$, and the output signal of a beamformer can be computed as
$$\mathbf{y} = \mathbf{w}^H \mathbf{X}$$
  - Two types of CRPAs are used in GNSS:
    1. Single-output adaptive nulling: sense the presence of an interference and place a null in its DOA, the output is a *cleaned* signal.
    2. Multiple-output beamsteering antennas: adaptive beamforming is used per satellite.

Architectures (Single-output adaptive nulling)

- Single-output adaptive nulling modifies weights at RF level using amplifiers and phase shifters
- Delivers a single, spatially-filtered output
- Plug-and-play into *any* GNSS receiver.



Architectures (Single-output adaptive nulling)

- Beamweights can be predefined or adaptively computed from RF front-tend outputs (e.g., calculated in digital and applied in analogue).
- N degrees of freedom
- $\hat{\mathbf{R}}_{\mathbf{XX}} = \frac{1}{K}\mathbf{X}\mathbf{X}^H$ is an estimation of the autocorrelation matrix of the received snapshots

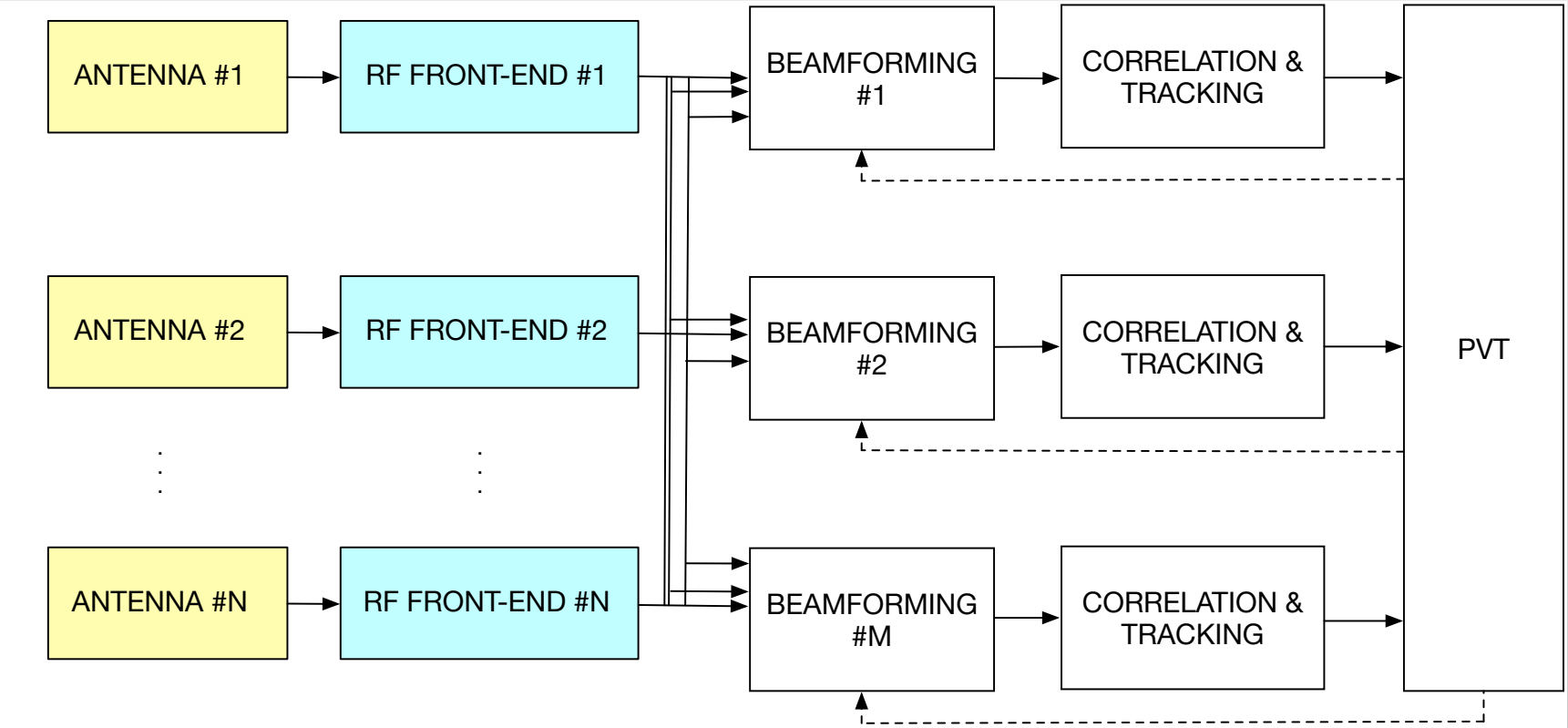
Name	Criterion	Optimum beamweight	Requires	Refs.
Power minimization	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\|\mathbf{w}^H\mathbf{X}\right\|^2\right\}$ subject to $\mathbf{w}^H\delta_0 = 1, \quad \delta_0 = [1,0,...,0]^\top$	$\hat{\mathbf{w}}_{\text{PMIN}} = \frac{\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\delta_0}{\delta_0^\top\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\delta_0}$	$\mathbf{X}$	[30], [62] [63]–[65]
Multiple-Constrained Minimum Variance	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\|\mathbf{w}^H\mathbf{X}\right\|^2\right\}$ subject to $\mathbf{w}^H\mathbf{h}_m = 1, \quad m = 1,...,M$	$\hat{\mathbf{w}}_{\text{MCMV}} = \frac{\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{H}}_{\text{LOS}}}{\hat{\mathbf{H}}_{\text{LOS}}^H\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{H}}_{\text{LOS}}}\mathbf{1}_{M\times 1}$	$\mathbf{X}$, $\hat{\mathbf{H}}_{\text{LOS}}$	[26], [55], [66]
Minimum Mean Square Error	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\|\mathbf{w}^H\mathbf{X} - \mathbf{a}^\top\mathbf{D}_{\text{LOS}}\right\|^2\right\}$	$\hat{\mathbf{w}}_{\text{MMSE}} = \hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{R}}_{\mathbf{X}\mathbf{D}_{\text{LOS}}}\hat{\mathbf{a}}^*$	$\mathbf{X}$, $\hat{\mathbf{a}}$, $\mathbf{D}_{\text{LOS}}(\hat{\tau}, \hat{\mathbf{f}}_d)$	[27], [67]

Architectures (Multiple-output beamsteering antennas)

- Instead of conforming nulls to reject interfering signals, the so-called multiple-output adaptive beamformers produce M independent beams, each one devoted to a given satellite and providing its corresponding output.
- Digital beamforming is a linear operation, so they can be implemented in
  - Pre-correlation:
    - desired signal is below noise (interference detection/mitigation),
    - high data rate for $\mathbf{w}$ calculation and spatial filtering,
    - operates before tracking loops.
  - Post-correlation:
    - desired signal is above noise (multipath detection/mitigation),
    - lower data rate for $\mathbf{w}$ calculation and spatial filtering,
    - operates after, or in parallel to, tracking loops.

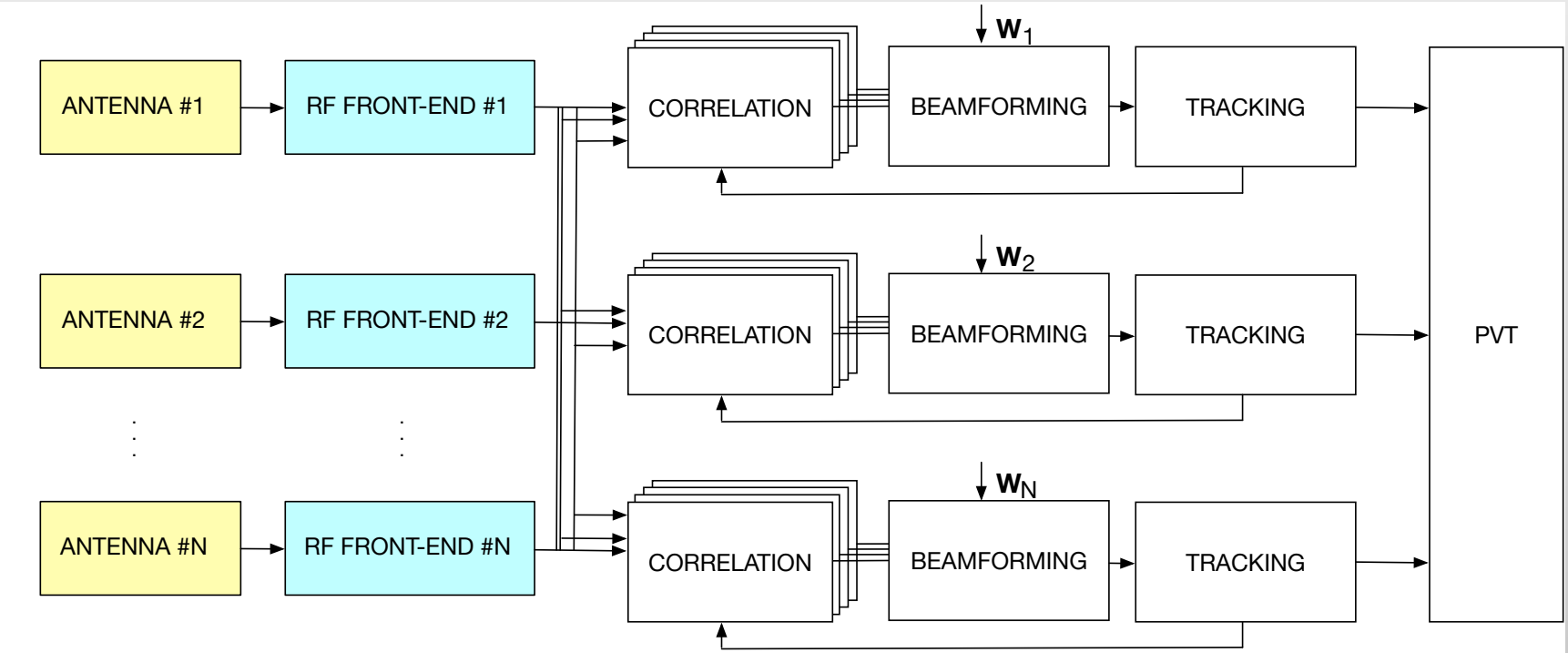
Architectures (Multiple-output beamsteering antennas)

- Pre-correlation



Architectures (Multiple-output beamsteering antennas)

- Post-correlation



Architectures (Multiple-output beamsteering antennas)

- The beamvector $\mathbf{w}$ can be designed following
  - time reference beamformers relying on *a priori* knowledge of a reference waveform, and
  - spatial reference beamformers relying on *a priori* knowledge of the spatial signature of the desired DOA.
- $\mathbf{w}_m$ refers to the beamweight of the m-th beamformer, $\hat{\mathbf{r}}_{\mathbf{xd}_m} = \frac{1}{K}\mathbf{X}\mathbf{d}_m^H$ is an estimation of the steering vector, and $\mathcal{P}\{\cdot\}$ is the operator that yields the principal eigenvector of a matrix.

Name	Criterion	Optimum beamweight	Requires	Refs.
Phased Array	$\mathbf{w}^H\mathbf{h}_m = 1$	$\hat{\mathbf{w}}_{\text{PAB}_m} = \hat{\mathbf{h}}_m\left(\hat{\mathbf{h}}_m^H\hat{\mathbf{h}}_m\right)^{-1}$	$\hat{\mathbf{h}}_m$	[82]–[84]
Linearly Constrained Minimum Variance	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\lvert\mathbf{w}^H\mathbf{X}\right\rvert^2\right\}$ subject to $\mathbf{w}^H\mathbf{h}_m = 1$	$\hat{\mathbf{w}}_{\text{MVB}_m} = \frac{\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{h}}_m^H}{\hat{\mathbf{h}}_m\hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{h}}_m^H}$	$\mathbf{X}$, $\hat{\mathbf{h}}_m$	[74], [85]
Temporal Reference Beamformer	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\lvert\mathbf{w}^H\mathbf{X} - a_{m,0}\mathbf{d}_m\right\rvert^2\right\}$	$\hat{\mathbf{w}}_{\text{TRB}_m} = \hat{\mathbf{R}}_{\mathbf{XX}}^{-1}\hat{\mathbf{r}}_{\mathbf{xd}_m}\hat{a}_{m,0}^*$	$\mathbf{X}$, $\hat{a}_{m,0}$ $\mathbf{d}_m\left(\hat{\tau}_{m,0}, \hat{f}_{d_{m,0}}\right)$	[86]
Hybrid Beamformer	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\lvert\mathbf{w}^H\mathbf{X} - a_{m,0}\mathbf{d}_m\right\rvert^2\right\}$ subject to $\mathbf{w}^H\mathbf{h}_m = 1$	$\hat{\mathbf{w}}_{\text{HB}_m} = \hat{\mathbf{w}}_{\text{TRB}_m} + \hat{\mathbf{w}}_{\text{MVB}_m}\left(1 - \hat{\mathbf{h}}_m^H\hat{\mathbf{w}}_{\text{TRB}_m}\right)$	$\mathbf{X}$, $\hat{\mathbf{h}}_m$, $\hat{a}_{m,0}$ $\mathbf{d}_m\left(\hat{\tau}_{m,0}, \hat{f}_{m,0}\right)$,	[31]
Eigenbeamforming	$\arg\min_{\mathbf{w}} \mathbb{E}\left\{\left\lvert\mathbf{w}^H\left(\mathbf{X} - \mathbf{h}_m^H a_{m,0}\mathbf{d}_m\right)\right\rvert^2\right\}$	$\hat{\mathbf{w}}_{\text{EIG}_m} = \mathcal{P}\left\{\frac{\lvert\hat{a}_{m,0}\rvert^2\hat{\mathbf{h}}_m^H\hat{\mathbf{h}}_m + \hat{\sigma}_n^2\mathbf{I}_{N\times N}}{\hat{\mathbf{R}}_{\mathbf{XX}} - \lvert\hat{a}_{m,0}\rvert^2\hat{\mathbf{h}}_m^H\hat{\mathbf{h}}_m}\right\}$	$\mathbf{X}$, $\hat{\mathbf{h}}_m$, $\lvert\hat{a}_{m,0}\rvert^2$, $\hat{\sigma}_n^2$	[87]

Implementation aspects

- Antenna phase center
  - GNSS measurements are referred to the so-called antenna phase center (APC).
  - Practical antenna implementations exhibit an irregular equiphase contour.
  - Causing the APC to depend on the DOA and signal frequency, with variations on the order of few millimiters.
  - Since the adaptive beamforming will dynamically change the array pattern, it has the potential to introduce phase center biases into the antenna array.
  - For applications demanding high accuracy, those phase biases must be mitigated or compensated because they will bring errors in the code and carrier phase measurements
- Calibration
- Adaptive schemes

Implementation aspects

- Antenna phase center
- Calibration
  - Calibration of the antenna array implies the measurement of matrix $\mathbf{C}$ and its compensation procedure.
  - Final objective to have the signature vectors $\mathbf{h}$ only parameterized by sources' azimuth and elevation.
  - Measurements are usually performed in anechoic chambers with high degree of automatization.
  - Phase compensations are performed in the digital domain with methods ranging from look-up tables to advanced adaptive algorithms acting as a pre-processor of the beamformer.
- Adaptive schemes

Implementation aspects

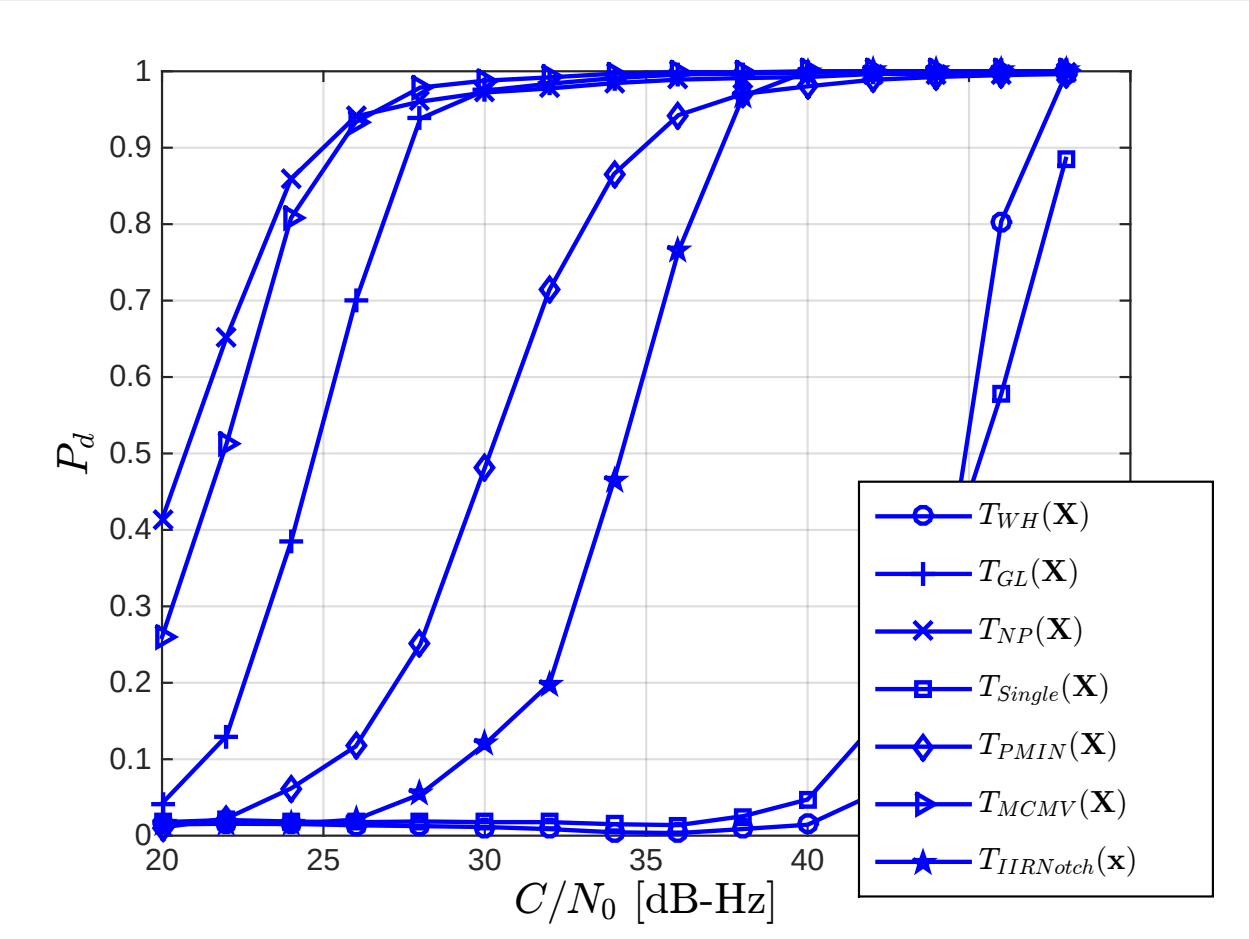
- Antenna phase center
- Calibration
- Adaptive schemes
  - Adaptive nullers and beamformers require online calculation of the covariance matrix inverse, $\hat{\mathbf{R}}_{\mathbf{XX}}$.
  - This operation is computationally expensive because obtaining $\mathbf{X}[k]\mathbf{X}[k]^H$ is $\mathcal{O}(N^2K)$ (where $K \geq \alpha \cdot 1023$, with $\alpha = 2$ in the simplest GPS L1 C/A case to $\alpha = 90$ for the wideband Galileo E5 signal), and its inverse is $\mathcal{O}(N^3)$.
  - This can be alleviated using QR decomposition-based recursive least squares algorithm, which allows the recursive computation of $(\mathbf{X}[k]\mathbf{X}[k]^H)^{-1}$ from $(\mathbf{X}[k-1]\mathbf{X}[k-1]^H)^{-1}$, being $\mathcal{O}(N^2)$.

Jamming rejection capabilities (Acquisition)

- Galileo E1B and E1C Open Service signals were synthetically generated.
- Circular, $N = 8$ omnidirectional element antenna array, $\lambda/2$.
- Acquisition time set to one PRN primary code period ($T_{acq} = 4$ ms, $K = 24000$ snapshots), and
- probability of false alarm P_{fa} was set to 0.001 for all the algorithms in order to set the particular detection threshold values.
- Tested methods:
  - $T_{\text{GL}}(\mathbf{X})$, array GLRT acquisition test,
  - $T_{\text{WH}}(\mathbf{X})$, array GLRT acquisition test assuming white noise,
  - $T_{\text{NP}}(\mathbf{X})$, Neymann-Pearson clairvoyant detector, provided as a reference performance bound,
  - $T_{\text{PMIN}}(\mathbf{X})$, power minimization plus conventional acquisition,
  - $T_{\text{MCMV}}(\mathbf{X})$, the minimum variance nuller that uses DOA estimations,
  - $T_{\text{IIRNotch}}(\mathbf{X})$, single-antenna acquisition plus notch filtering, and
  - $T_{\text{Single}}(\mathbf{X})$, single-antenna acquisition.

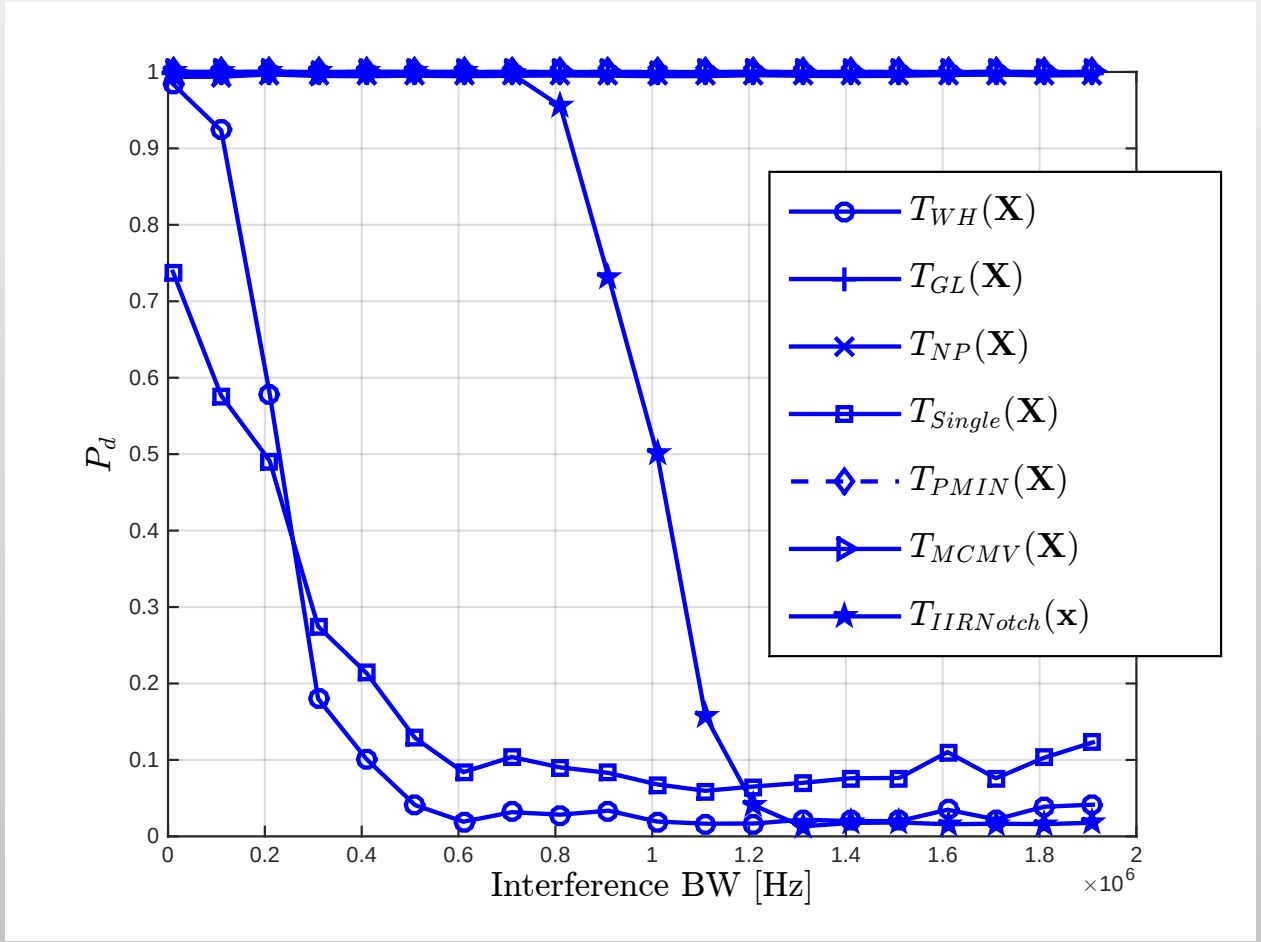
Jamming rejection capabilities (Acquisition)

- Jammer: Gaussian noise-like in-band, bandwidth of 500 kHz, and $C_I/N_0 = 80$ dB-Hz



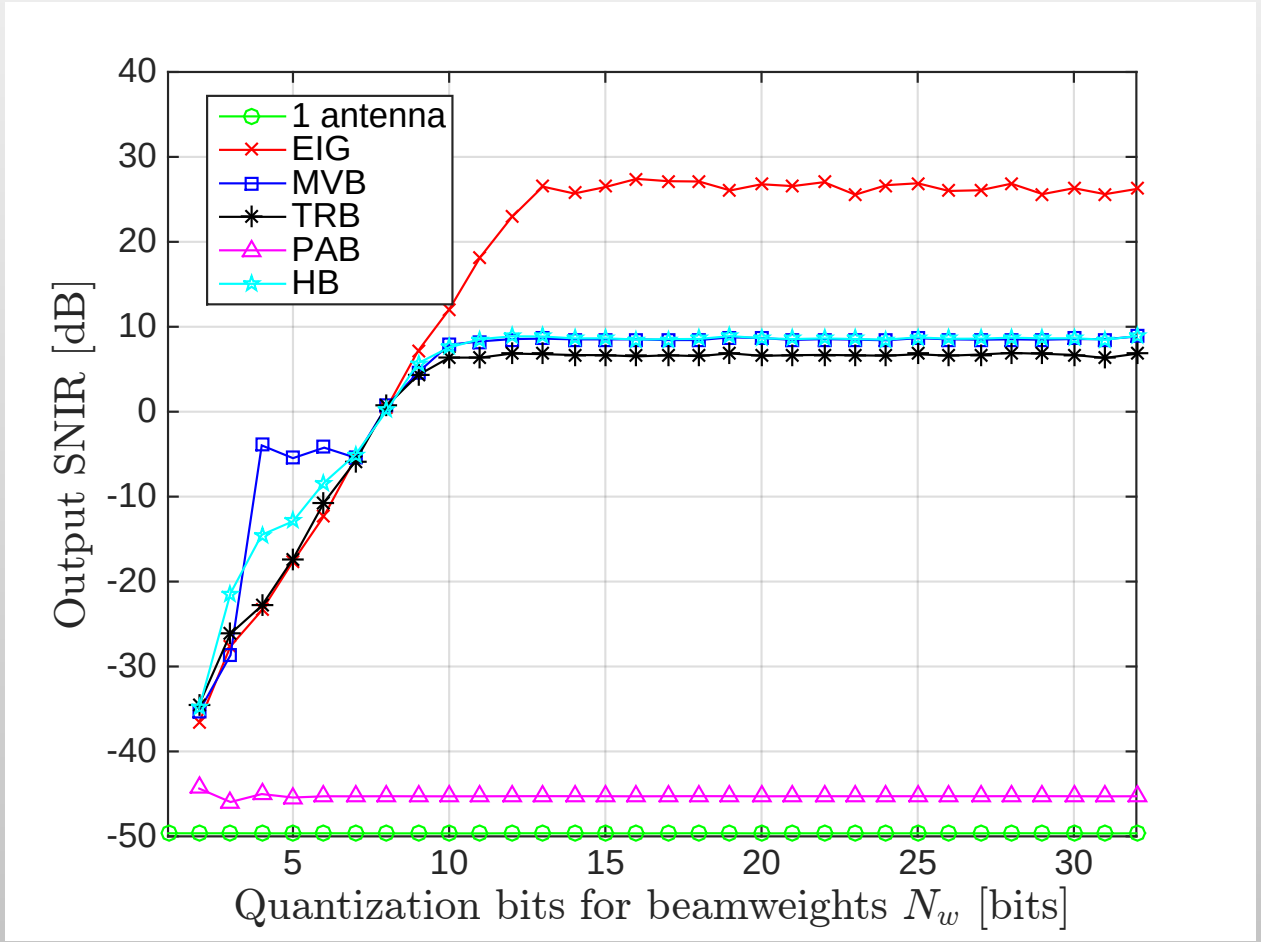
Jamming rejection capabilities (Acquisition)

- Jammer: Gaussian noise-like in-band, and $C_I/N_0 = 80$ dB-Hz
- Signal: $C/N_0 = 42$ dB-Hz



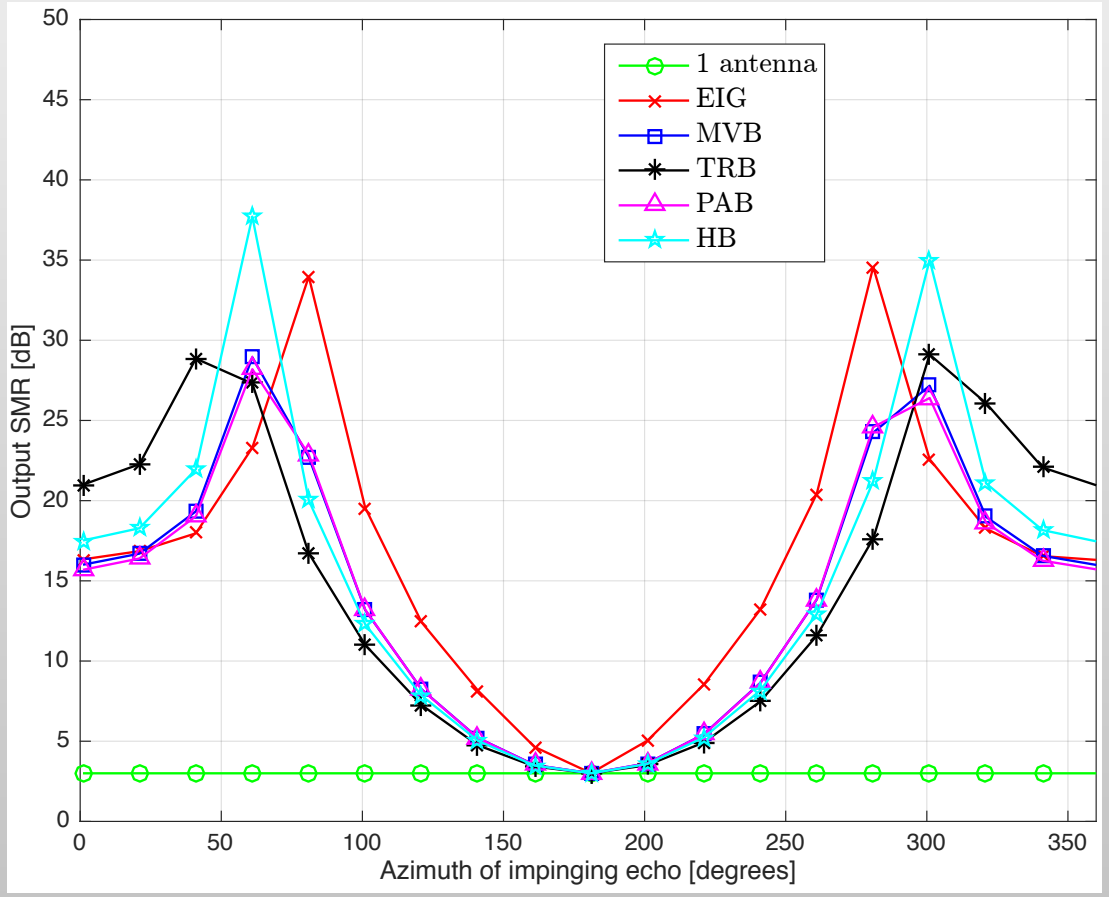
Jamming rejection capabilities (Tracking)

- Impact of beamweight quantization.
- In-band CW jammer, $C_I/N_0 = 80$ dB-Hz and $C/N_0 = 35$ dB-Hz



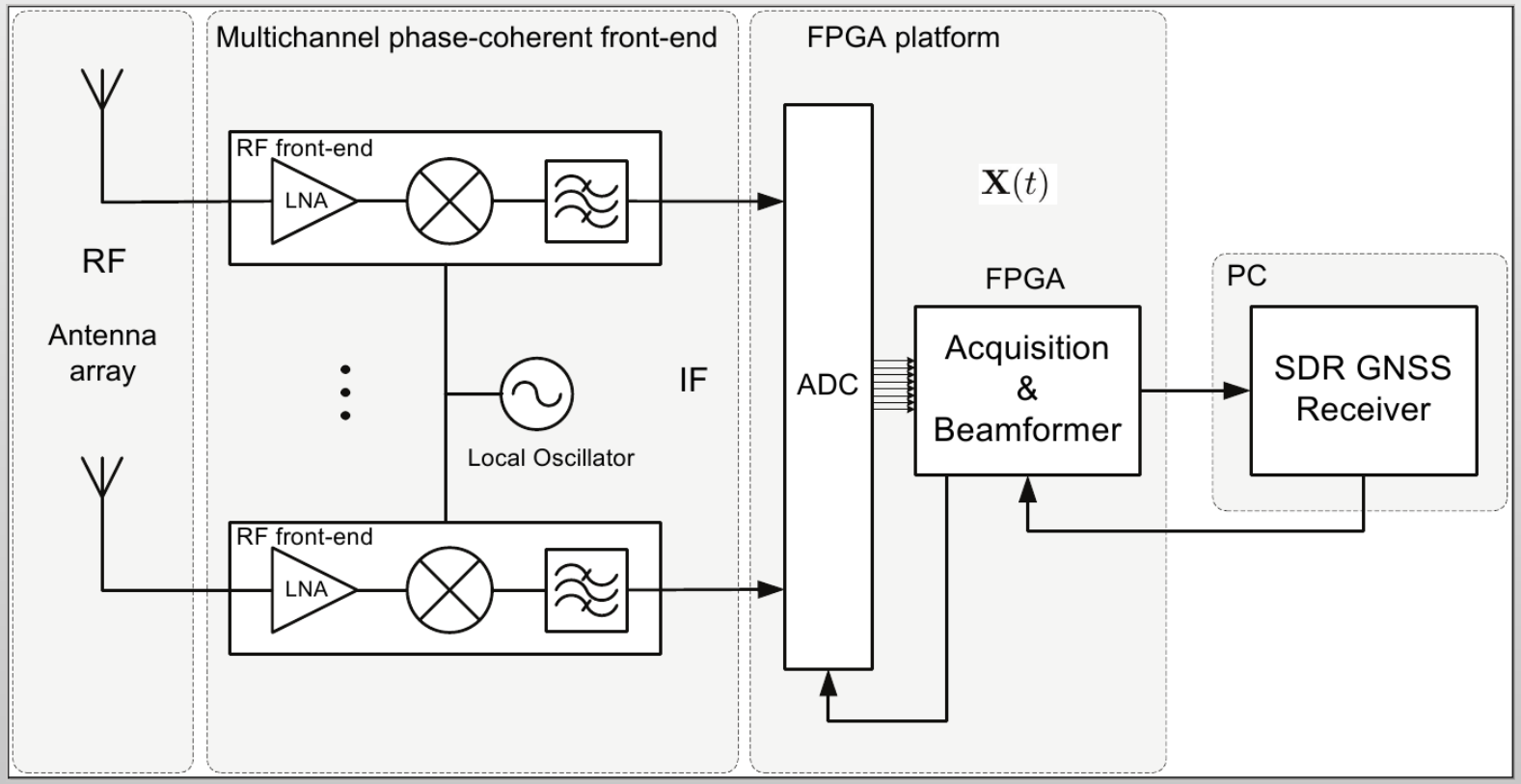
Jamming rejection capabilities (Tracking)

- Effect of a close echo: 0.25 chips, 45^o elevation, 180^o azimuth, and signal-to-multipath ratio of 3 dB
- $C/N_0 = 35$ dB-Hz



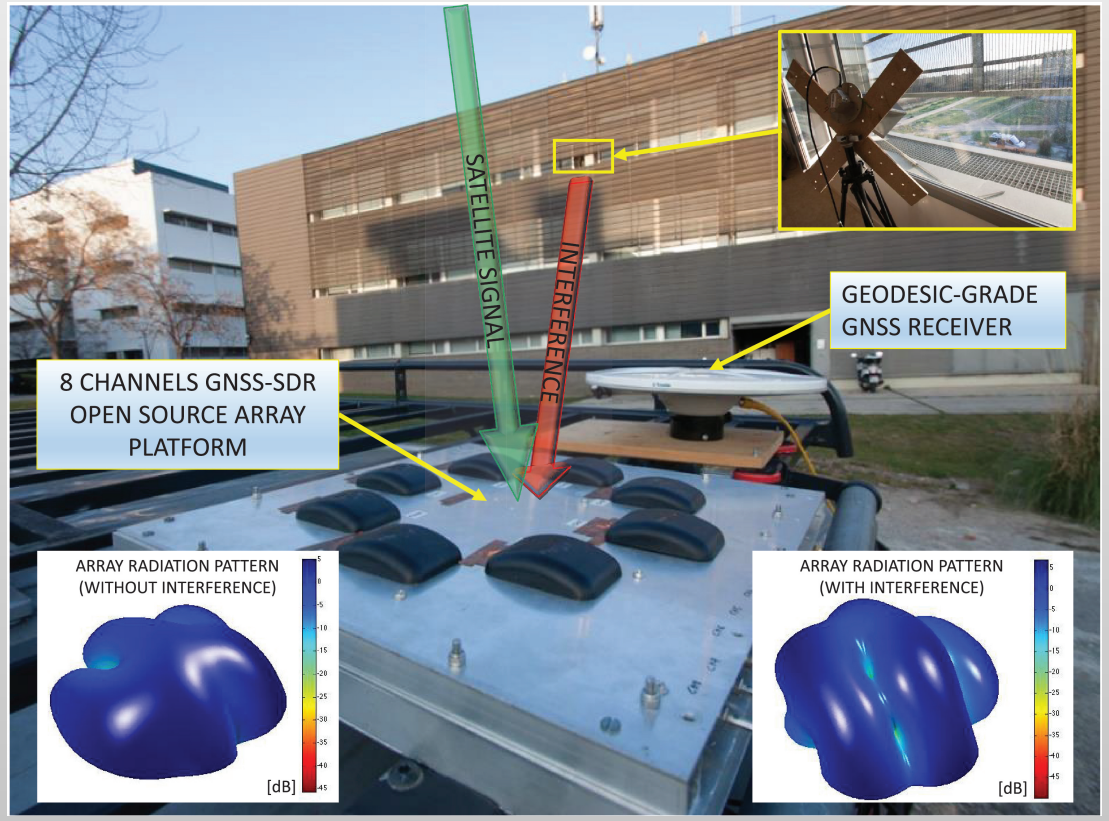
Jamming rejection capabilities (Experimental setup)

- 8-element array prototype
- Plugged to the GNSS-SDR open-source receiver (gnss-sdr.org)



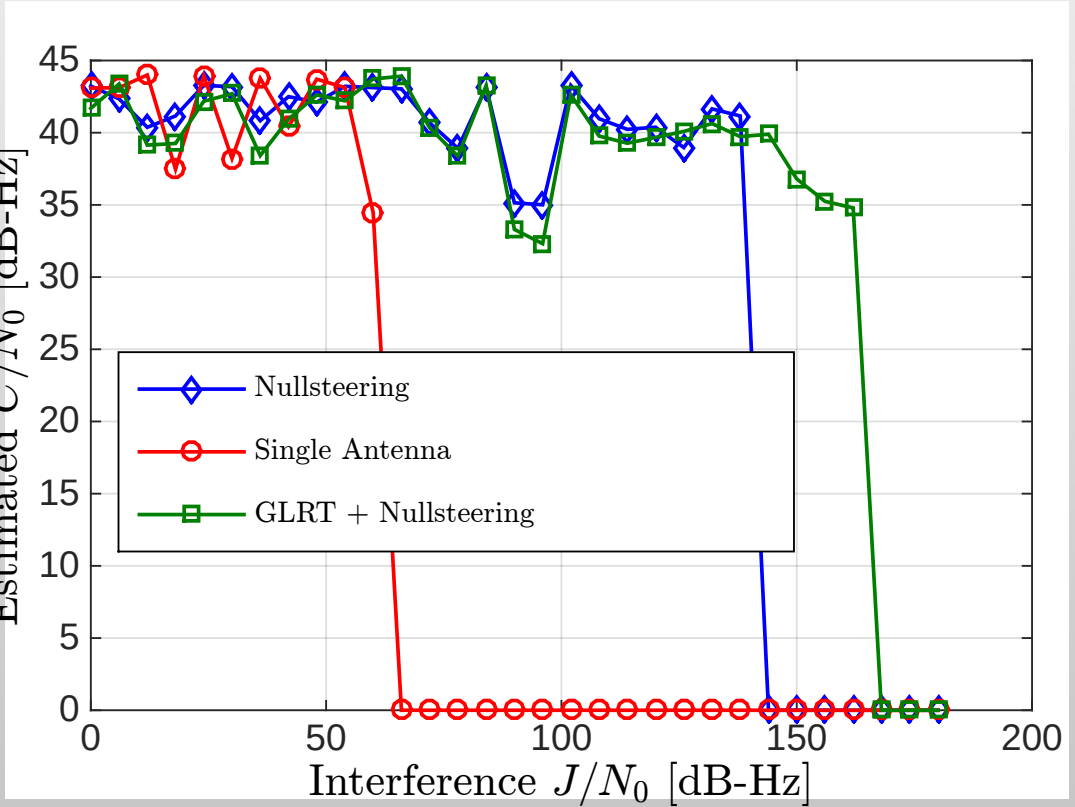
Jamming rejection capabilities (Experimental setup)

- 8-element array prototype
- Plugged to the GNSS-SDR open-source receiver (gnss-sdr.org)



Jamming rejection capabilities (Experimental setup)

- 8-element array prototype
- Plugged to the GNSS-SDR open-source receiver (gnss-sdr.org)



Summary (so far, V)

- Multi-antenna receivers allow for additional robustness to interferences.
- Attenuate or amplify certain directions-of-arrival (DOA) through fixed (FRPA) or adaptive (CRPA) schemes.
- Array processing involves sophisticated techniques and high prototyping complexity (w.r.t. single-antenna)
- Several CRPA architectures are possible
  - Single-output adaptive nulling
  - Multiple-output beamsteering antennae (pre-correlation).
  - Multiple-output beamsteering antennae (post-correlation).
- A number of beamweight design criteria were reviewed and discussed.

[Fer16] C. Fernàndez-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: theory and implementation," in Proceedings of the IEEE, vol 104, no 6, pp 1207–1220, June 2016.

Outline

Take home message...

- GNSS is a tremendously important technology.
- A large number of services and (critical) infrastructures leverage on its use (positioning or timing)
- It is important to secure GNSS service against intentional or unintentional interferences, since consequences of GNSS disruption would be catastrophic.
- In this course we had an overview of
  - Interference types, characteristics, and mathematical models.
  - Interference impact on a generic GNSS receiver chain.
  - Countermeasures for detection and mitigation, both for single- and multi-antennae receivers.
- Notice this is an overview, so many methods/approaches/ideas were excluded.
- Check/read/research yourself!

Bibliography

- M. Amin, P. Closas, A. Broumandan, J. Volakis (Eds.), "*Scanning the Issue: Vulnerabilities, Threats, and Authentication of Satellite-Based Navigation Systems*", in Proceedings of the IEEE, vol 104, no 6, pp 1169–1173, June 2016.
- R. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of GNSS, status and potential mitigation techniques," in Proceedings of the IEEE, vol 104, no 6, pp 1174–1194, June 2016.
- D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," in Proceedings of the IEEE, vol 104, no 6, pp 1233–1245, June 2016.
- M. Psiaki and T. Humphreys, "GNSS spoofing and detection," in Proceedings of the IEEE, vol 104, no 6, pp 1258–2170, June 2016.
- J. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding Aspects of Secure GNSS Receivers," in Proceedings of the IEEE, vol 104, no 6, pp 1271–1287, June 2016.
- C. Fernàndez-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: theory and implementation," in Proceedings of the IEEE, vol 104, no 6, pp 1207–1220, June 2016.
- A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," in Proceedings of the IEEE, vol 104, no 6, pp 1246–1257, June 2016.

Bibliography

Robust Interference Mitigation:

- Borio, D., Closas, P. (2017). A fresh look at GNSS anti-jamming. Inside GNSS, 12, 54-61.
- Borio, D. (2017). Myriad non-linearity for GNSS robust signal processing. IET Radar, Sonar and Navigation, 11(10), 1467-1476.
- Borio, D., Closas, P. (2018). Complex signum non-linearity for robust GNSS signal processing. IET Radar Sonar and Navigation, 12(8) 900-909.
- Borio, D., Li, H., Closas, P. (2018). Huber's non-linearity for GNSS interference mitigation. Sensors, 18(7), 2217.
- Borio, D., Closas, P. Robust transform domain signal processing for GNSS. NAVIGATION. 2019; 66: 305-323.
- H. Li, D. Borio, P. Closas, "Dual-Domain Robust GNSS Interference Mitigation," in Proc. of the ION GNSS+ 2019, 16-20 September 2019, Miami, FL.

Robust Global Navigation Satellite Systems

Focus on anti-jamming

Pau Closas

Assistant Professor
Northeastern University
Department of Electrical and Computer Engineering
Boston, Massachusetts (USA)

closas@northeastern.edu
http://www.ece.neu.edu/people/closas-pau

Northeastern University

Robust GNSS Day @ TéSA, 10 July 2019