

Security aspects of Global Navigation Satellite Systems (GNSS)



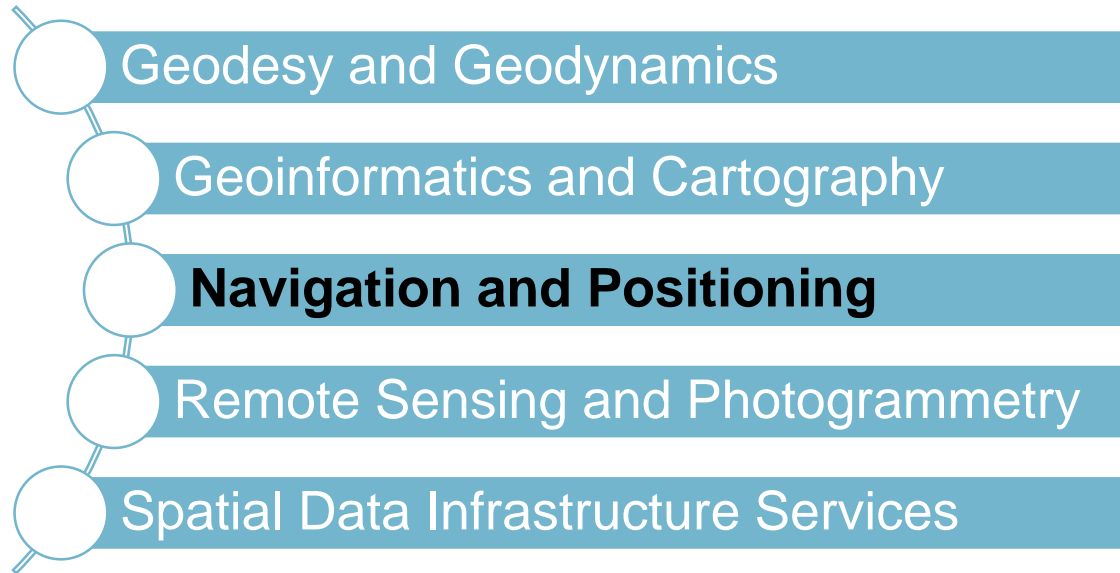


Nicola Linty,
PhD, associate professor



Navigation and Positioning Department (NAVI)
Finnish Geospatial Research Institute (FGI), National Land Survey of Finland (NLS)

FGI IS PART OF THE NATIONAL LAND SURVEY (MAANMITTAUSLAITOS)



DEPARTMENT OF NAVIGATION AND POSITIONING

Current staff: 25, with 9 PhDs
9 nationalities

Two research groups:

[Satellite and Radio Navigation](#) (**SaRaNa**)

[Sensors and Indoor Navigation](#) (**SINa**)

A navigation laboratory with state-of-the-art equipment (signal simulators, roof antennas, repeaters, receivers and sensors)



CC BY-NC



school - Jun 2015



RESEARCH FOCUS AREAS

Seamless/Hybrid Navigation

Robust GNSS Technologies

Arctic Navigation Challenges

Optical Sensing

Galileo PRS

Collaborative Navigation

Low-Cost Precise GNSS Positioning

(E)GNSS Based Timing

Privacy of Geospatial Data

Situational/Context Awareness

Maritime Safety



Introduction and Motivations

MOTIVATIONS

Brad Parkinson once remarked that GPS represents, next to the Internet, the **most successful** civilian adoption of military-developed, dual-use technology.

GNSS is becoming quite common in several **civil application fields** (mobility, agriculture, ICT).

The development of the **Galileo** system is one of the major technological project in Europe.

Location based services are one of the most important added value of future personal communication systems.

however

As GNSS-enabled applications become **increasingly woven** into the fabric of our global economic and social infrastructure, consequences of **breach-of-service** become greater.

As a resource becomes more valuable to our civil infrastructure, criminal or **malicious agents** will seek to discover and exploit weaknesses in order to disrupt legitimate users or to perpetrate fraud.

Blooming market

Risks!

SECURITY FOR/FROM NAVIGATION

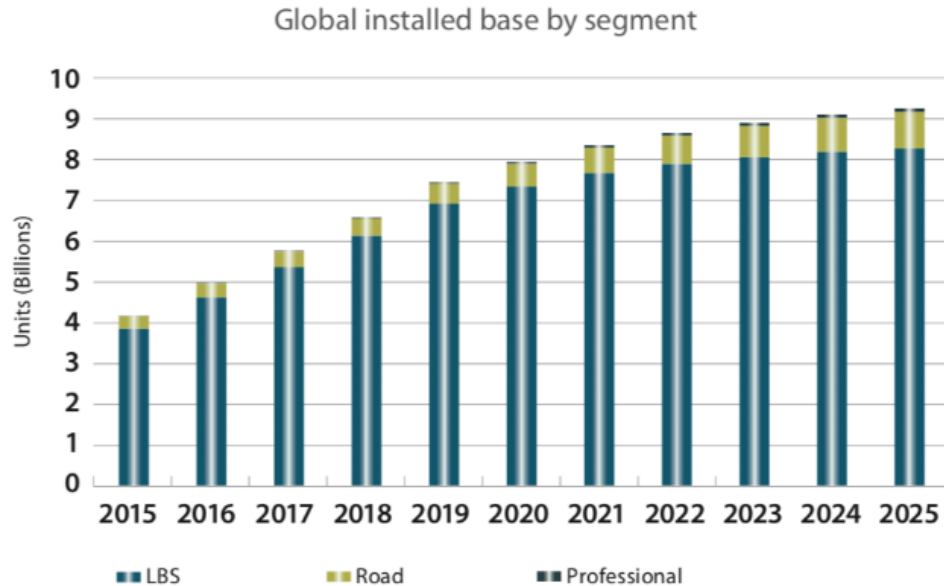
Navigation system security is ever more important for two reasons.

- 1) To ensure that the position, navigation, and time (PNT) information upon which we increasingly rely are indeed trustworthy.
- 2) Secure PNT can serve as a building block for protection of critical data and assets in the global fight against information technology attack.

FOR

FROM

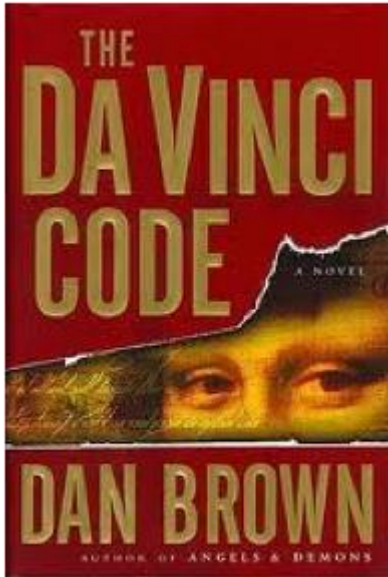
MOTIVATIONS



First dual-frequency GNSS smartphone fitted with a Broadcom BCM47755 chip, **May 31, 2018** world's first smartphone providing up to decimetre-level accuracy for mass-market apps



WHAT PEOPLE BELIEVE ABOUT GPS...

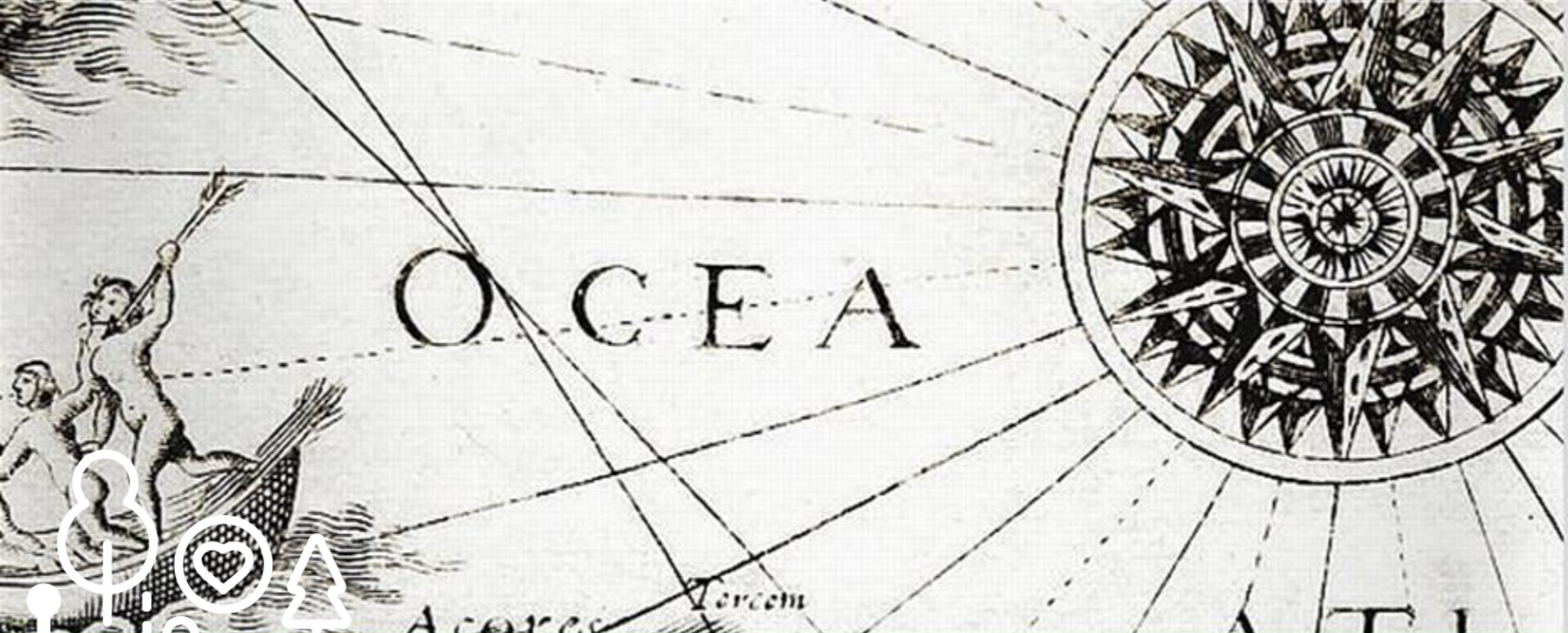


Pinching the tiny object between his fingers, Langdon pulled it out and stared in astonishment. It was a metallic, button-shaped disk, about the size of a watch battery. He had never seen it before. "What the...?"

"GPS tracking dot," Sophie said. "Continuously transmits its location to a Global Positioning System satellite that DCPJ can monitor. We use them to monitor people's locations. It's accurate within two feet anywhere on the globe. They have you on an electronic leash."

WHAT GPS CAN'T DO

- GPS doesn't know your position: that's why your receiver is for
- GPS doesn't know you live on a one-way street
- GPS has no clue about how to reach a place
- GPS can't track you
- GPS can't be used everywhere



Navigation and GNSS



THE NAVIGATION PROBLEM

The problem of knowing the position with respect to some **reference frame** or a map

The early navigators and mapmakers relied on **celestial observations** to determine both **time** and position on Earth

The science of **timekeeping** and the advent of clocks allowed for an improvement of navigation (especially at open sea)



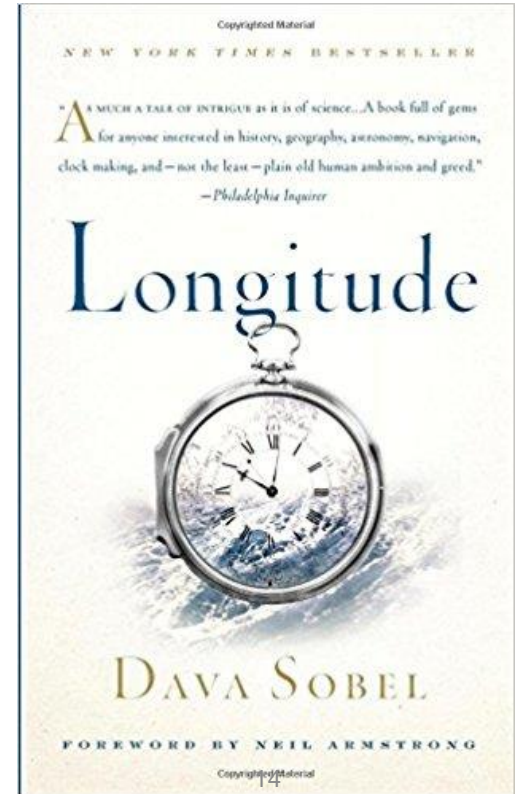
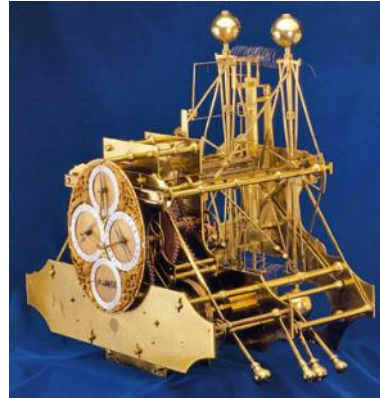
THE LONGITUDE ACT

“...nothing is so much wanted and desired at sea, as the discovery of the longitude, for the safety and quickness of voyages, the preservation of ships, and the lives of men...”

British government, 1714

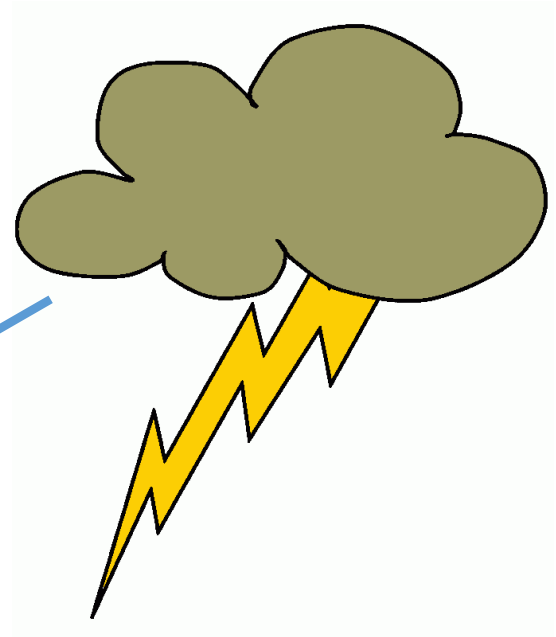
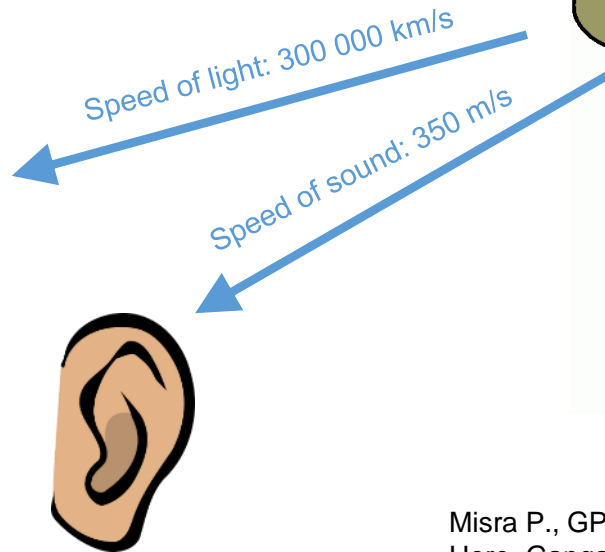
£20,000 for a solution which could find longitude to within half a degree (equivalent to 2 minutes of time)

John Harrison, 1737



BASIC IDEA

When you see a flash of lightning, you start counting *until* you hear the thunder



Misra P., GPS for Everyone: You are Here, Ganga-Jamuna press

WHERE DID THE LIGHTNING STRIKE?



RADIONAVIGATION PRINCIPLES

Determination of position and speed of a user by means of the **estimation** of parameters of an electromagnetic signal

- Propagation time

- Phase

- Received Signal Strength

- ...

Such parameters are converted to estimated **distances** with respect to reference points the position of which is known

Trilateration: the position is obtained by the intersection of geometrical loci, named Line of Positions

SPHERICAL SYSTEMS

The receiver evaluates a parameter of the signal incoming from the sources whose value is proportional to the distance

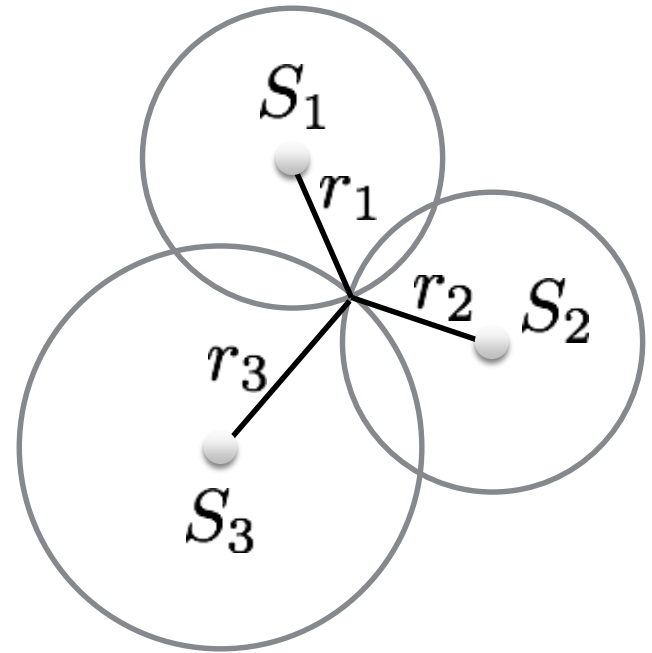
time of arrival (TOA): the signals must be timestamped with the transmission time

received signal strength (RSS)

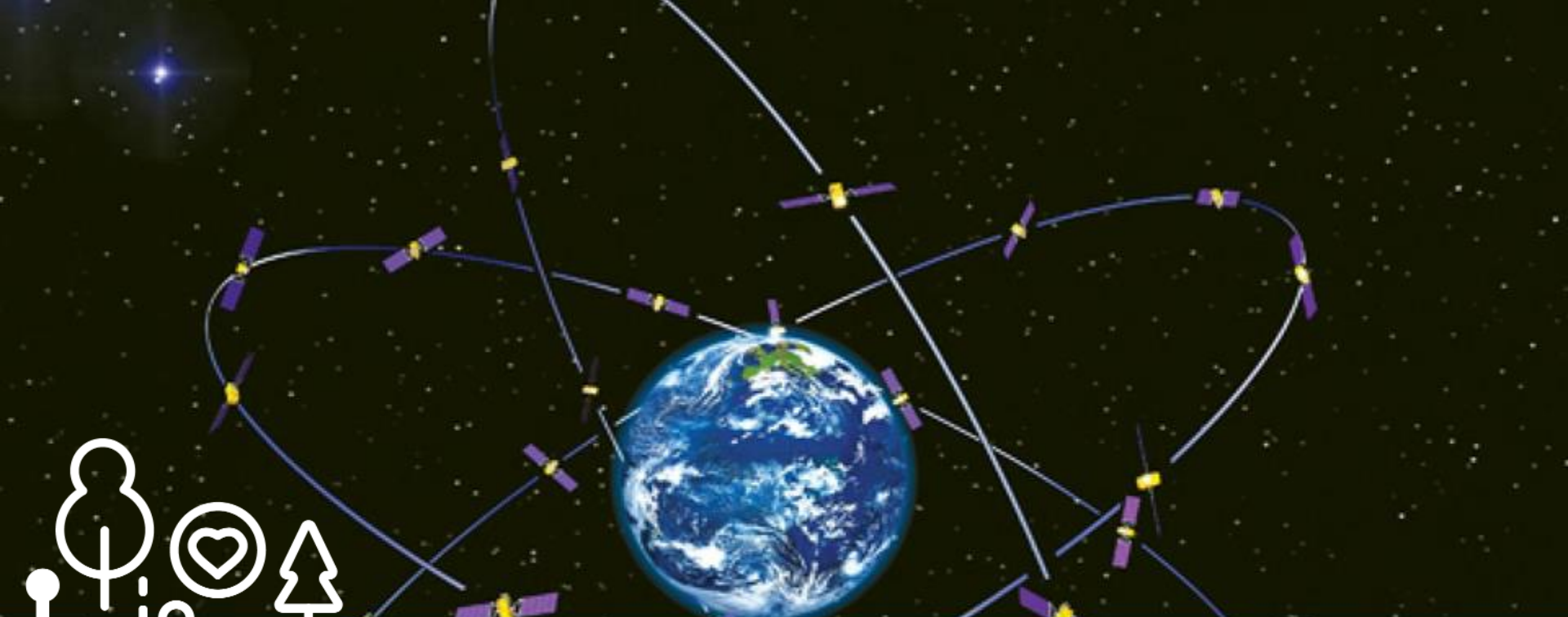
The sources are the center of the **spheres** and the distance the radius

The position must be inferred by the intersection of at least three spheres

Example: GNSS



F. Dovis, "Interference and spoofing", lecture notes, NavSAS, Politecnico di Torino



SATELLITE NAVIGATION SYSTEMS

GLOBAL NAVIGATION SATELLITE SYSTEMS

Global Navigation Satellite Systems (GNSS) provide signals from a **constellation of satellites**

By processing the signal received, the user get an estimate of their position in a reference frame

They aim at providing an almost **global coverage** on the Earth surface

All the transmitters (satellites) are synchronous

Primary goal is to provide signal for positioning but in the last few years GNSS signals started to be exploited also for other purposes



GNSS OR GPS?

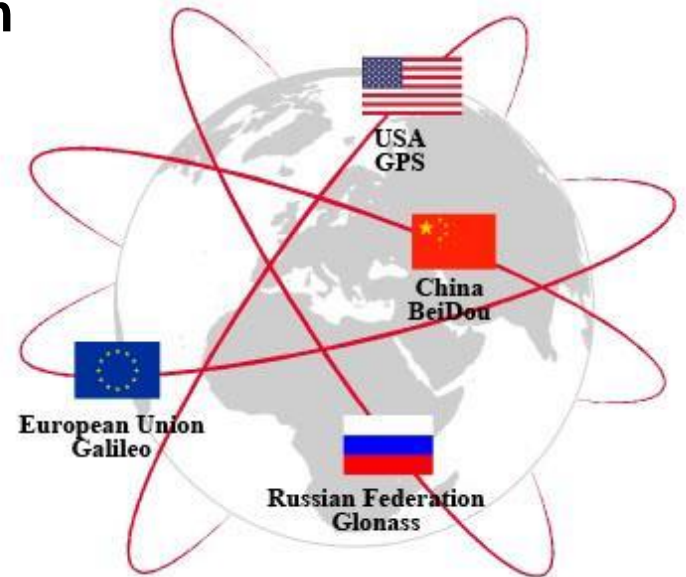
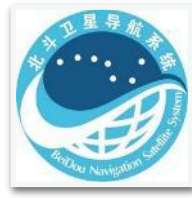
GNSS: Global Navigation Satellite System

GPS: Global Positioning System

GLONASS, ГЛОНАСС: ГЛОбальная НАвигационная Спутниковая Система

Galileo

Beidou, 北斗 (*star of the north*)



COMMON FEATURES

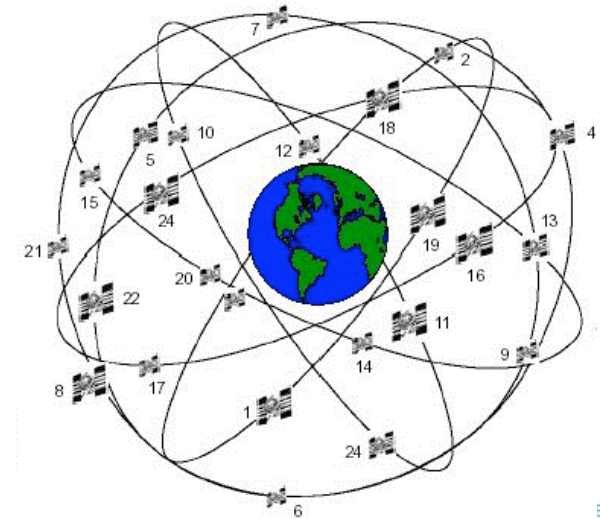
- Radio-frequency **electromagnetic signal**
- Operate in the **L-Band**, a portion of the radio spectrum between 1 and 2 GHz.
- Trilateration
- **One-way** broadcast
- Unlimited number of users
- **Free of charge** (basic service)
- Satellites have very precise and synchronized atomic **clocks**

GPS: Global Positioning System

GPS was invented from the need for an independent military navigation system..

Owned and operated by the U.S. Government through the U.S. Air Force and the Department of Defense (DoD)

It's the oldest GNSS system



HOW MUCH DOES GPS COST?

\$ 20 billions in design, development, test and deployment spread over 22 years (1973 – 1995)

\$ 1 billion each year to operated and maintain

Who pays for GPS?

If you are American, you pay it with your taxes

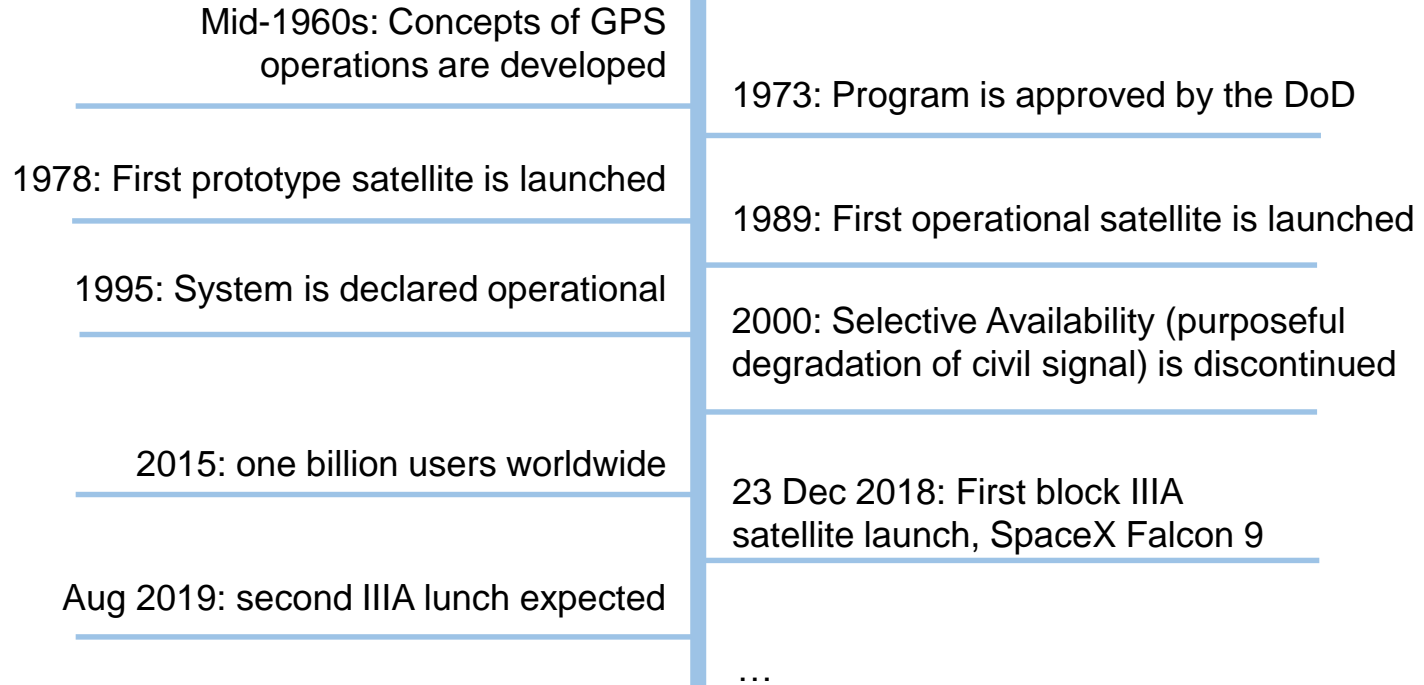
If you are not, you got it for free

Access to civilian GPS signals is free of direct user charges

Economic value of GPS:

about \$ 100 billion a year

GPS TIMELINE





https://youtu.be/yRiLPoy_Mzc

Program is approved by the DoD

First operational satellite is launched

Selective Availability (purposeful
degradation of civil signal) is discontinued

2018: First block IIIA
satellite launch, SpaceX Falcon 9

July 25, 2019: second IIIA launch expected

...

GPS PRESENT CONSTELLATION

Block I: concept validation satellites

Block II: operational satellites

Block IIA: second generation operational satellites

Block IIR: replenishment satellites

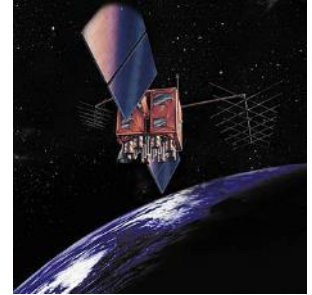
Block IIR-M: new civil signal (L2C) and a new military signal on L1 and L2

Block IIF: satellites transmit all signals including on the L5 frequency

Block IIIA: new signals, higher power levels

Block IIIF: from 2025 to 2034

Global GPS civil service performance commitment
has been met continuously **since December 2003**



GPS MODERNIZATION

Process began in 1998, three years after declaration of operativity.

New signals, more robust:

- Innovative M-Code for military applications

- Second Civil Signal: L2C

- Third Civil Signal: L5

- Fourth Civil Signal: L1C (TMBOC modulation)



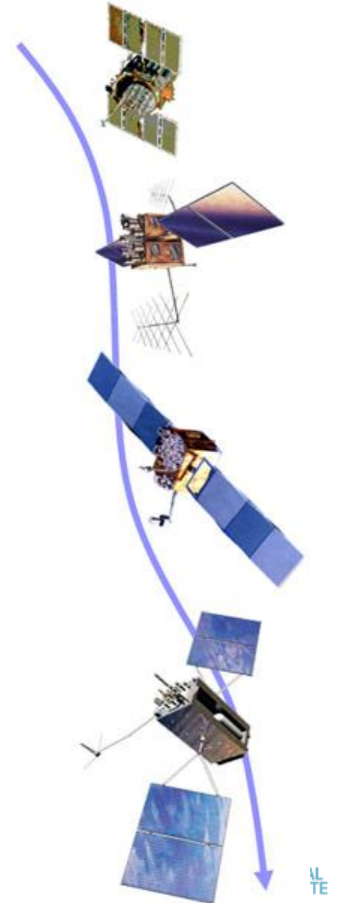
Read more:

<https://www.gps.gov/systems/gps/modernization/civilsignals/>



GPS Modernization Video

<https://www.youtube.com/watch?v=chNQW22vVNI>

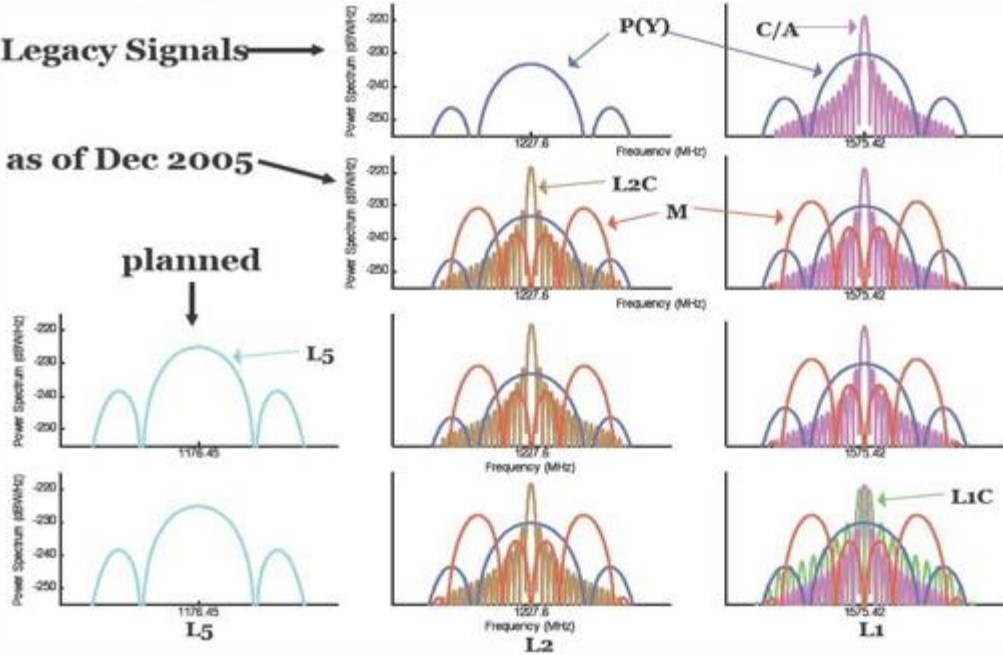


GPS MODERNIZATION

Legacy Signals

as of Dec 2005

planned



Block IIA, 1990



Block IIR-M, 2005



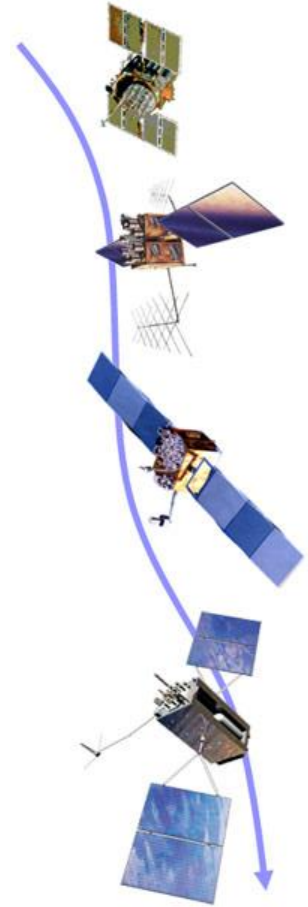
Block IIF, 2009



Block III, 2014



(artist's concept)



GLONASS

Developed by the Sovietic Union during the cold war (1976)

Based on the same geometrical principles of the GPS

All the satellite transmit the same code on different frequencies (FDMA)

24 MEO satellites constellation on three orbital at high inclination in order to serve better regions at high latitude (e.g. Siberia)

C/A code and P code (no SA)



ГЛОНАСС
ГЛОБАЛЬНАЯ НАВИГАЦИОННАЯ СПУТНИКОВАЯ СИСТЕМА
(Global'naja Navigacionnaja Sputnikovaja Sistema)

GLONASS SATELLITES

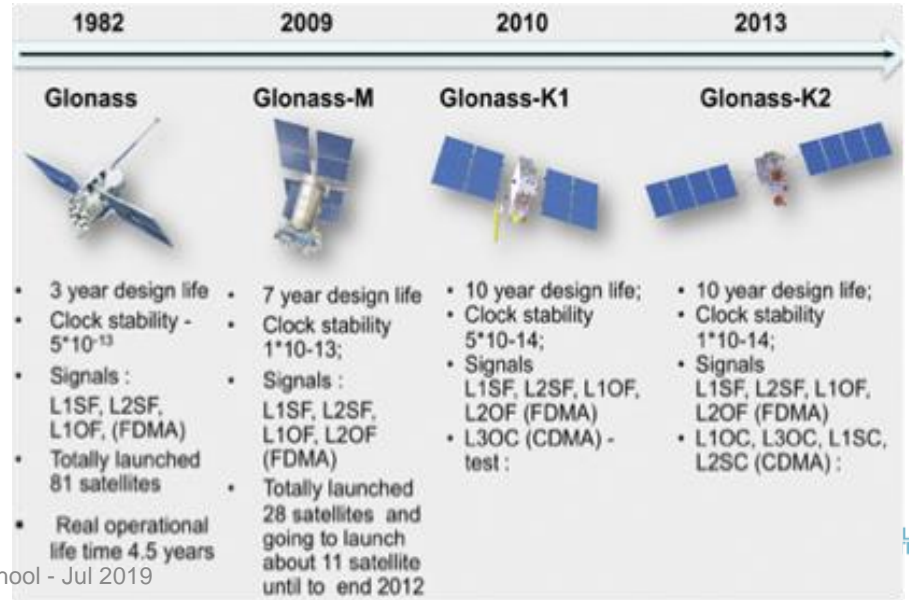
Original Glonass (1982, dismissed)

Glonass-M (2003)

Glonass-K1 (2011)

Glonass-K2 (2015)

Glonass-KM (2025 –
currently in research phase)

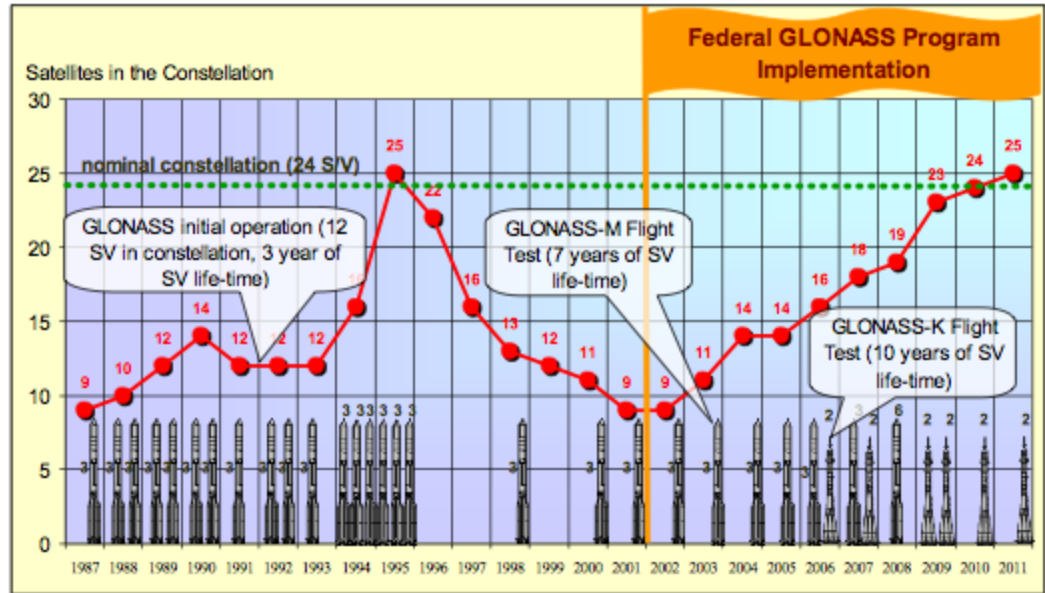


GLONASS MODERNIZATION

By 2010 has achieved again 100% coverage of Russia

In October 2011 the full orbital constellation of 24 satellites was restored, enabling full global coverage

GLONASS program is in progress and has been extended to 2020, by which time the system is scheduled to have all satellites transmitting both the new CDMA and legacy FDMA signals



BEIDOU – 北斗



Evolution of a regional military system (1997)

Operational in China since December 2011

Named after Big Dipper constellation



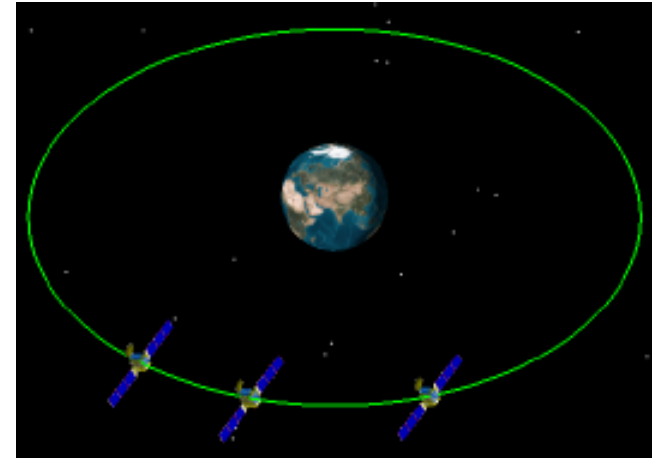
PHASE 1

BeiDou Satellite Navigation Experimental System

Three satellites

Limited navigation services and coverage

decommissioned at the end of 2012



Orbit characteristics

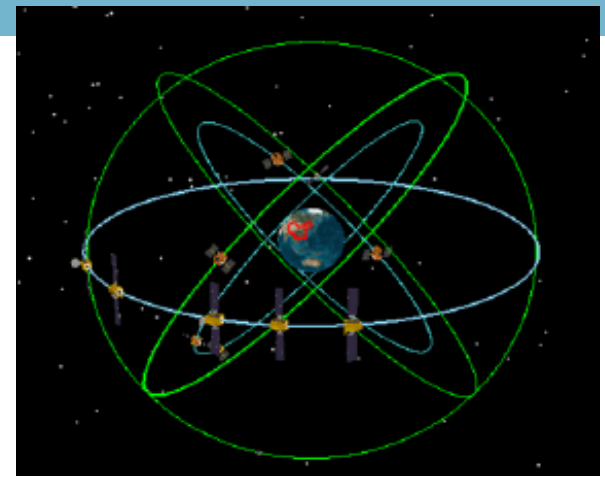
Orbit	GEO
Semi/major Axis	42164 km
Eccentricity	0
Inclination	0 deg
Argument Perigee	0 deg
Mean Anomaly	0 deg

PHASE II

Sometimes called COMPASS

Started operating in December 2011 with a partial constellation of 10 satellites.

It has been providing services to customers in the Asia-Pacific region since the end of 2012.



Orbit	GEO	IGSO	MEO
Satellites	5	5	4
Planes	1	3	2

Orbits characteristics			
Orbit	GEO	IGSO	MEO
Semi/major Axis (km)	42164	42164	27878
Eccentricity	0	0	0
Inclination (deg)	0	55	55
Argument Perigee (deg)	0	0	0

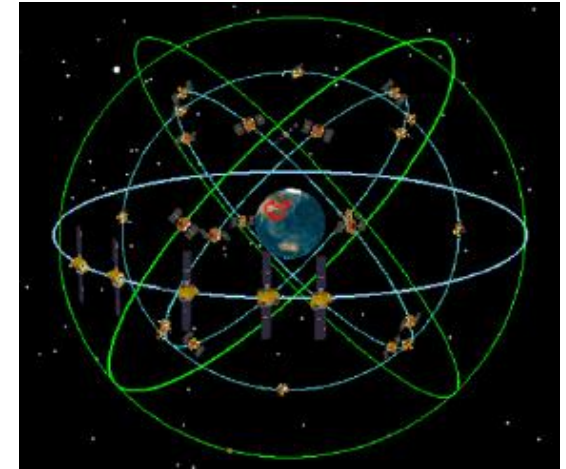
PHASE III

Global coverage

Started in 2015

35 satellites in orbit and global services by 2020

According to China Daily, in 2015 (fifteen years after the BeiDou-1 system was launched) it was generating a turnover of \$31.5 billion per year for major companies such as China Aerospace Science and Industry Corp, AutoNavi Holdings Ltd, and China North Industries Group Corp.



Orbit	GEO	IGSO	MEO
Satellites	5	2	30
Planes	1	3	3

Orbits characteristics			
Orbit	GEO	IGSO	MEO
Semi/major Axis (km)	42164	42164	27878
Eccentricity	0	0	0
Inclination (deg)	0	55	55
Argument Perigee (deg)	0	0	-

Beidou satellite navigation network

29 satellites launched between 2000 and November 2017, including



2 third-generation satellites launched Nov 5.



16 satellites to be launched by end of 2018



Launches in 2019 and 2020 will comprise **2** into geostationary orbits



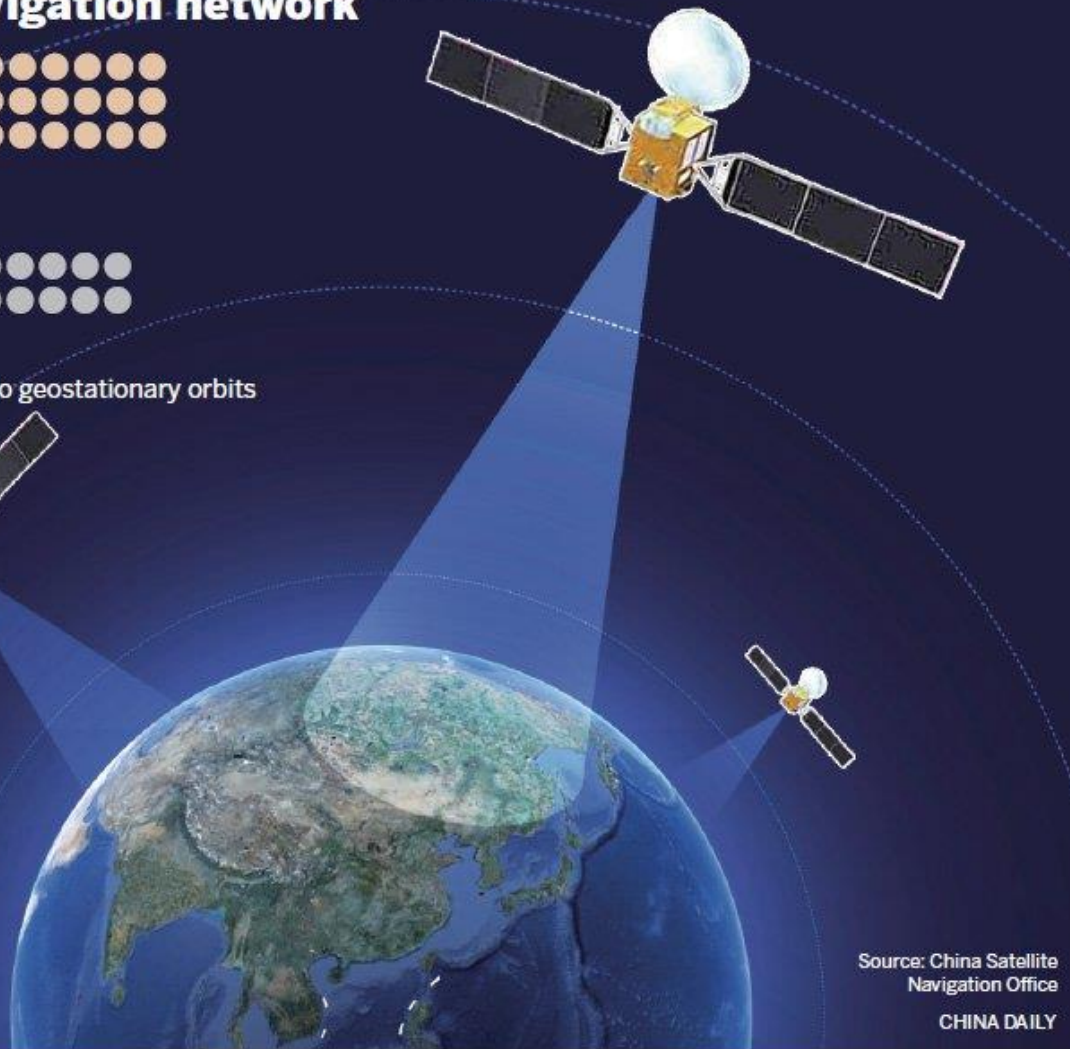
3 into inclined geosynchronous satellite orbits

6 into medium Earth orbits



By end of 2020: Network will consist of more than **30** satellites (several now in orbit will be decommissioned) to give global coverage.

* **Third-generation satellites:** They are more accurate, stable and with better signal clarity, and also more compatible with GPS, GLONASS and Galileo systems.



Source: China Satellite Navigation Office

CHINA DAILY

CONSTRUCTION PRINCIPLES

Open. High quality service free of charge for users all over the world.

Independent. China will construct and operate the BeiDou Navigation Satellite System independently, and the system can provide global service on its own.

Compatibility and interoperability between BeiDou and other countries' satellite navigation systems.

Progressive. China will actively promote BeiDou construction and development, improve service quality continuously, and realize the seamless integration between each stage.

Source: www.beidou.gov.cn

GALILEO

Initiative of the European Union (EU) and the European Space Agency (ESA),
in collaboration with European Industries and Universities

European Public Funds for the system development

Under **civilian** control

Global coverage (30 satellites)

Fully operational by 2020: Full Operating Capability (FOC)

Independent from other existing systems

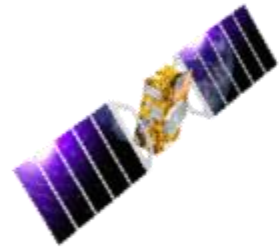
Interoperable

New services and signals

Expected better performances for future receivers



GALILEO IMPLEMENTATION PLAN



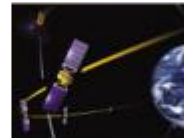
Galileo System Testbed v1
Validation of critical algorithms
2003



GIOVE A/B
2 test satellites
2005/2008



In-Orbit Validation
4 fully operational satellites and ground segment
2013

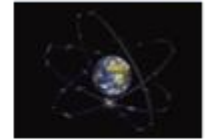


Initial Operational Capability
Early services for OS, SAR, PRS

2014/2015



Full Operational Capability
Full services, 30 satellites
2018



GALILEO IS AVAILABLE!

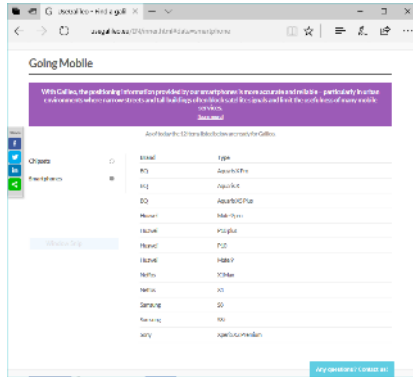
Since December 15, 2016



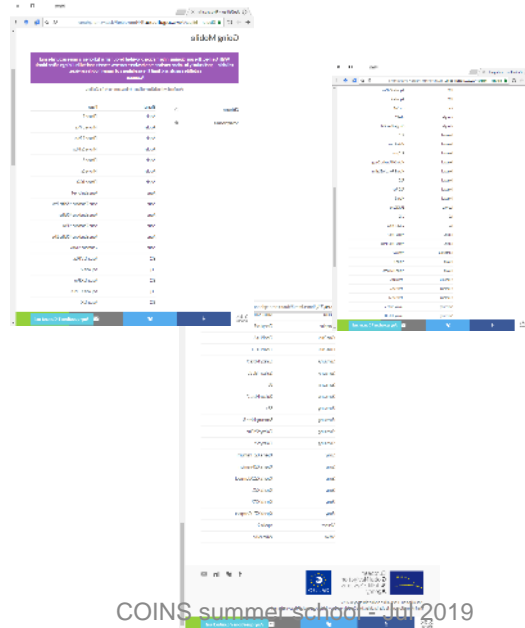
www.usegalileo.eu

GALILEO ENABLED SMARTPHONES

2017



2018



2019

<https://www.usegalileo.eu/EN/inner.html#data=smartphone>



GALILEO TODAY

21/10/2011: SV 11 and 12

12/10/2012: SV 19 and 20

22/08/2014: SV 18 and 14

27/03/2015: SV 26 and 22

11/09/2015: SV 24 and 30

17/12/2015: SV 8 and 9

24/05/2016: SV 1 and 2

17/11/2016: SV 7, 3, 4 and 5

12/12/2017: SV 21, 25, 27 and 31

25/07/2018: SV 36, 13, 15, 33

2020: ?

Unavailable (from 27/05/2014)

Testing only

*Unavailable
(since 08/12/2017)*



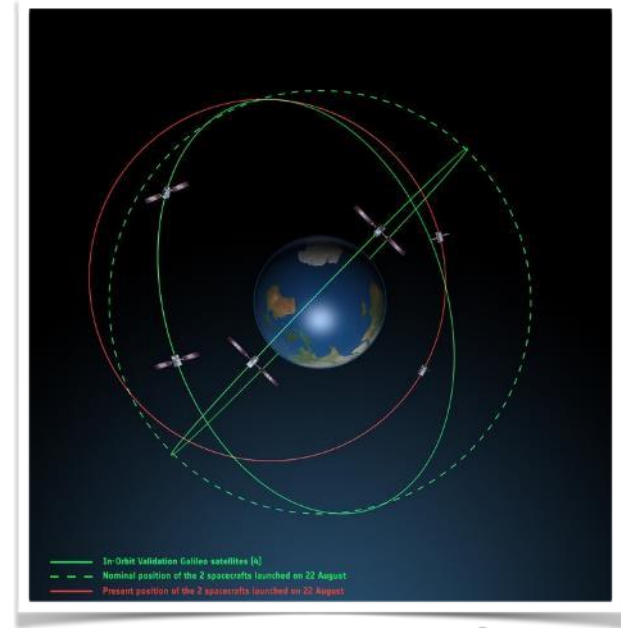
WHERE ARE DORESA AND MILENA?

Injected in a wrong orbit: **lower and elliptical orbits** instead of the expected circular orbits

The satellites did not have enough fuel on board to achieve the correct orbit for full Galileo operations

In "safe state" since 28 August, fully under control from ESA's centre in Darmstadt, Germany

The potential of exploiting the satellites to maximum advantage, despite their unplanned injection orbits and within the limited propulsion capabilities, is being investigated



<http://insidegnss.com/galileo-5-and-6-eccentric-satellites-mission-recovery-and-exploitation-part-i/>

GALILEO SERVICES (UPDATE)

Open Service (OS): Galileo open and free of charge service set up for positioning and timing services.

High Accuracy Service (HAS): A service complementing the OS by providing an additional navigation signal and added-value services in a different frequency band. The HAS signal can be encrypted in order to control the access to the Galileo HAS services.

Public Regulated Service (PRS): Service restricted to government-authorized users, for sensitive applications that require a high level of service continuity.

Search and Rescue Service (SAR): Europe's contribution to COSPAS-SARSAT, an international satellite-based search and rescue distress alert detection system.

NAVIC

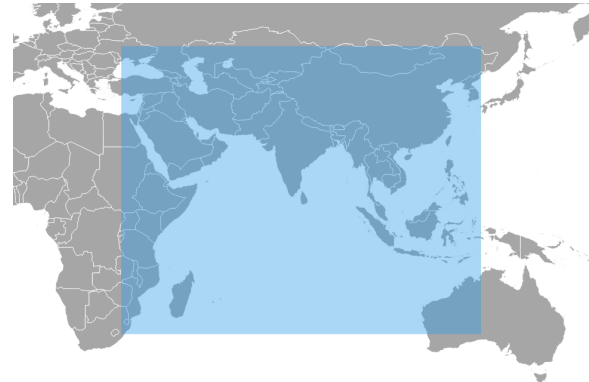
Indian Regional Navigation Satellite System (IRNSS)

Operational name: NavIC
NAVigation with Indian Constellation

sailor or *navigator* in Sanskrit and Hindi

being developed by ISRO:
Indian Space Research Organization (

first satellite successfully
launched on July 1, 2013



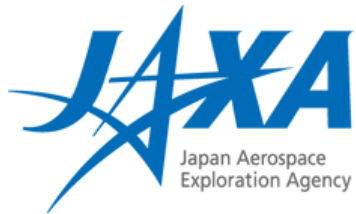
QZSS

Quasi-Zenith Satellite System

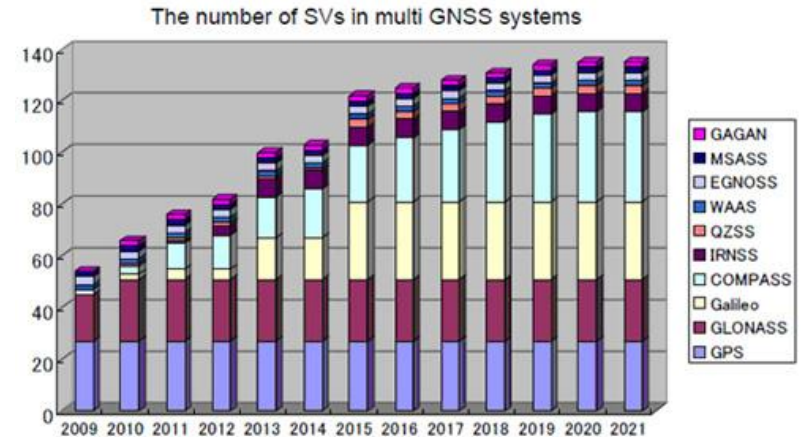
Commissioned by the Japanese Government as a National Space Development Program

29 March 2017: Start of Trial Services

QZSS currently uses one geostationary satellite orbit and three in the QZO orbit (highly inclined, slightly elliptical, geosynchronous orbit)



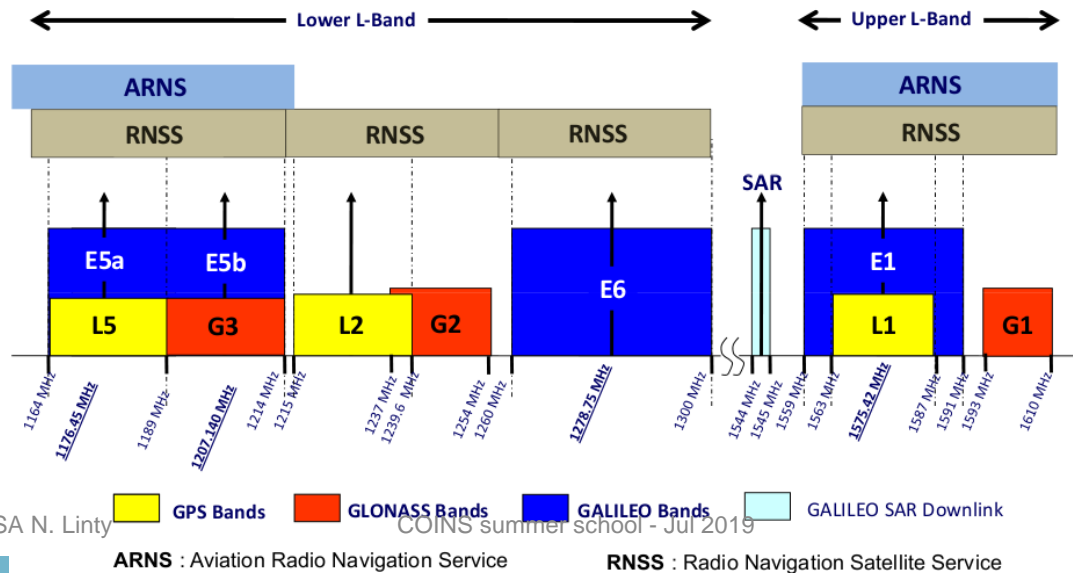
DO WE NEED SO MANY GNSS?



COMPATIBILITY AND INTEROPERABILITY

Agreement on common coordinate frame and time standard

Compatibility: tolerate each other and coexist peacefully. As in any crowded situation, you want to make sure that the neighbors act responsibly and have not loud parties.



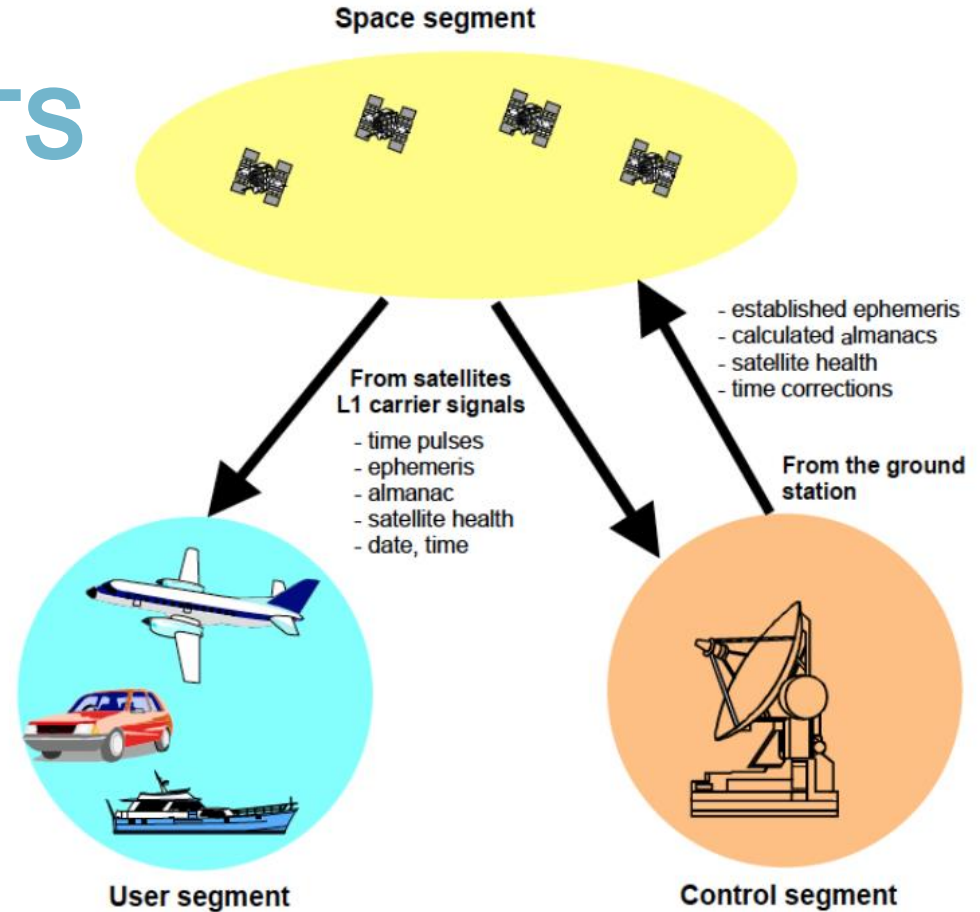


GNSS FUNCTIONAL PRINCIPLES



GNSS SEGMENTS

Space
Control/Ground
User



Source: Wireless Security GNSS Security
Srdjan Čapkun, Department of Computer Science
ETH Zurich, Switzerland

CONTROL SEGMENT

A network of stations, distributed all around the Earth, monitors the status of the satellites and of the signals

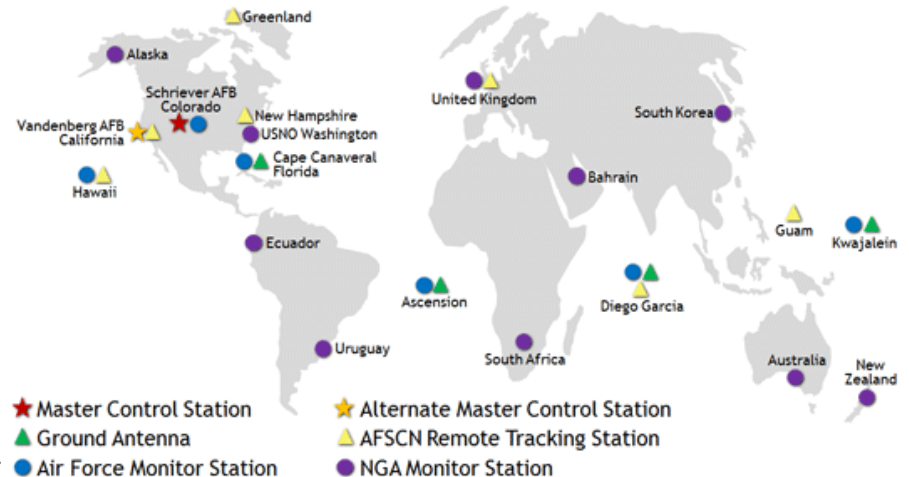
Master station:
data processing, update orbits and time scale

Tracking stations:
continuously monitoring the orbital data

Uploading stations:
transmit updated data to satellites

Picture source:

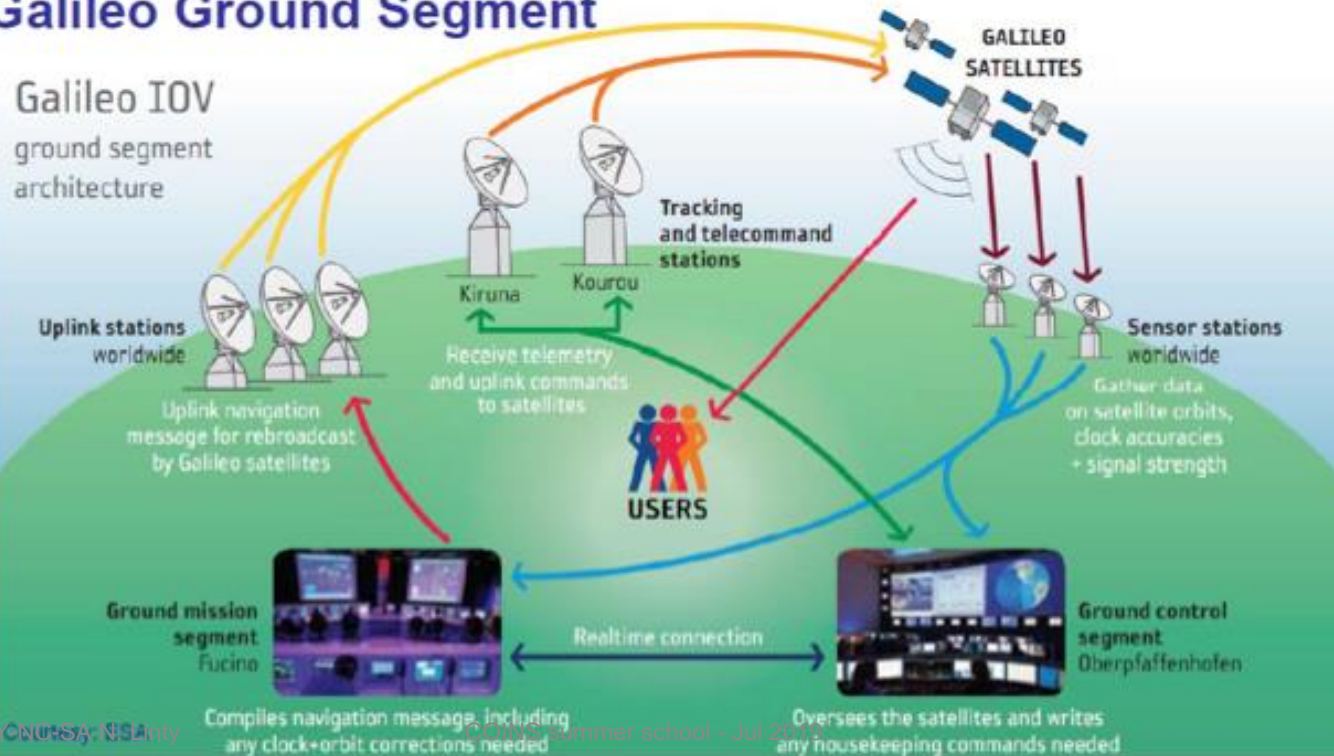
<https://www.gps.gov/systems/gps/control/>



CONTROL SEGMENT

Galileo Ground Segment

A network of satellite ground stations
Master satellite data processing
Tracking and command
Continuous operation
Upload navigation messages



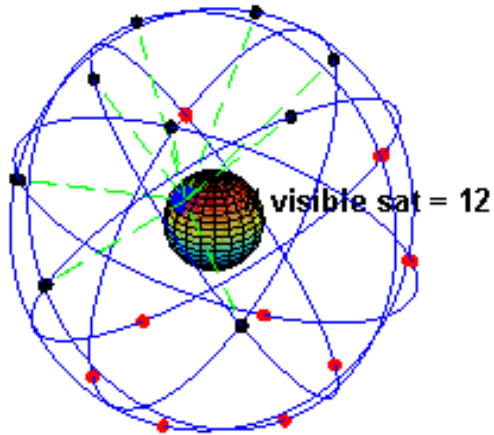
is of the

SPACE SEGMENT

Satellites constellation (Low or Medium Earth Orbit)

Transmission of radio signals

Azimuth and Elevation

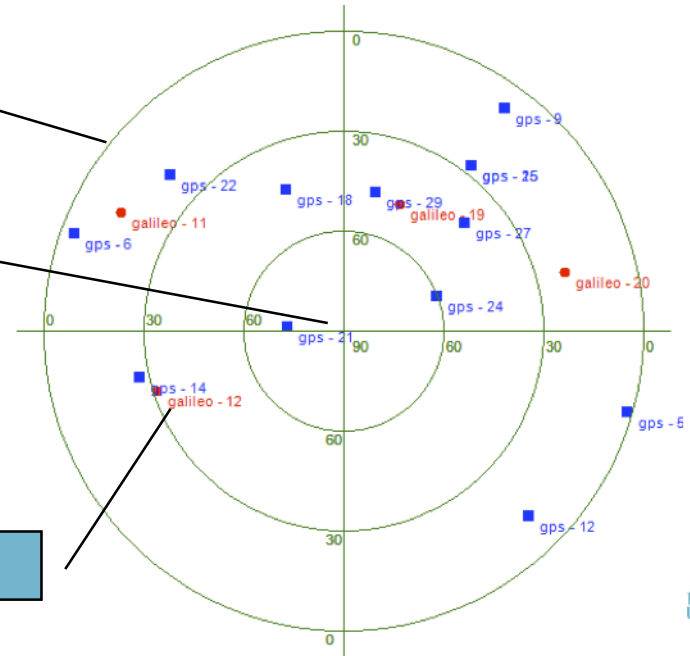


CC BY-NC-SA N. Linty

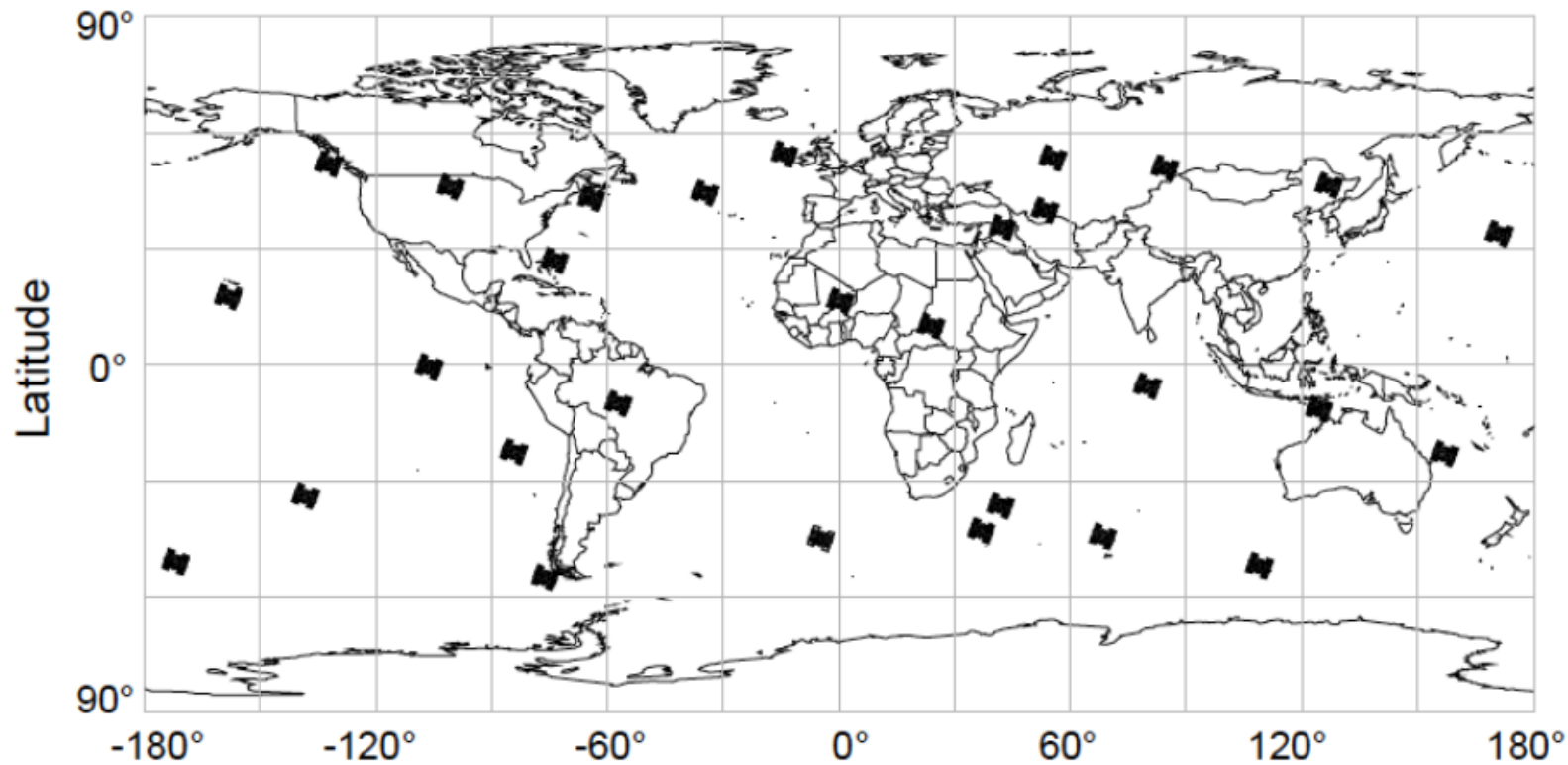
Horizon

Zenith

Satellite Vehicle (SV)



COINS summer school - Jul 2019



Source: Wireless Security GNSS Security
Srdjan Čapkun, Department of Computer Science
ETH Zurich, Switzerland

Longitude

USER SEGMENT

Wide range of different receivers, with different performance levels, determining their own position, velocity and time

The receiver estimates the position of the user on the basis of the signals transmitted by the satellites

First mobile commercial receiver: 1980

Two revolutions: *electronics* and *digital maps*



Texas Instruments TI 4100

150 000 \$

Story told about Dallas oliman...

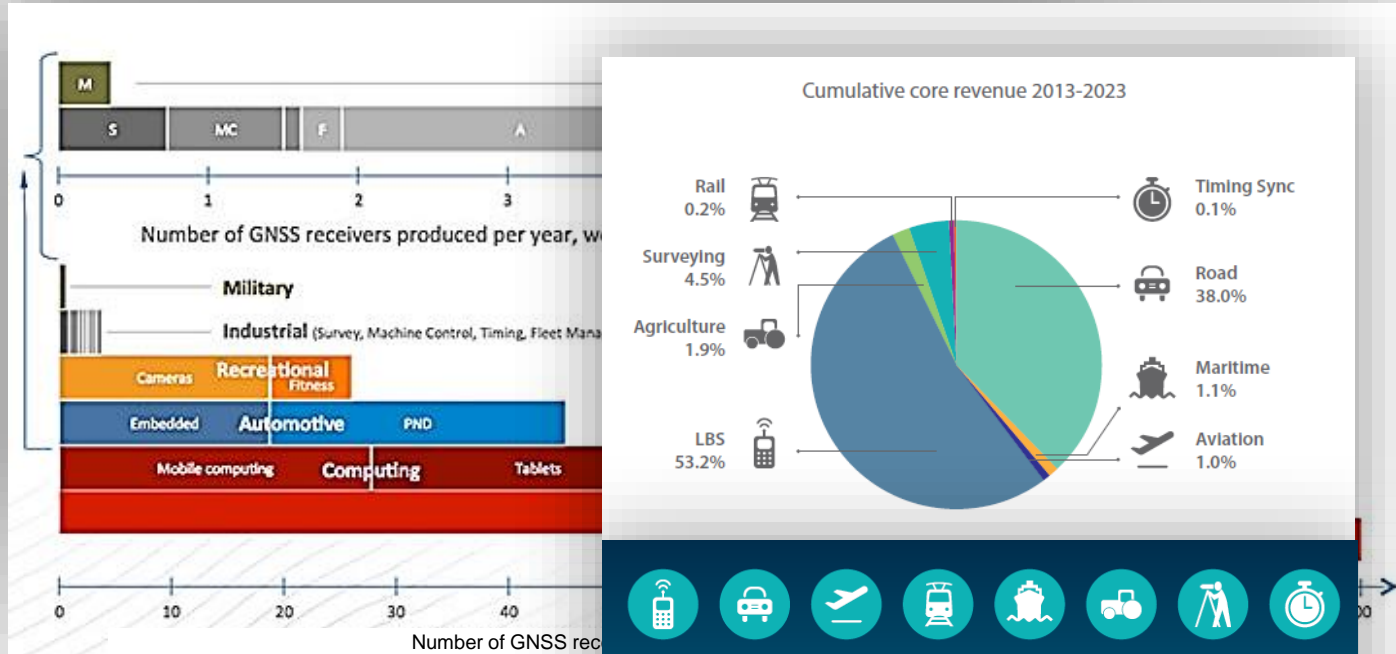
USER SEGMENT



Professional		Mass market
Survey, construction, security, military	Objective	Navigation, gaming, social, leisure, sport
1 000 – 100 000 \$	Cost	1 – 10 \$
> 1 dm ³	Size	< 1 cm ²
Millimetre-level	Accuracy	Metre-level
Doppler, code delay, carrier phase	Observables	Doppler, code delay
Dual frequency, differential	Surplus value	Assisted-GNSS
Closed tracking loops (DLL, PLL)	Architecture	Snapshot estimation (open loop)
Small	Market share	Huge



USER SEGMENT



GNSS MARKET REPORT ISSUE 4

USER SEGMENT

The core functionalities common to any kind of receiver can be summarized as

- Identification of the satellites in view
- Estimation of the distance user-satellite
- Trilateration

Additional functionalities aim at

- easing and/or improving the position estimation (augmentations)
- improve the user output interface
- added value services (e.g. route calculation, integration with communication systems)



FUNCTIONAL BASICS

A satellite transmits a pulse at time t_0

the pulse is received at time $t_0 + \tau$

the distance between TX and RX can be estimated as:

$$R = c \cdot \tau$$

with c the speed of light

If both the oscillators are perfect the measure of $t_0 + \tau$ allows for R determination

FUNCTIONAL BASICS

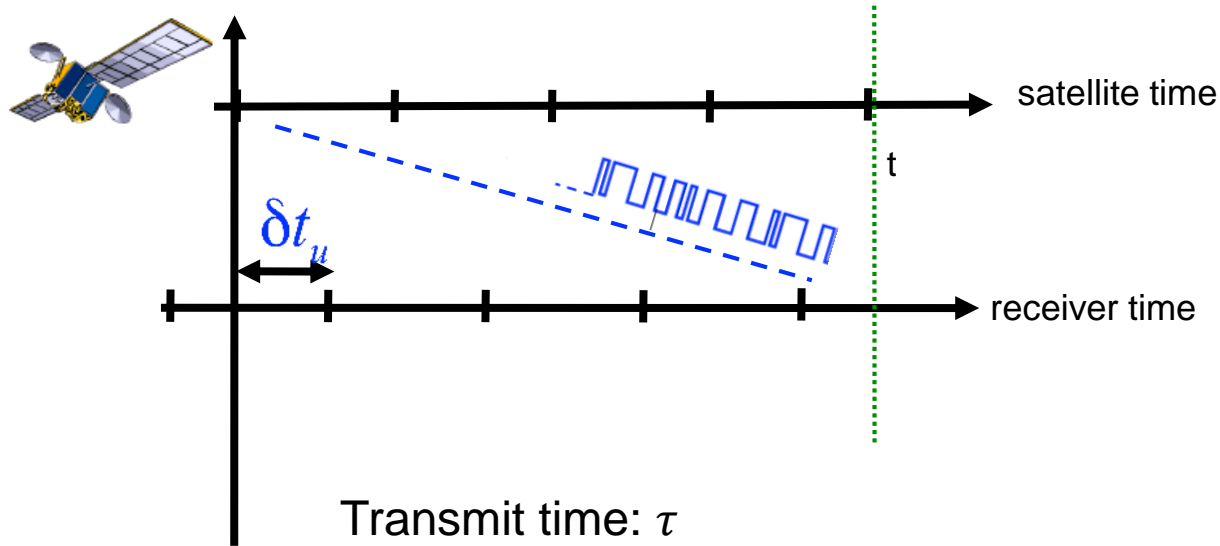
The satellites' payloads host synchronous clocks

It is not possible to have user clocks aligned with the satellite time scale at low cost and complexity

Being δt_u the user clock misalignment the measured distance is the **pseudorange**:

$$\rho = c \cdot \tau + c \cdot \delta t_u$$

FUNCTIONAL BASICS



Transmit time: τ
Pseudo transmit time: $\tau + \delta t_u$
Pseudorange: $c(\tau + \delta t_u)$

Dovis F., Satellite Navigation Systems, lecture notes, NavSAS, Politecnico di Torino

FUNCTIONAL BASICS

The user measuring 4 pseudoranges with respect to 4 satellites with known coordinates can determine 4 unknowns:

$$(x_u, y_u, z_u)$$

User coordinates

$$\delta t_u$$

The bias of the user clock with respect to the GNSS time scale

FUNCTIONAL BASICS

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} - c \cdot \delta t_u \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} - c \cdot \delta t_u \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} - c \cdot \delta t_u \\ \rho_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} - c \cdot \delta t_u \end{cases}$$

(x_j, y_j, z_j) Satellite position: center of the pseudo-sphere

ρ_j Pseudorange: radius of the pseudo-sphere

$b_{ut} = c \cdot \delta t_u$ Clock bias

SOLUTION

After a linearization procedure,
set of equations in matrix form

$$\Delta \mathbf{x} = \mathbf{H}^{-1} \Delta \rho$$

Distance between
true position and
linearization point

H matrix, depends
only on satellites
position

Pseudorange
(difference between measured
pseudorange and distance to the
linearization point)

POSITIONING ERRORS

The pseudorange measurement is affected to errors, due to system intrinsic uncertainties, propagation in atmosphere, receiver noise and other factors

$$\rho_j = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2} - b_{ut} + \epsilon$$

The error in the pseudorange measurement affects the user position

POSITIONING ERRORS

The set of equations to solve is then

$$\Delta \rho + \delta \rho = \mathbf{H} (\Delta \mathbf{x} + \delta \mathbf{x})$$

where δx represents the error in the position and time estimation

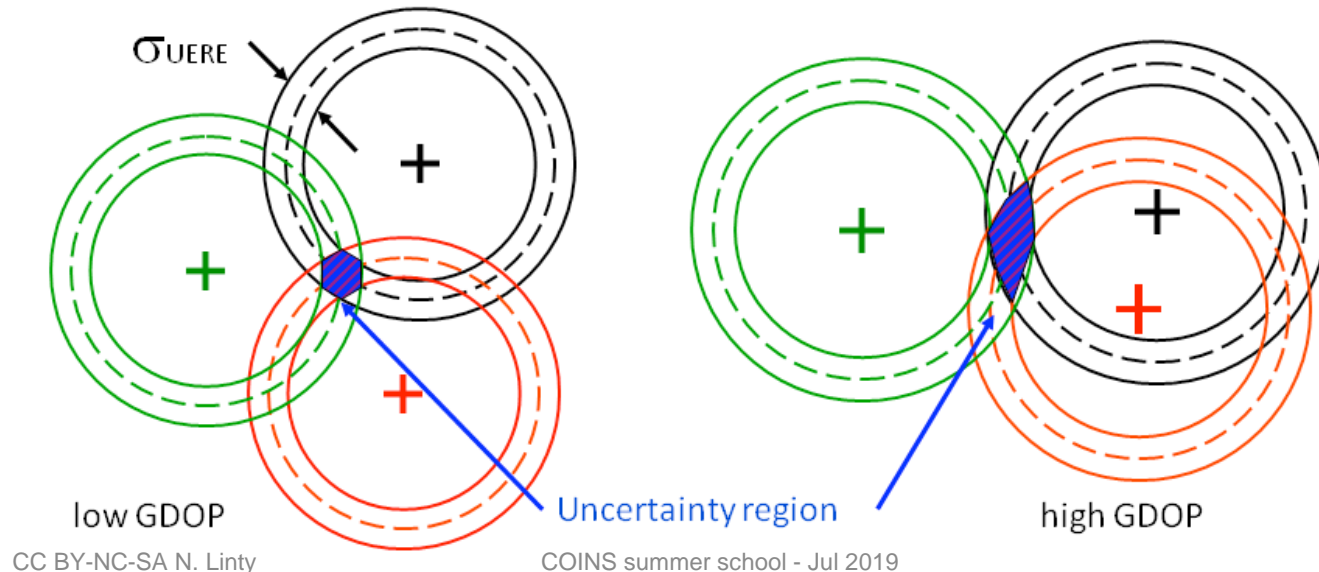
$$\delta \mathbf{x} = \left[(\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T \right] \delta \rho$$

Error contribution depending only on
the **satellite geometry**

Error contribution depending only on
the **pseudorange estimation**

THE GEOMETRICAL PROBLEM

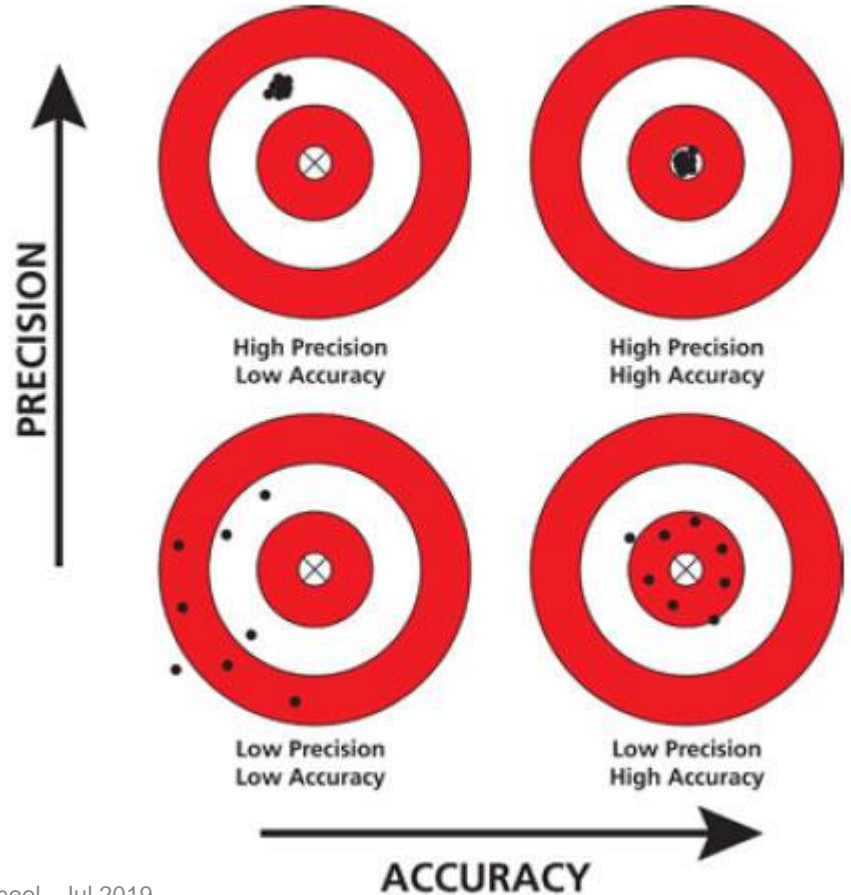
The impact of the pseudorange error on the final estimated position depends on the displacement of the satellites (reference points)



DEFINITIONS

Accuracy: measure of how close a point is to its true position

Precision: measure of how closely the estimated points are in relation to each other



PSEUDORANGE ERRORS

Can be modeled as random variables:

- gaussian with zero mean
- identically distributed
- independent
- with variance σ_{URE}^2

control system: ephemerides, clocks, codes, measurement errors

Ionosphere

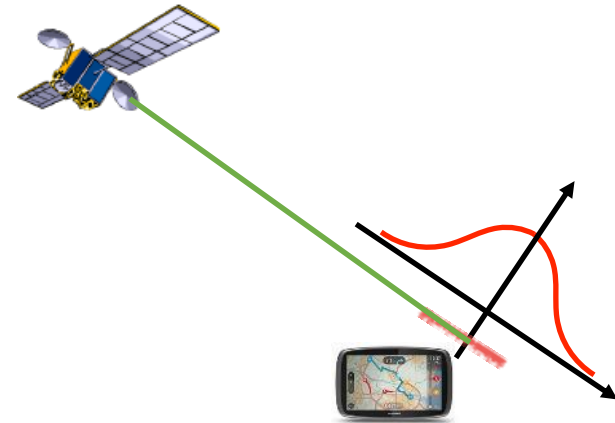
troposphere: pressure, temperature, humidity of the air

Multipath

receiver noise

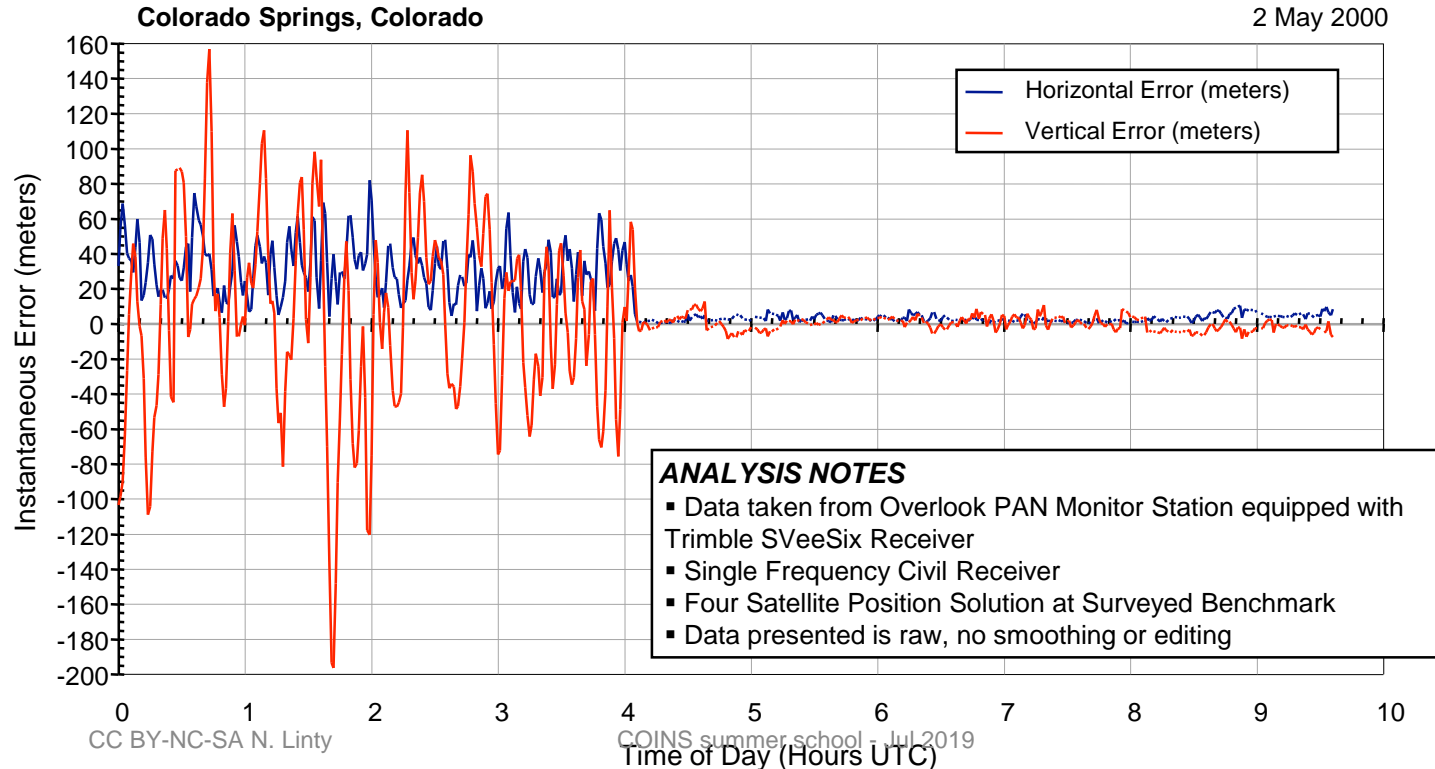
uncompensated relativistic effects

selective availability (SA)



Dovis F., Satellite Navigation Systems, lecture notes, NavSAS, Politecnico di Torino

SELECTIVE AVAILABILITY



IONOSPHERIC MODEL

$$I_{\rho} = \frac{40.3 \cdot \text{TEC}}{f^2}$$

Ionosphere induces a pseudorange delay, which depends on the carrier frequency and on the density of electrons (TEC, totale Electron Content) along the path

The delay introduces an error on the measured pseudorange

The propagation path length of a signal through the ionosphere increases with the zenith angle > the increased path length is accounted for in terms of a multiplier of the zenith delay

RELATIVISTIC EFFECTS

GPS is a bunch of synchronized clocks

Although extraordinarily stable, they are not at rest on Earth at mean sea level

Move at 4 km/s

At 20 000 km Earth's gravity is one fourth that a sea level

Special relativity: a moving clock is slower

About $-7 \mu\text{s}$ per day for a GPS satellite

General relativity: a clock in weaker gravitational field is faster

About $+45 \mu\text{s}$ per day for a GPS satellite

Effect on range measurements: 11 km

However, a common error is harmless, can be solved in PVT

Relativistic effect is compensated:

Satellites clock frequency is adjusted so that the frequency observed by the user at sea level has the nominal value 10.22999999543 MHz

Net effect:
about $+38 \mu\text{s}$ per day

RELATIVISTIC EFFECTS

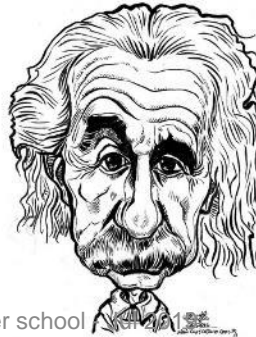
But orbits aren't circular:

At the perigee, the satellite velocity is higher and the gravitational potential is higher → the satellite clock runs slower

At the apogee, the satellite velocity is lower and the gravitational potential is lower → the satellite clock runs faster

Each satellite is speeding up and slowing down at a different time and rate
(up to 45 ns, 15 m)

This effect is accounted for at the receiver level using orbital parameters



and you thought it
was just a theory!



The GNSS signal



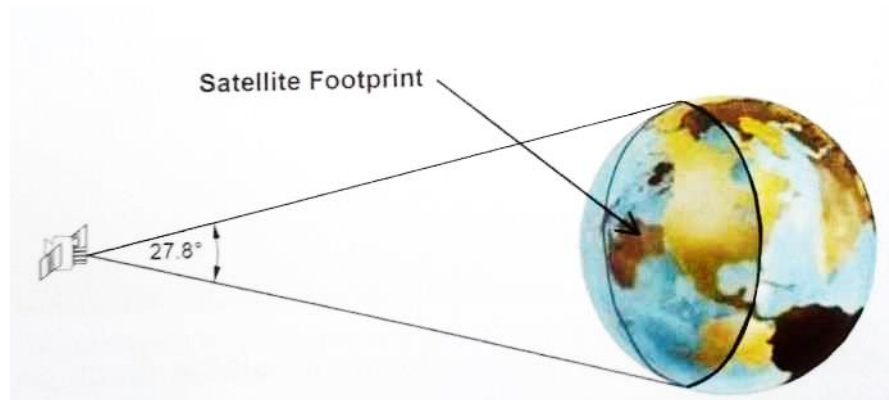
SIGNALS POWER

GNSS signals are extremely weak

30 Watts transmitter, 20000 km away

Received power: 10^{-16} W

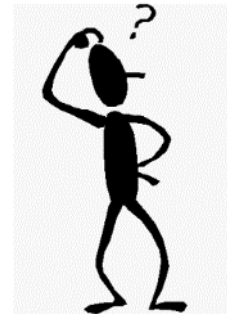
Obstructions weaken further the signals



SUMMING UP, WE (ONLY) NEED TO...

- to understand signals without interference and be robust to the transmission through the atmosphere
- be able to **simultaneously** listen to signals from different satellites, identify the, in a unique way
- determine the **signal arrival time** (TOA) with an accuracy of nanoseconds (to determine metre-level **ranges**)
- transmit some useful **information** (e.g. time of transmission, satellite position, ...)
- Use relatively small antennas at the receiver level

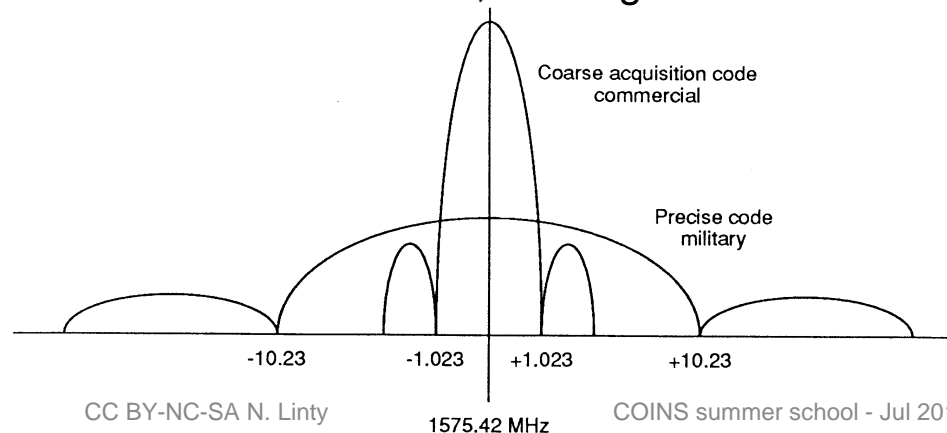
The signal broadcast by the navigation satellites is usually denoted as Signal-In-Space (SIS)



SPREAD SPECTRUM TECHNIQUE

Spread the power over much larger frequency band

- 24 MHz of the radio spectrum allocated to GPS in L1 (as all FM transmissions)
- Spreading obtained by introducing rapid phase variations
- A **binary code** modulates the signal (ranging code)
- The faster the code, the larger the bandwidth



HOW TO ACHIEVE ORTHOGONALITY

In the **time** domain transmitting the signals in different time-slots

In the **frequency** domain transmitting the signals over different frequency bands

In the “**code**” domain using codes that provide a null (or very small) cross-correlation between the signals

GPS uses a Code-Division-Multiplexing (CDMA) technique to identify the satellites without ambiguity

Each satellite uses a different and unique code, using the same carrier frequency, without time division

CORRELATION PROPERTIES

Correlation is a measure of the **similarity** between two sequences

To determine the TOA, we'd like each code to be uncorrelated with any delayed replica of itself:

auto-correlation

$$R_x(\tau) = \int_{-\infty}^{+\infty} x(t)x(t + \tau)dt$$

To reduce interference with each other, we'd like each signal to be uncorrelated with all others:

cross-correlation

$$R_{x,y}(\tau) = \int_{-\infty}^{+\infty} x(t)y(t + \tau)dt$$

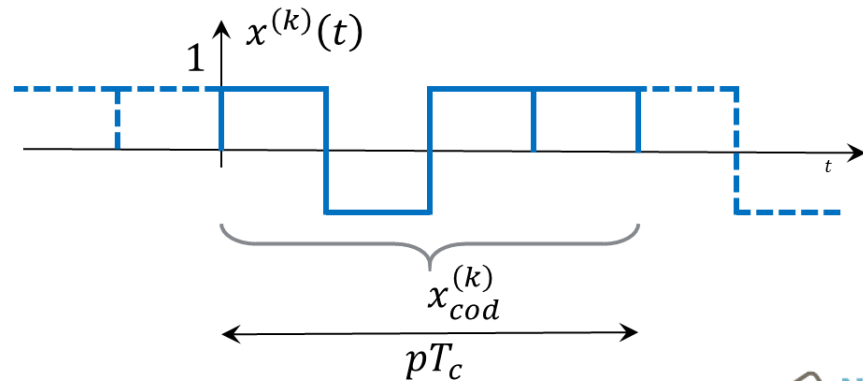
Two signals can be orthogonal, i.e. there is a domain in which they can be separated

GPS CODES

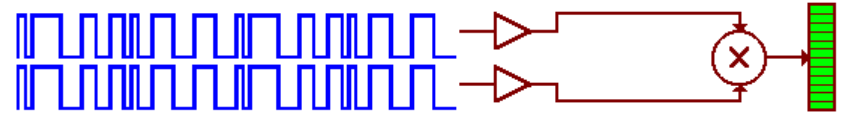
Family of Pseudo Random Noise (PRN) codes: gold codes, or memory sequences

Codes are **mutually orthogonal** in order to permit to the receiver to separate the signal of the satellite of interest from the others

The longer the codes, the better they orthogonality properties, the higher the computational load on the receiver



CODES CORRELATION PROPERTIES



Here are two 31 long PRN codes

C1: 1001011001111100011011101010000

C2: 1100100111110111000101011010000

Correlation = similarity : (number of similar bits – number of dissimilar bits)/ 31

C1 is perfectly correlated with itself:

C1: 1001011001111100011011101010000

C1: 1001011001111100011011101010000

} Auto-Correlation: 31/31

C1 and C1 delayed by one bit:

C1: 1001011001111100011011101010000

C1+1: 0100101100111110001101110101000

} Auto-Correlation: -1/31

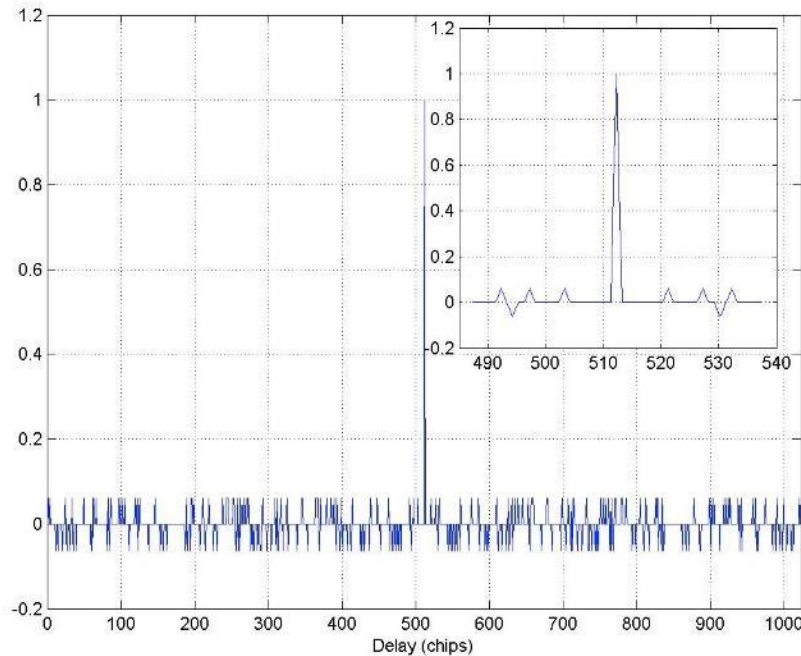
C1 and C2:

C1: 1001011001111100011011101010000

C2: 1100100111110111000101011010000

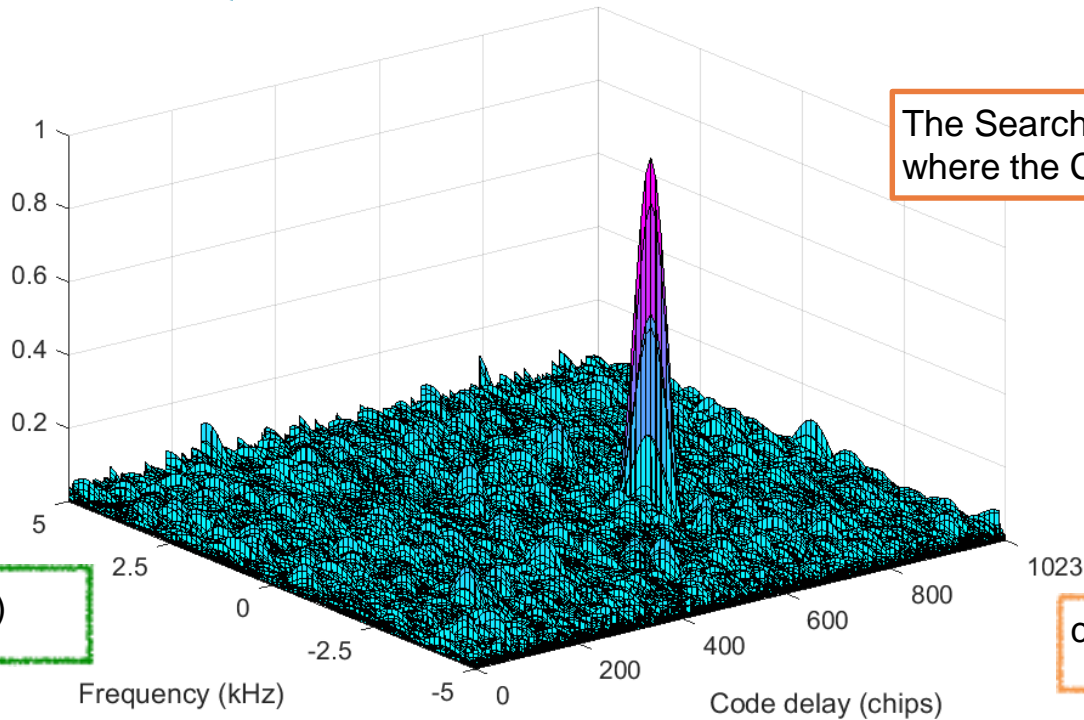
} Cross-Correlation: -1/31

THE CORRELATION FUNCTION



Autocorrelation of PRN code 26.

...AT ACQUISITION LEVEL

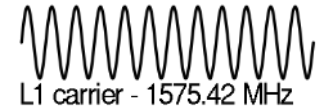


The Search Space is a 3D domain where the CAF is plotted

Doppler (Hz)

code phase (chips)

CARRIER



The signal is modulated on a carrier in the UHF band, (L-band)

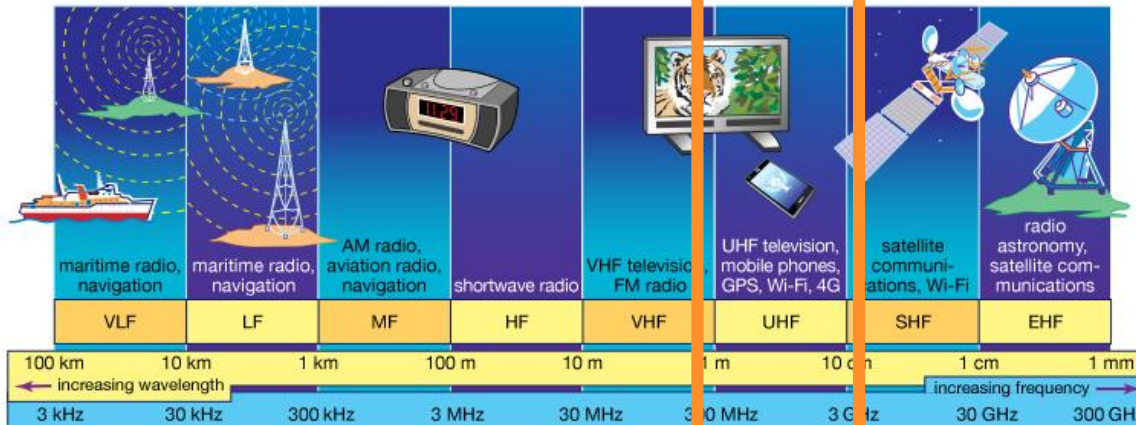
$$f_{L1} = 1575.42 \text{ MHz} = 154 \cdot f_0$$

$$f_{L2} = 1227.60 \text{ MHz} = 120 \cdot f_0$$

$$f_{L5} = 1176.45 \text{ MHz} = 115 \cdot f_0$$

$$f_0 = 10.23 \text{ MHz}$$

Fundamental frequency



CC BY-NC-SA N. Linty

COINS summer school - © 2013 Encyclopædia Britannica, Inc.

DATA AND MESSAGES



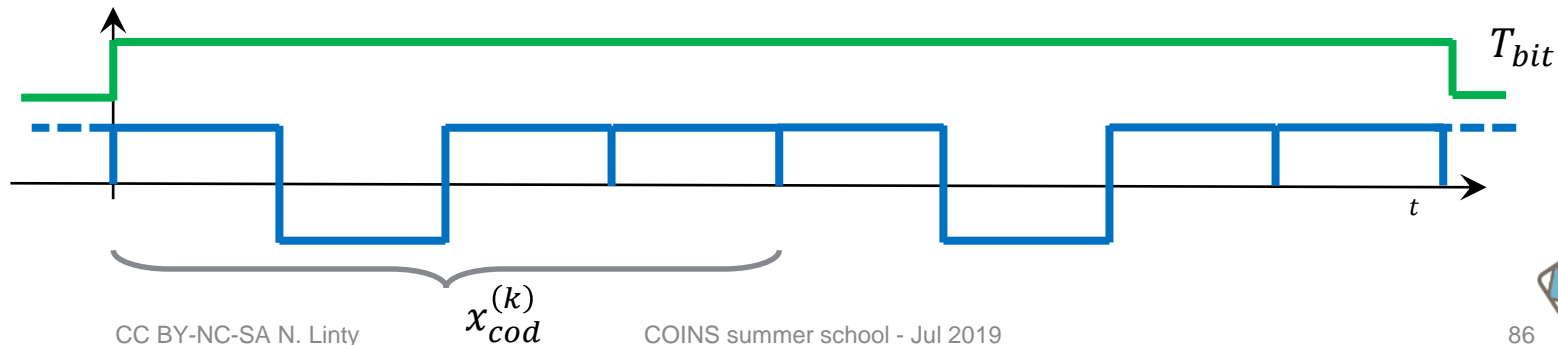
The codes are deterministic periodic signals; they do not carry any kind of information

A navigation message is modulated on top of them to include **useful information**

Modulation is a bit by bit multiplication of the signals.

Navigation data: Binary-coded message with data on the satellite's:

health status, ephemeris parameters (orbital parameters). SV clock bias parameters, almanac (reduced-precision ephemeris data on all satellites), ionospheric corrections



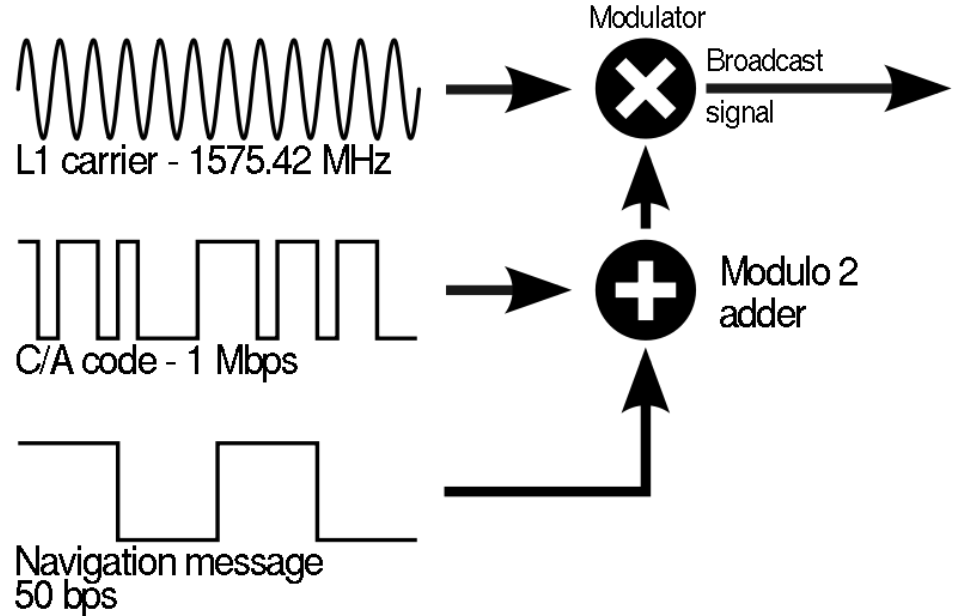
GPS SIGNAL IN SPACE

Each signal consists of 3 components:

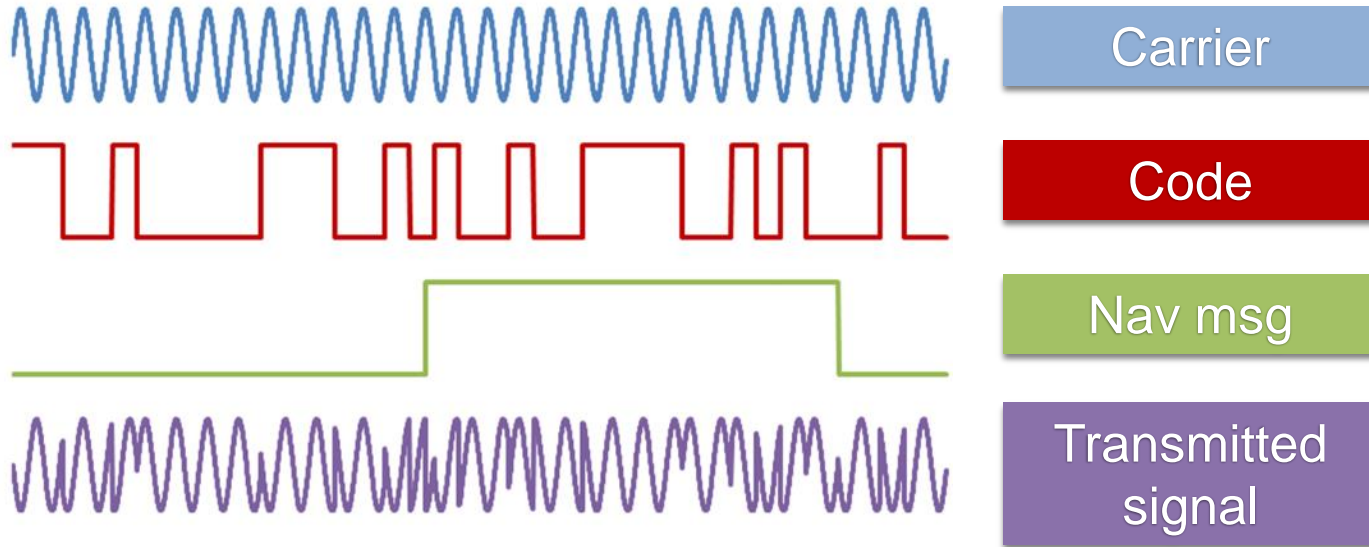
Carrier: RF sinusoidal signal
at frequency f_{L1} , f_{L2} or f_{L5}

Ranging code: Each satellite transmits
a unique PRN code

Navigation message



THE TRANSMITTED GPS SIGNAL



Note: the signal periods are not realistic (not in scale, only pictorial)

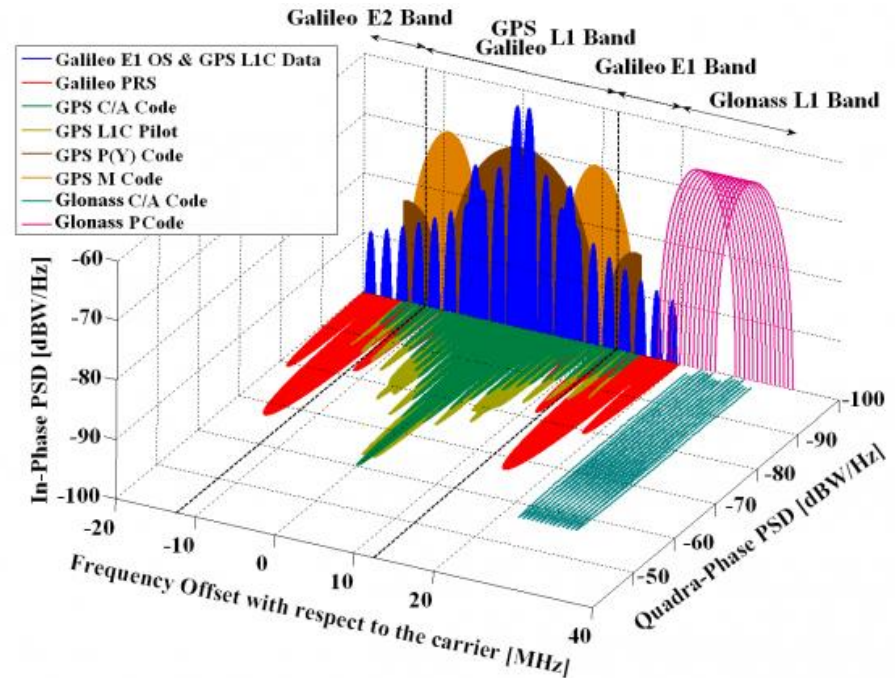
$$y_{T,i}(t) = \sqrt{2P_T} c_i(t) d_i(t) \sin(2\pi f_{RF} t)$$

CC BY-NC-SA N. Linty CGINS summer school - Jul 2019

GNSS IN THE FREQUENCY DOMAIN

Each signal can be represented by means of its **harmonic components** in the frequency domain

Power Spectral Density: a representation of the contribution of each frequency component to the total power of the signal



MORE ON SIGNALS

Page on gnss-sdr project website:

<https://gnss-sdr.org/docs/tutorials/gnss-signals/>

Navipedia:

GPS signal plan

https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan

Galileo signal plan

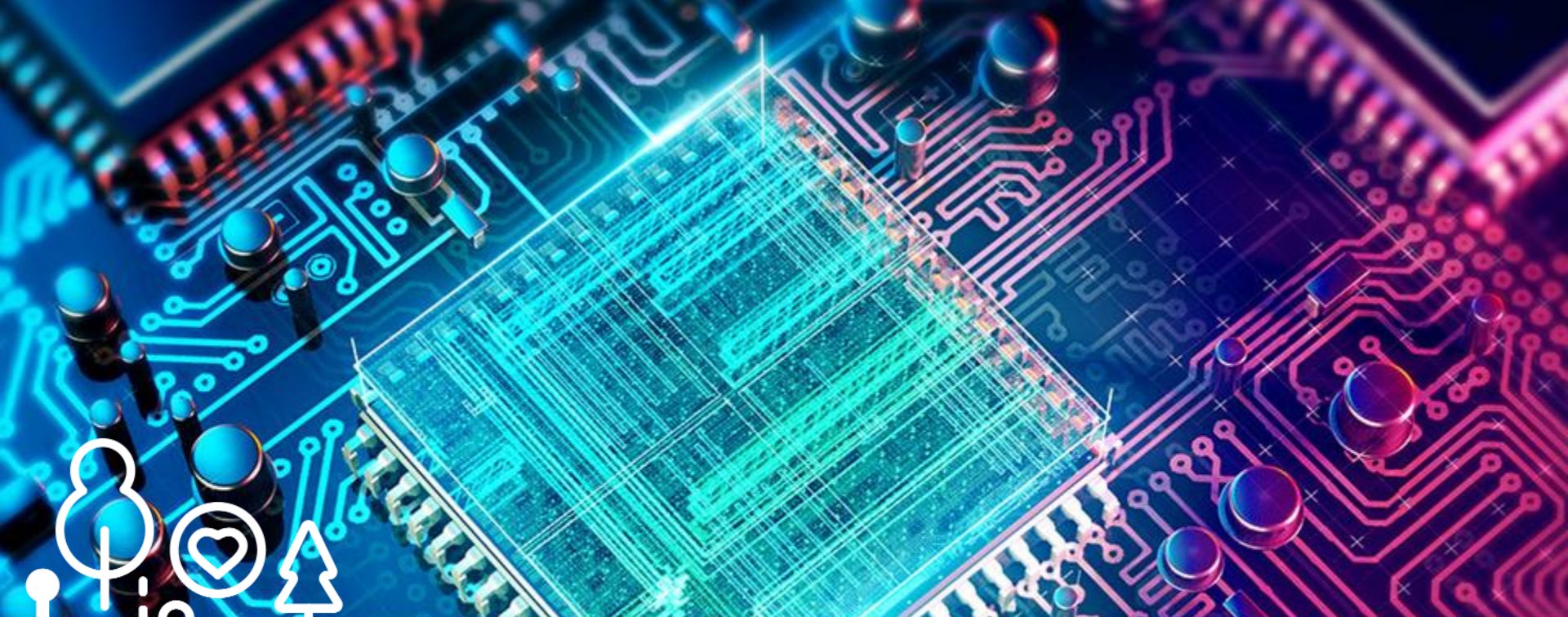
https://gssc.esa.int/navipedia/index.php/Galileo_Signal_Plan

Glonass signal plan

https://gssc.esa.int/navipedia/index.php/GLONASS_Signal_Plan

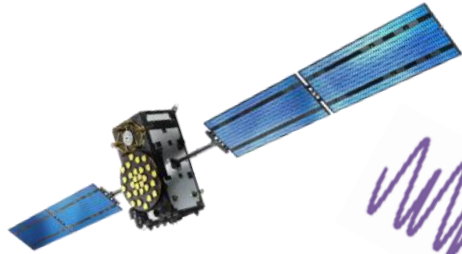
Beidou signal plan

https://gssc.esa.int/navipedia/index.php/BeiDou_Signal_Plan



THE GNSS RECEIVER

SCENARIO



The received signal differs from the transmitted one

- Weaker (below the noise floor)
- Delayed (70 to 90 ms)
→ phase
- Doppler shift



RECEIVERS CORE FUNCTIONS

A navigation receiver has to:

- Gather radio signals transmitted by satellites in a 2 MHz band centered at 1575.42 MHz (“receive”)
- Amplify and filter the signals (“preprocessing”)
- Analog-To-Digital convert the signals
- Determine which satellites are in view and separate the different channels
- Generate local codes for correlation
- Determine and keep track of signals code phase for pseudorange measurements
- Determine and keep track of signals carrier phase for carrier phase measurements
- Decode the navigation message to determine satellites position, velocity and time
- Calculate your position, velocity and time (solve the PVT equations)

THE GNSS RECEIVER

The main task of a navigation receiver is to measure with high accuracy the propagation time of the signal

It is necessary to align the local sequence recovering the delay between a locally generated and the received code (synchronization)

Doppler affecting the code and carrier has to be recovered

The receivers operations can be grouped in four main functions:

Antenna and front-end processing

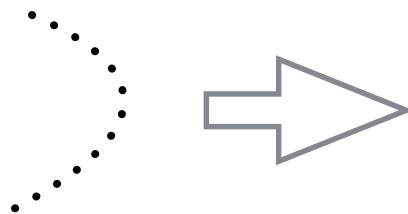
Acquisition

Tracking

code tracking

phase tracking

Demodulation and position estimation



Sub-optimal
Implementation of the
ML estimation of the
propagation delay

MAJOR DRIVERS

Low power consumption

The RX must assure a relatively long operational time (something around 4 hours of continuous operation using external batteries). Key driver for mass-market applications!

Reduced Time to First Fix

The RX must be able to provide the PVT as soon as possible depending on the application's requirements

High accuracy

The major goal of every GNSS RX is to provide user positioning with a high level of accuracy

High acquisition sensitivity

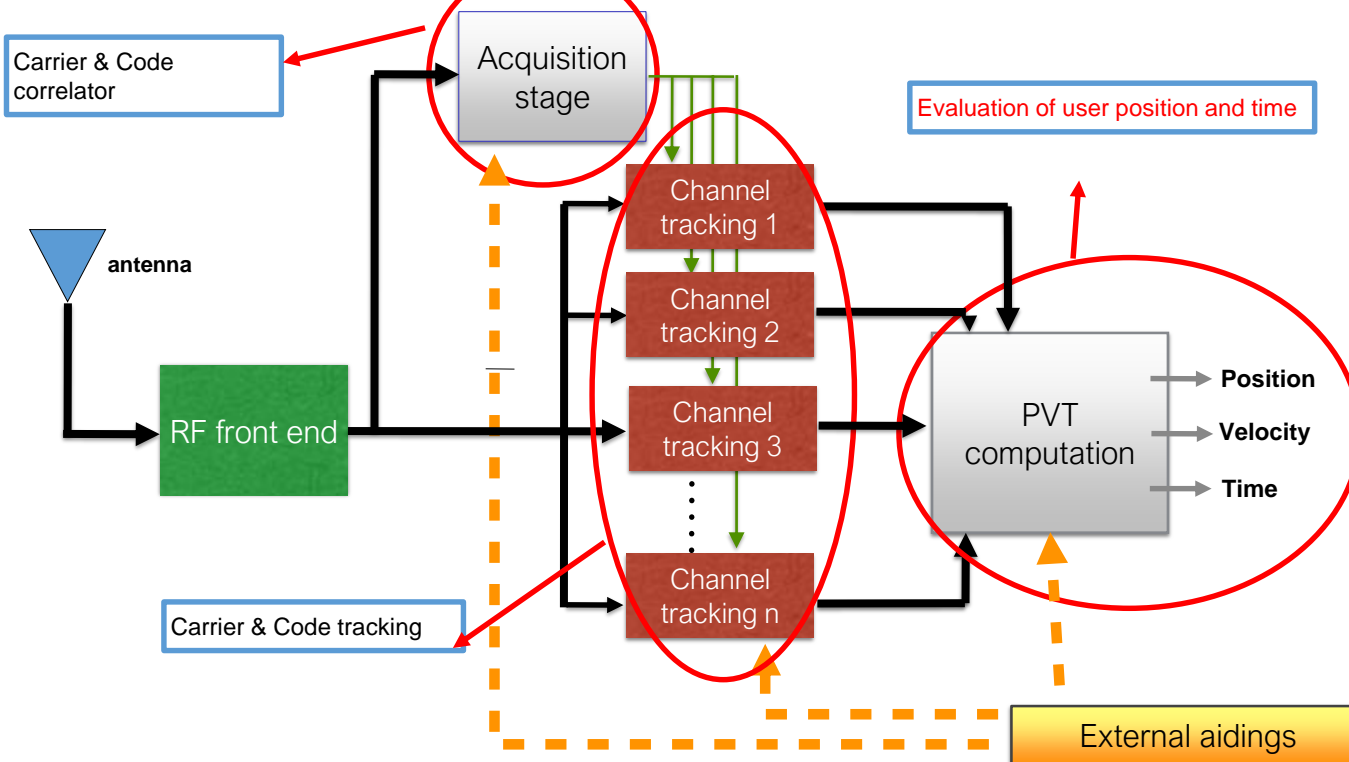
The RX must be able to “see” (acquire) all the satellites available in the sky. In some cases (indoor) the RX must be able to “see” strongly attenuated signals with low C/N0

High tracking sensitivity

The RX must be able to follow the evolution of the SIS even in case of low C/N0.

E.g. urban environment, heavy foliage, ...

GNSS RECEIVER FUNCTIONAL SCHEME



FRONT-END

The first analogue stages of the receiver are used:

- To **capture** the signal in the band of interest

- To band-pass **filter** to isolate the signal of interest

- To **amplify** the signal

- to move the signal from radio frequency (RF) to **intermediate frequency** (IF)

- to sample and quantize (**A/D conversion**) the signal for the following stages

Shaping effect of the filter front-end

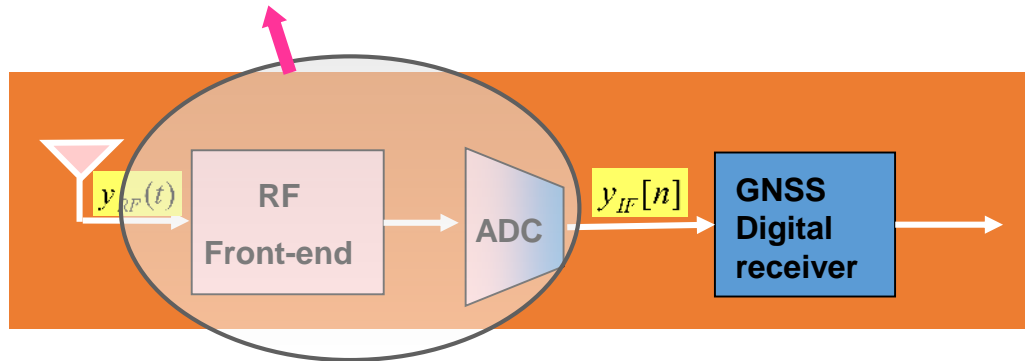
Noise filtering

THE SIGNAL AT BASE BAND INPUT

$$y_{T,i}(t) = \sqrt{2P_T}c_i(t)d_i(t)\sin(2\pi f_{RF}t)$$

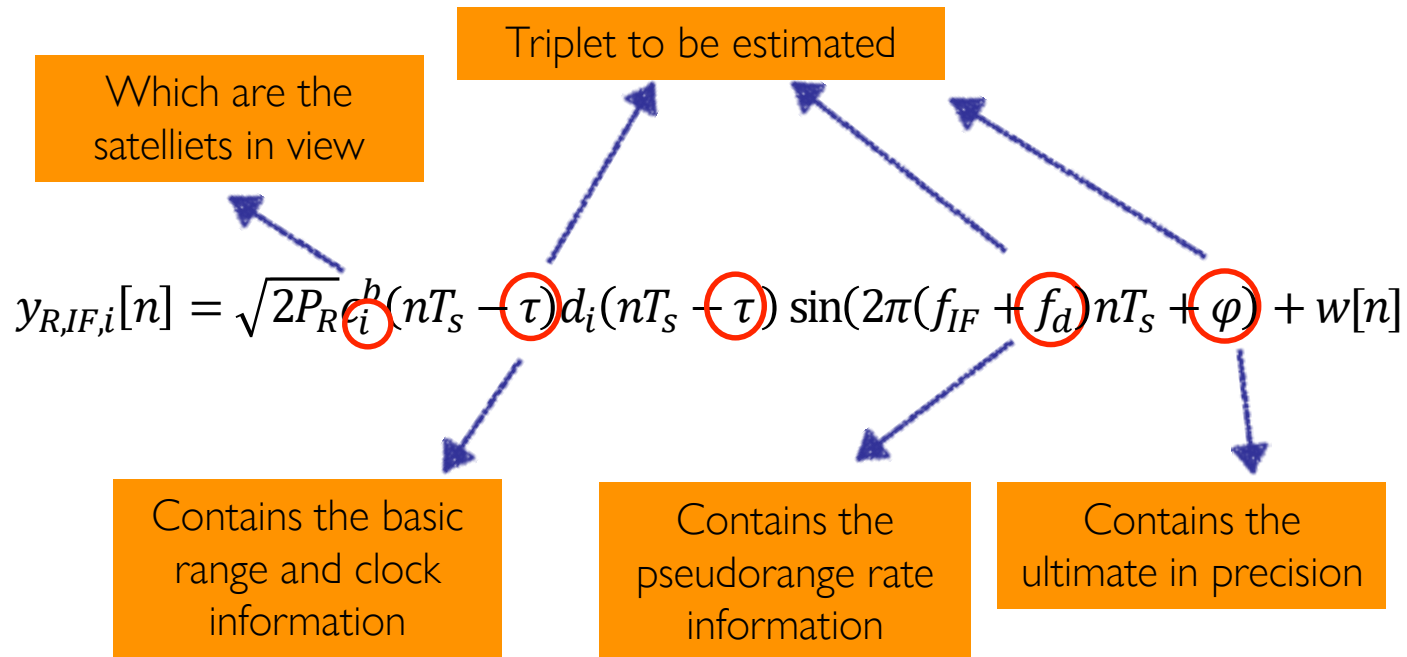
$$y_{R,RF,i}(t) = \sqrt{2P_R}c_i(t-\tau)d_i(t-\tau)\sin(2\pi(f_{RF}+f_d)t+\varphi)+\eta(t)$$

$$y_{R,IF,i}[n] = \sqrt{2P_R}c_i^b(nT_s-\tau)d_i(nT_s-\tau)\sin(2\pi(f_{IF}+f_d)nT_s+\varphi)+w[n]$$



Note: Single contribution from a single satellite i

PARAMETERS TO BE ESTIMATED



ACQUISITION & TRACKING

The synchronization procedure of the codes consists of two distinct steps:

Acquisition: initial rough estimate of the delay between the incoming code and the local replica and of the Doppler shift on the carrier

Tracking: keep the codes synchronized to dynamically recover the delay between sequences (fine alignment), refinement of the Doppler shift and of the phase

GNSS AND ANDROID

<http://gpsworld.com/google-opens-up-gnss-pseudoranges/>



<https://www.youtube.com/watch?v=vwGgSrGODU>

© 2014 Google LLC. All rights reserved.

COINS summer school - Jul 2019



<http://g.co/gnsstools>

Download and try!

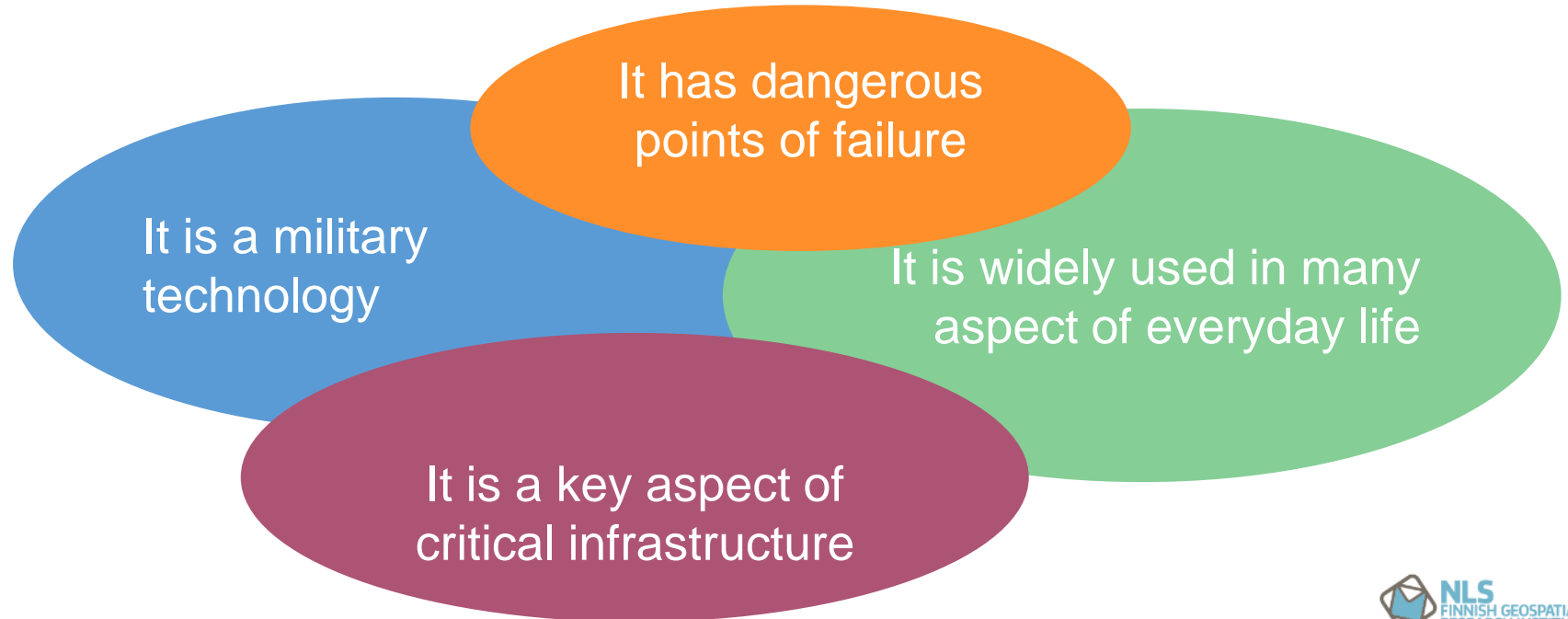


SECURITY BREACH

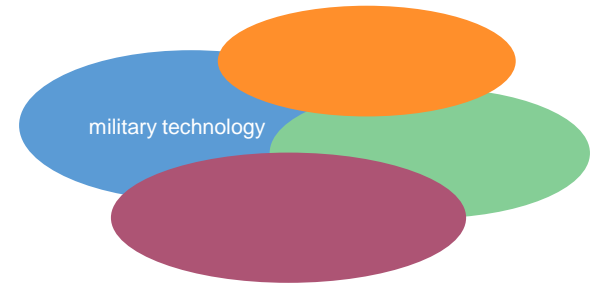
HACKING DETECTED

SECURITY ASPECTS

WHY THERE ARE IMPORTANT SECURITY CONCERNS IN GNSS?



MILITARY TECHNOLOGY



Open signals vs. military signals

GPS: P(Y) code, M code

Galileo: PRS (Public Regulated Service)

Encrypted, secret

Civilian systems vs. military systems

Galileo

All the others

GNSS CHANGE OF PERSPECTIVE

Original GPS purpose: military
(bombs, aircrafts, soldiers, sailors)

clear view of sky

1 minute start-up time

continuous operation

Today: civilian purposes

GNSS expected to work anywhere

push-to-fix application require instant fix

small, chip and low-power devices

automotive

aviation

agriculture

Railroads

boats and ships

sport

entertainment

Timing

dangerous works

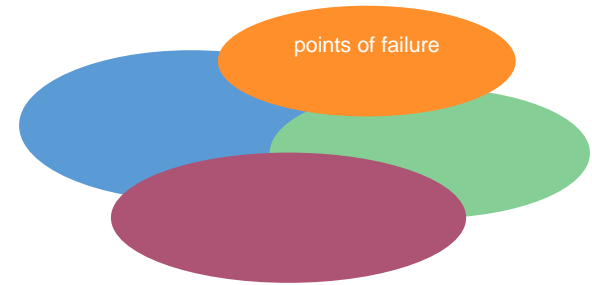
surveying, mapping

environmental protection

scientific research

Van Diggelen, F. S. T. (2009). *A-GPS: Assisted GPS, GNSS, and SBAS*. Artech House.

POINTS OF FAILURE



1. The received signal **power** is low, the signal is below the noise level
→ Jamming is easy, cheap and completely denies its usability
2. The GPS L1 **C/A code** was not originally designed to provide a positioning service.
3. It is simple, **open** and relatively easy to be deployed
4. It is a **space** technology: limited actions to modify it
→ Problems of Glonass orbits; problem of Galileo ephemeris (Jul 2019)

GNSS SIGNAL POWER

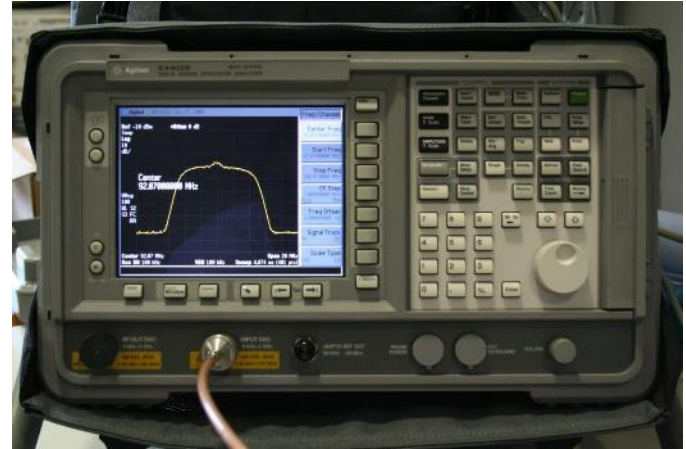
The **robustness** of GPS signal derives from the spread spectrum nature of the transmitted signal (DSSS, Direct Sequence Spread Spectrum)

Although the DSSS signal structure, navigation receivers are vulnerable to interfering signals, that might prevent the correct signal processing.

Received signal power extremely low:

Min. received power:

- GPS L1 C/A code: -158.5 dBW
- Galileo E1: -157dBW



No visible signal using conventional antennas and receiving hardware.

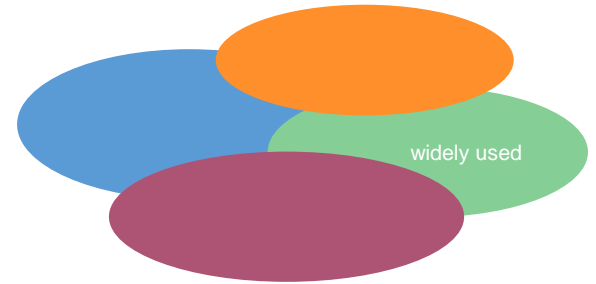
The lobe in the spectrum results from the combined signal power received by all the satellites in view.

BLOOMIGN MARKET

Widely used in many aspects of everyday life.

What would happen if GPS failed?

What about a second Carrington Event?



<https://geoawesomeness.com/what-would-happen-if-gps-failed/>

<https://www.theatlantic.com/technology/archive/2016/06/what-happens-if-gps-fails/486824/>

<https://www.newyorker.com/tech/annals-of-technology/what-would-happen-if-gps-failed>

CRITICAL INFRASTRUCTURES

Power grids

Oil pipeline transport networks

Water pipeline distribution networks

Telecommunications network

Railways transportation systems

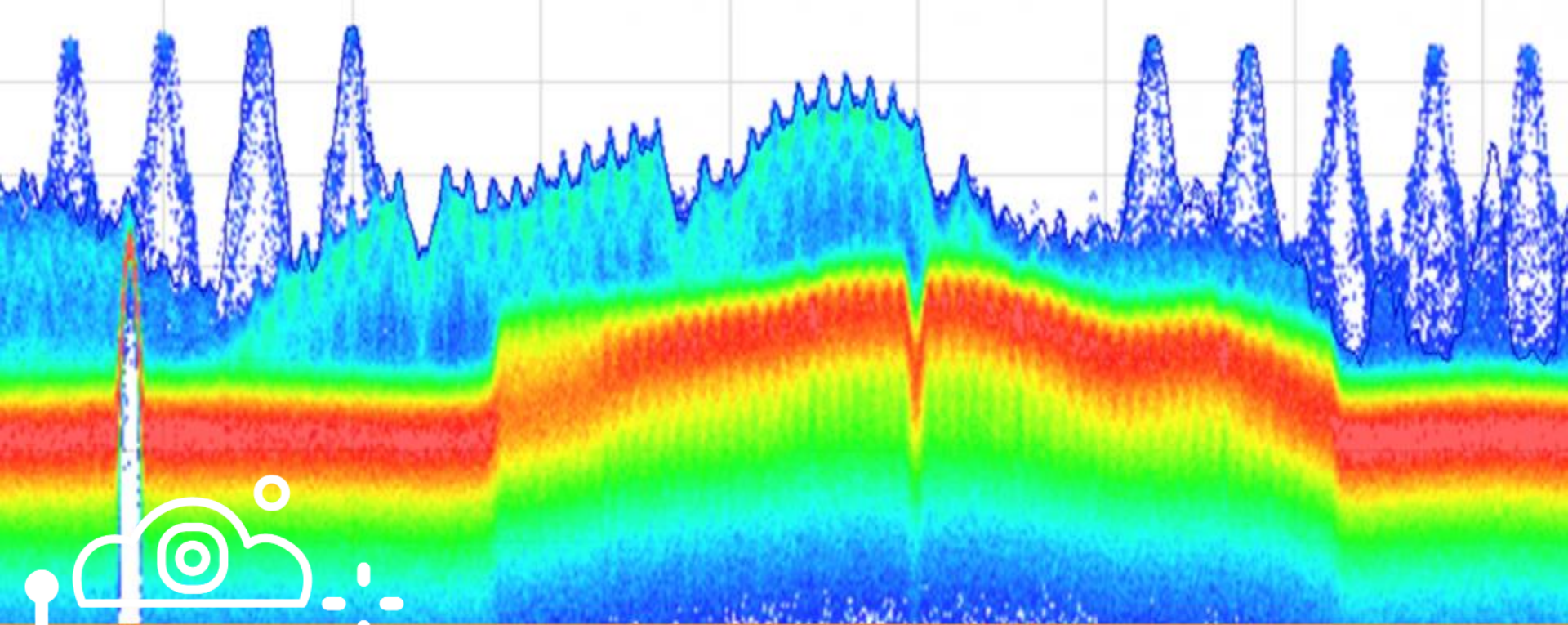
Maritime transportation systems

Air traffic control system

Financial networks



The electric power grid, as well as many other critical infrastructures, would literally collapse in case of a total, worldwide GNSS failure, mostly because of their dependency on an exact timing reference.



INTERFERENCE AND SPOOFING

SOURCES OF DEGRADATION OF GNSS SIGNALS

Artificial

EVIL WAVEFORMS

Distortions of the broadcast signal due to failures in the onboard satellite payload

RADIO FREQUENCY INTERFERENCE

Unintentional emissions of RF power in the GNSS frequencies

JAMMING and SPOOFING

Intentional emissions aimed at disrupting the GNSS service

Natural

MULTIPATH

Reflections of the received signal causing excess path and excess delay

IONOSPHERIC SCINTILLATIONS

Random phase and amplitude variations due to electron content gradients

SPREAD SPECTRUM AND INTERFERENCE

Spread Spectrum is robust to the presence of interfering signals

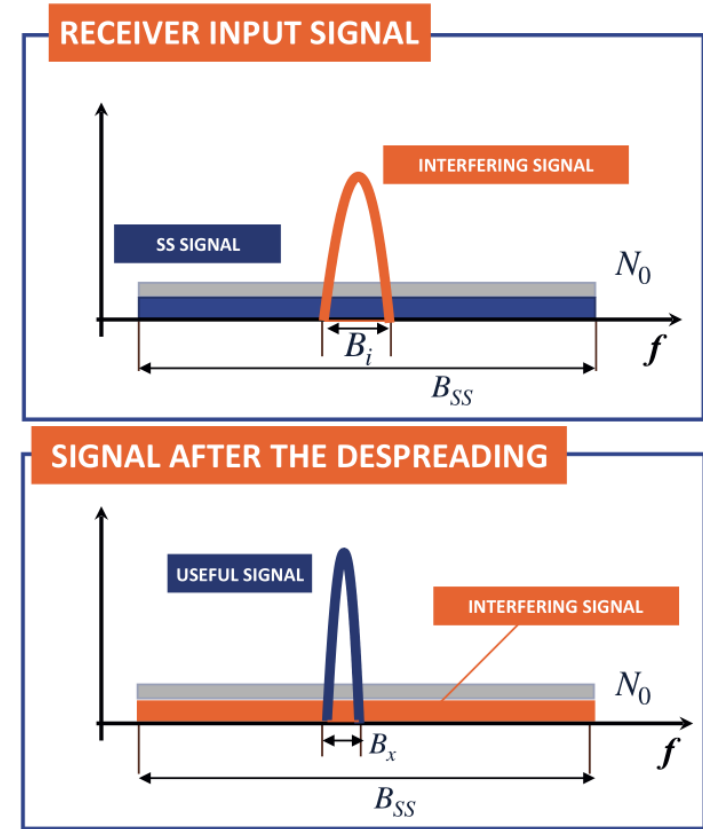
The product with the PRN code **spreads the power** over a larger bandwidth

$$B_x \rightarrow B_{SS}$$

If an interference of bandwidth affects the signal, only a portion of the power will be actually received as “additional noise”

The despreading operation made at the receiver spreads the power of the interfering signal over a wide bandwidth

F. Dovis, Recent trends in Interference Mitigation and Spoofing Detection, ICL-GNSS 2011

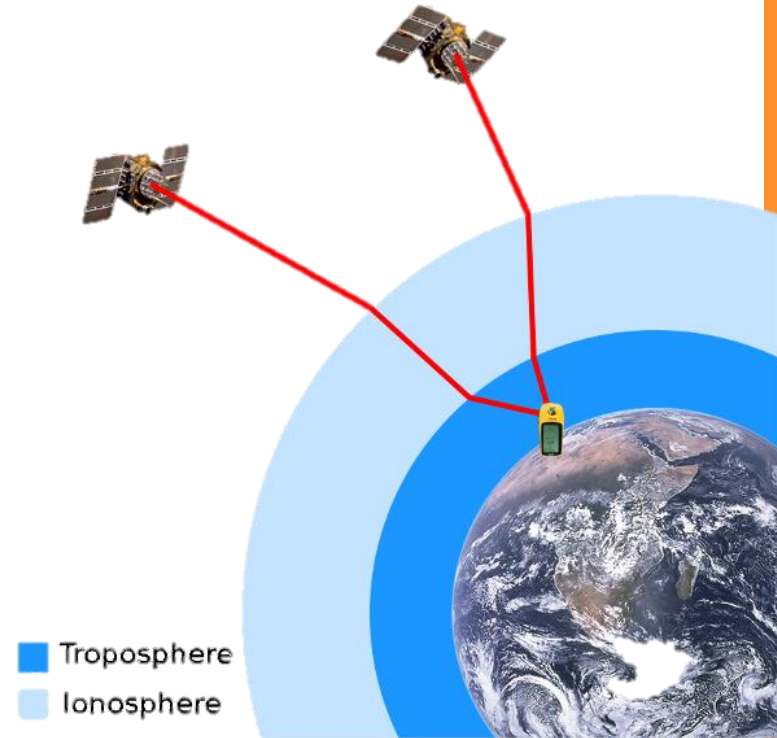


IONOSPHERE AS A NATURAL THREAT TO GNSS

If not modeled sufficiently well, the Earth atmosphere is the largest contribution of error in GNSS receivers

- Especially ionosphere
- GNSS signals are trans-ionospheric signals
- In particular single frequency GNSS receivers

Linty, N., DAVIS, F., & ALFONSI, L. (2018). Software-defined radio technology for GNSS scintillation analysis: bring Antarctica to the lab. *GPS Solutions*, 22(4), 96.



Source: commons.wikimedia.org

IONOSPHERIC SCINTILLATIONS

Ionospheric scintillations are produced by ionospheric **irregularities**

Transionospheric radio waves are scattered by the irregularities and interfere with each other constructively and destructively

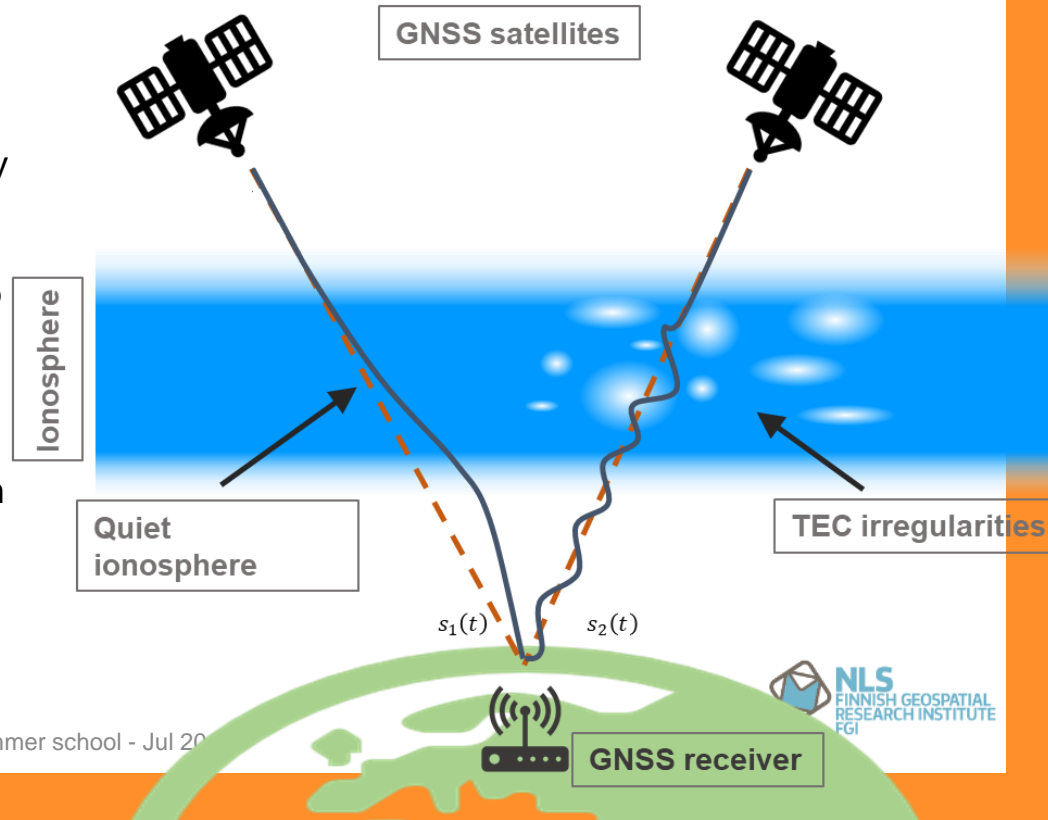
Consequently, GNSS signals experience deep signal fading and random phase fluctuations

Amplitude scintillations

Phase scintillations

Scintillation is a form of space based multipath

Planar radio waves strike a volume of irregularities and emerge with varying amplitude and phase



GEOMAGNETIC ANOMALIES

Less intense fades experienced near the magnetic equator and immediately north and south of the anomaly regions

Equatorial Ionospheric Anomaly (EIA)
approximately 15° north and south of the magnetic equator

South Atlantic Magnetic Anomaly (SAMA)
geomagnetic equator deviates sharply from the geographic equator

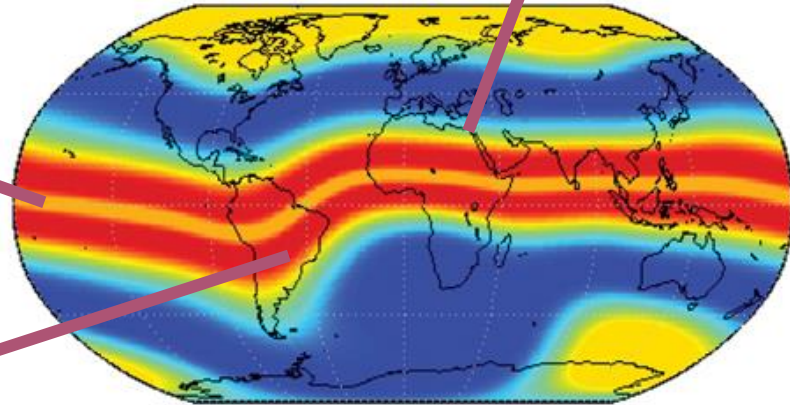


Image source: P. M. Kintner, T. Humphreys, and J. Hinks, "GNSS and ionospheric scintillation," Inside GNSS, vol. 4, no. 4, pp. 22–30, 2009.

RFI

Radio frequency interference
Electromagnetic radiation disturbing GNSS
receivers operations

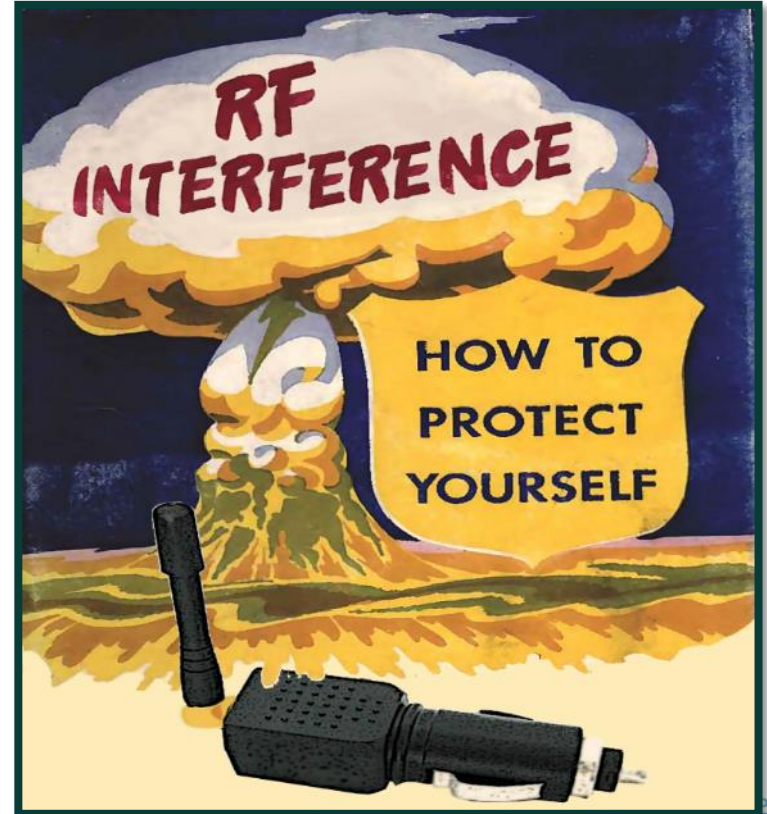
Impact on the receiver

Measurements degradation, increased
variance and biases

Discontinuous operations (losses of lock)

Complete outage (no navigation solution)

Adrian Graham. Communications, "Radar and
Electronic Warfare"
John Wiley & Sons, January 2011



INTENTIONAL VS UNINTENTIONAL

Unintentional

Usually from faulty electronics, secondary or out-of-bands harmonics (DVB-T), spurious components

Unintentional interference events can be unpredictable

Jan 2007, San Diego (CA): training exercise of 3 navy ships, 3 days of blackout

2010, Newark airport: LAAS and air control system jammed by a truck driver personal privacy device

2011: Lightsquared

2006, Sydney: UHF harmonics in TV antennas induce anomalous AGC behaviour

Intentional:

Not only related to military contest, new attention for commercial and security oriented GNSS applications

jamming, spoofing, meaconing



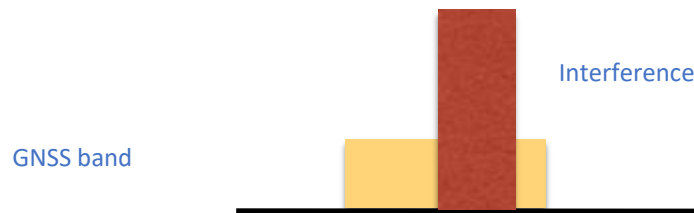
INTERFERENCE CLASSIFICATION

Out-of-band Interference: interference carrier frequency close to the GNSS band



Theoretically it should not affect the GNSS signals, but if in close bandwidths and high power, it can create issues for the front-end (e.g. due to the non perfect selectivity of the filters)

In-Band Interference: interference carrier frequency within the GNSS frequency band



Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Artech House.

INTERFERENCE SPECTRAL FEATURES

Interference can be further classified according to the spectral and time features w.r.t. the GNSS signal

Narrow Band interference

$$B_{int} \ll B_{GNSS}$$

Wide Band Interference

$$B_{int} \sim B_{GNSS}$$

Continuos-wave (CW) Interference: single pure tone

$$B_{int} \rightarrow 0$$

Pulsed Interference

Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Artech House.

UNINTENTIONAL INTERFERENCE

Spurious emissions from components located by the antenna (multi-system integrated solutions, cell phones, etc)

Interference from malfunctioning systems

Since E5/L5 are wide-band signals, the narrow-band interference have less impact on E5/L5 than on the L1 signals

L1

Second and third harmonics of some television channels
DVB-T
10th harmonics from VHF communication channels
12th and 13th harmonics of aviation communications at 131 and 121 MHz

L2

Military radars: ARSR-4 (1215-1400 MHz)
Amateur radio (1215-1300 MHz)
Military radars: SPS-49 (1215-1400 MHz)
Share band with ATC and military radars

L5/E5

ARNS band without exclusivity to RNSS
TACAN (960-1215 MHz), Pulsed interference
DME (962-1213 MHz), Pulsed interference
JTIDS/MIDS (969-1206), Pulsed interference

INTRA-SYSTEM INTERFERENCE

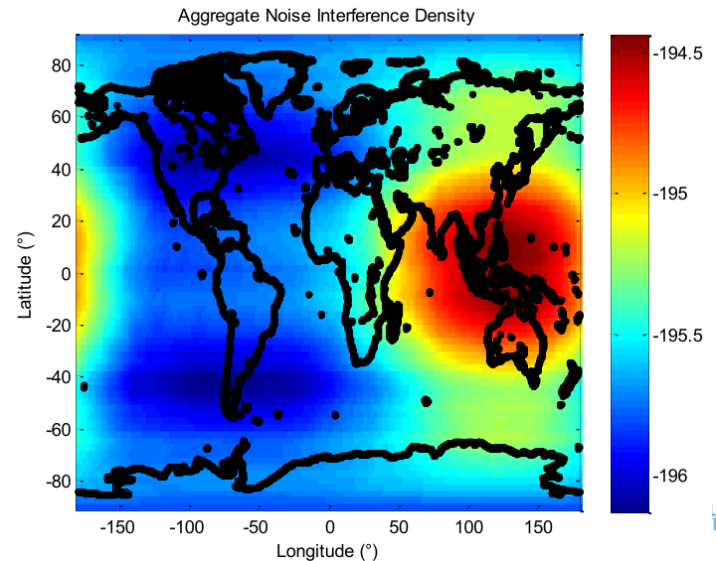
All future GNSS systems (+ SBAS) will broadcast 1 to 5 signal in the L1 band
close to around **50 visible satellites** in the worst case

This type of interference usually creates background noise (no receivers working at low C/N_0)

It is expected that this kind of interference dominates thermal noise as more satellites are launched

Typical approximated
representation of expected worst
case inter- and intra-system
interference in 2025

Dovis F., "Interference and spoofing", lecture notes, NavSAS, Politecnico di Torino



INTENTIONAL INTERFERENCE

The objective is **denial of navigation service**

Signal radiation on the GNSS bands is **not legal!**

3 types of attack:

- Jamming
- Meaconing
- Spoofing

Severe threat for liability-critical mass-market applications, such as GNSS-based road tolling or fleet management

Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Artech House.

JAMMING

Some definitions

The act of intentionally directing electromagnetic energy towards a communication (and navigation) system to disrupt or prevent signal transmission/reception, by masking GPS signals with **noise**.

Jamming is all about getting sufficient energy into the victim receiver at the right time and in the right place.

By raising the equivalent noise PSD level, the equivalent received C/N_0 goes below the acquisition/tracking thresholds.

Intentional transmission of radio frequency signals that can interfere with GNSS signals leading to a degradation or blocking of GNSS navigation and timing services

Under jamming attack the victim receiver is unable to acquire and process navigation signals.

But jamming is **easily detectable**

JAMMERS ARE ILLEGAL!

The GNSS bandwidth is protected. It is forbidden to transmit anything.

The use of jammers is forbidden.

The possession of jammers... no!

Review of jammers...

Author: PatrickMiles November 27, 2012

Quality: ★★★★★

I like that jammer because it is simple. You don't have to be a rocket scientist if you want to use it. Nothing special is here, just plug it in and it is done. Another thing I like about this small gadget is that it has precisely calculated output signal power so it never comes out of my car and that is just perfect because nobody can spot and track that jammer.

Author: AndyDecker November 7, 2012

Quality: ★★★★★

I'm a truck driver and I'm working with one company for almost four years and we've trusted each other. I hauled their cargo and everything was ok, until they have decided to install a tracker in my lorry. I was really angry and I've decided to protect my privacy myself. Now I just plug that thing in my car lighter slot and enjoy my ride!

Author: Stewie October 2, 2012

Quality: ★★★★★

I'm using this GPS jammer for almost a month. I like it, it jams GPS and leaves everything else untouched, exactly what I needed. With it I'm sure I won't be tracked, and it fits my budget!

The screenshot shows the Jammer website interface. At the top, there's a navigation bar with categories: CELL PHONE JAMMERS, GPS JAMMERS, BLUETOOTH JAMMERS, WIFI JAMMERS, SPY CAR JAMMERS, and HIGH POWER JAMMERS. Below this, there are three featured products:

- Portable GSM/WiFi Bluetooth 3G Jammer**: 15 meters radius, priced at \$319.99.
- GSM, GPS, CDMA, 3G Jammer**: 10 meters radius, priced at \$279.99.
- Desktop Powerful GSM, GPS, CDMA, 3G Jammers**: priced at \$349.99.

Each product has a 'Click here' link. To the right of these products are three promotional boxes: 'Free Worldwide shipping', '14 day money back guarantee', and 'Keep your tracking'. Below the featured products is a category list on the left and a detailed product listing for the 'GP6000 Car use GPS jammer, GPS blocker, tracking jammer' on the right. The GP6000 listing shows a price of \$129.00, shipping costs, product number GP-5000, and an 'ADD TO CART' button.

JAMMING AS PRIVACY PROTECTION

Why jamming?

To prevent your **enemy's**
receiver to work properly

from **electronic
warfare** to **privacy
protection**

To prevent **your** receiver to
work properly/to track you



Jammers often seen as
PPD: Personal Protection Device

MEACONING

Interception and rebroadcast, with a delay, of an entire block of RF spectrum including the real GNSS signal
Typically with **higher power** in order to cover the true signal

Consequences on a GNSS receiver:

If the receiver only tracks the signal from the meaconer:

- The position estimated by the target receiver is the position of the meaconer
- The constant delay added to each measurements will impact the clock estimation

If only part of the meaconer's signals are tracked by the receiver

- Inconsistency of the pseudoranges

Difficult to counteract

- at receiver level time consistency must be cross-checked for detection. Very difficult for near-zero delays
- at signal level a time dependent encryption should be implemented to increase the robustness

MEACONING TECHNOLOGY

Simple to perform (no knowledge required)

Unsynchronized meaconing ($e > 100$ ns)

→ Medium cost: COTS record-and-replay device (<5000\$) + amplifier + transmitting front-end

Synchronized meaconing ($e < 100$ ns)

→ Low cost: RX antenna + amplifier + TX antenna

SPOOFING

Intentional malicious transmission of counterfeit fake GNSS-like signals intended to force the victim receiver to compute **erroneous positions** and lead the users to believe they are in a different location or (or at a different time) from where they effectively are.

The victim receiver track the counterfeit signals instead of the true signals

Attacks can be very effective depending on the quality of the generated signal

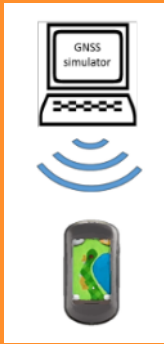
It has always been present in the military field, but with the extensive use of GNSS it may threaten several applications

The present technology allows for the implementation of spoofers also at a reasonable cost

Spoofing attacks are **the major threat** for future civilian GNSS applications

TYPES OF SPOOFING ATTACKS

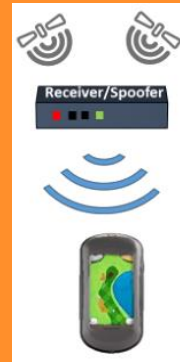
Simplistic



signals not consistent with the satellites signals
HW GNSS signal generator
high cost and easily detectable

CC BY-NC-SA N. Linty

Intermediate



signals consistent with the satellites signals
requires a GNSS receiver
lower cost and more difficult to detect

COINS summer school - Jul 2019

Sophisticated



signals consistent with the satellites signals
requires GNSS receiver and multiple transmitting antennas
high implementation complexity

430

SIMPLISTIC ATTACK

Principle:

- Generation of counterfeit GNSS-like simulated signals.
- The counterfeit signals are unsynchronized with the authentic GNSS signals.

Technology:

- Simple to perform
- Medium to low cost GPS signal generator, a power amplifier and a RF transmitting front-end

Approaches to defeat the receiver:

- Direct spoofing (hoping that it may cause the victim receiver to lose lock and undergo a partial to complete reacquisition of the fake signals)
- Jam and spoof: first jam to force the receiver to lose lock, then spoof to capture the receiver on the spoofing signals

Impact on the receiver

- Inconsistency of processed signals



INTERMEDIATE ATTACK

Principle

- The spoofer generates counterfeit signals that are aligned with the genuine/true GPS signals (at the target antenna)
- Increase of the power of the counterfeit signals to dominate the true signals and catch the tracking loops
- Position is then dragged-off.

Attack with a receiver-spoofers

- the spoofer is placed inconspicuously near the target receiver's antenna, in the same vehicle it can estimate the position and the velocity of the vehicle with the receiver component (must avoid self spoofing) so that it can generate a coherent counterfeit signal



INTERMEDIATE ATTACK

Impact on the targeted GPS receiver

If the receiver only tracks the signal from the spoofer:

- The receiver reports the counterfeit position
- Receiver clock state might be affected
- User velocity might be affected

If only part of the spoofer's signals are tracked by the receiver

- Inconsistency of the measurements

Impact on the non-targeted GPS receivers

Same as the simplistic spoofing attack for GPS receivers located far enough from the targeted receiver

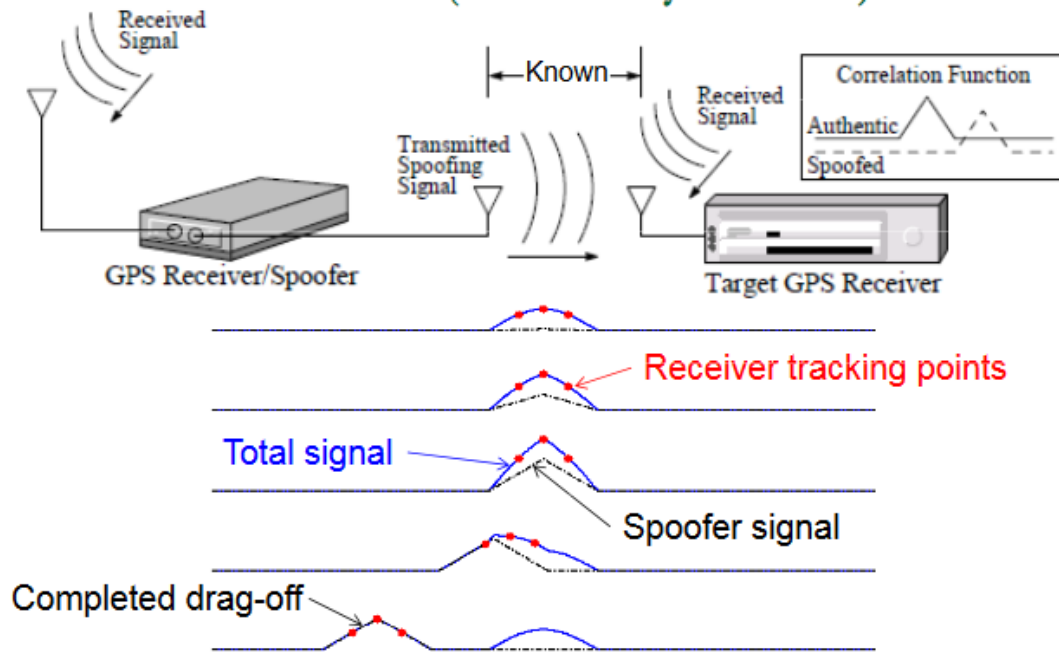
Technology

Low-cost hardware

Sophisticated software in the spoofer

Attack at a distance is complicated

INTERMEDIATE SPOOFING ATTACK



SOPHISTICATED ATTACK

Principle

A network of coordinated intermediate spoofers replicates the content and mutual alignment of visible signals and their spatial distributions

- To defeat antenna arrays
- Multiple phase-locked portable receiver-spoofers (intermediate spoofers) are mandatory

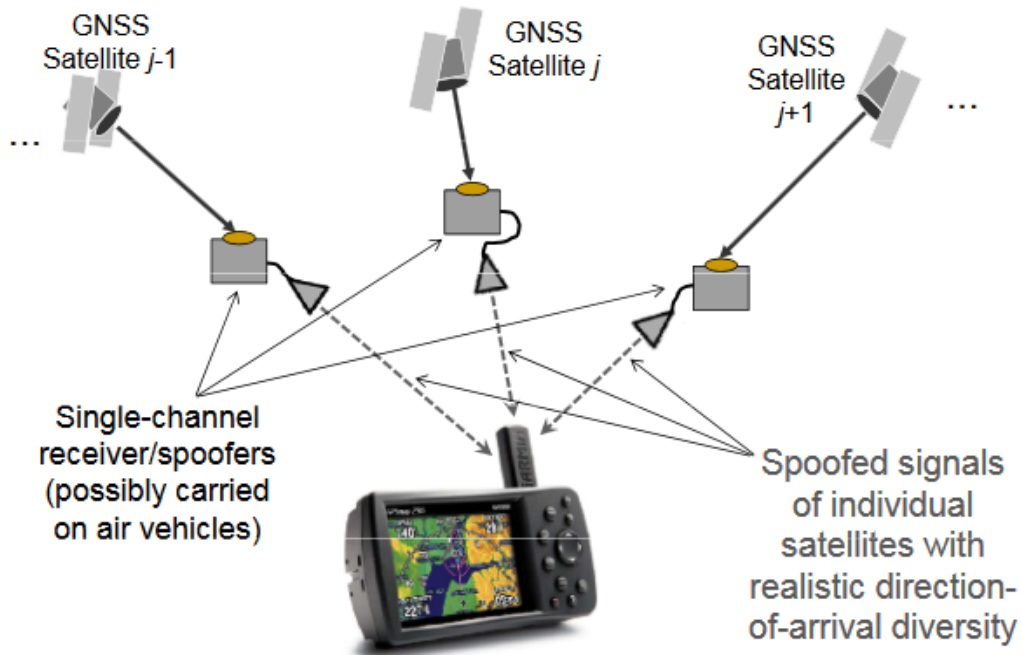
Requires sub-centimeter-level knowledge of the position and velocity of the target receiver antenna phase center

Most complex spoofing category

- Very high cost and complexity

No open literature has reported any sophisticated attack

SOPHISTICATED ATTACK



Psiaki, techniques for Spoofing and Spoofing Mitigation, ITSNT2015

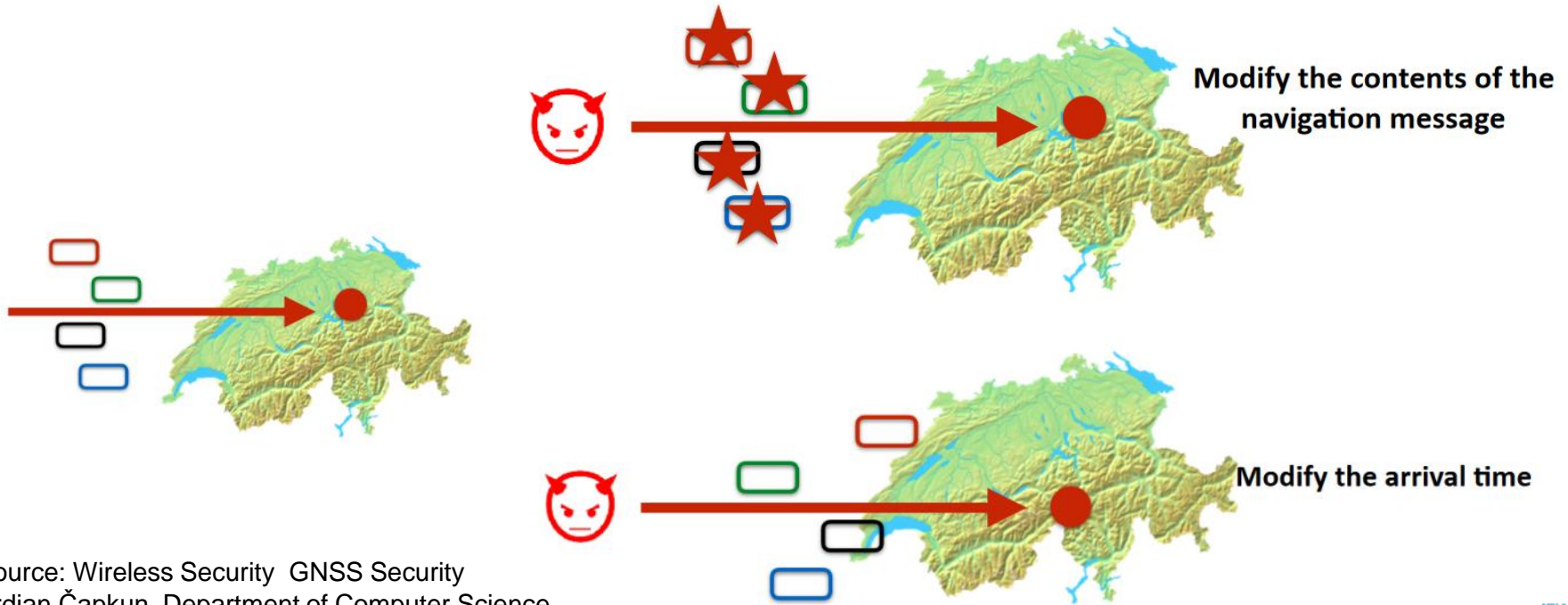
CORRELATION DISTORTION

During spoofing attacks, false signals align in frequency and time to the real ones.

This produces a distortion of the correlation, similar to that produced by a strong multipath, forcing the tracking loop to lose the lock on the real signal and to lock on the false one.

Jam&Spoof: first jam to force the receiver to lose lock, then spoof to capture the receiver on the spoofing signals

PICTORIAL EXAMPLE



Source: Wireless Security GNSS Security
Srdjan Čapkun, Department of Computer Science
ETH Zurich, Switzerland

CC BY-NC-SA N. Linty

COINS summer school - Jul 2019

137

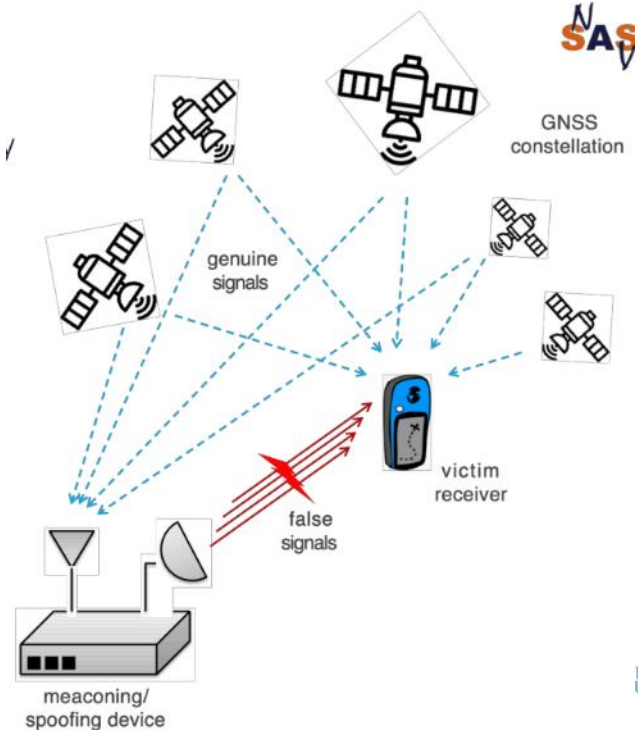
SPOOFING VS JAMMING

Spoofing is more malicious than intentional interference and jamming:

the false signals take control of the target receiver and the victim is fooled without any notice

“Better have a deny of service than a fake position”

D. Margaria et al., Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives (2017) IEEE Signal Processing Magazine, 34 (5)



GROWING JAMMING AND SPOOFING MENACES

Potential threats and major concerns for liability-critical and payment-critical applications

“Denial-of-service” attacks, simply based on intentional interference (jamming)

Information about the user’s position or velocity is used at the basis for legal decisions or economic transactions, such as:

- Road User Charging
- Pay-As-You-Drive insurances
- commercially-sensitive LBS
- mobile payments
- geographic Digital Rights Management
- on-line gambling.
- Safety-critical applications (e.g. ADAS, eCall)

COUNTERMEASURES

Detection:

Process of revealing the presence of interference





It is an hypothesis testing problem

Detection makes sense only if interference is harmful!

Mitigation:

Processing of reducing the interference impact

It is an estimation problem

INTERFERENCE	harmful	not harmful
detected		
not detected		

INTERFERENCE DETECTION AND MITIGATION

Classical countermeasures to interference are classified as

Time-domain techniques: based on the modification of the receiver parameters, or on signal “gating”, to cut-off portions affected by interference

Frequency-domain techniques: based on the characteristics of the spectrum of the interfered GNSS received signal

Time-space techniques: based on spatial filtering; require complex hardware configuration and antenna arrays

...

- C/N_0 monitoring
- Correlation function distortion
- Power Spectra Assessment
- ADC/AGC monitoring
- Doppler change
- Receiver clock jump
- Inconsistency check
- RAIM
- Authentication
- Post-correlation statistical analysis
- Pseudorange monitoring
- PVT solution observation
- Antenna array/angle of arrival
- Independent clock
- Consistency with other sensors
- ...

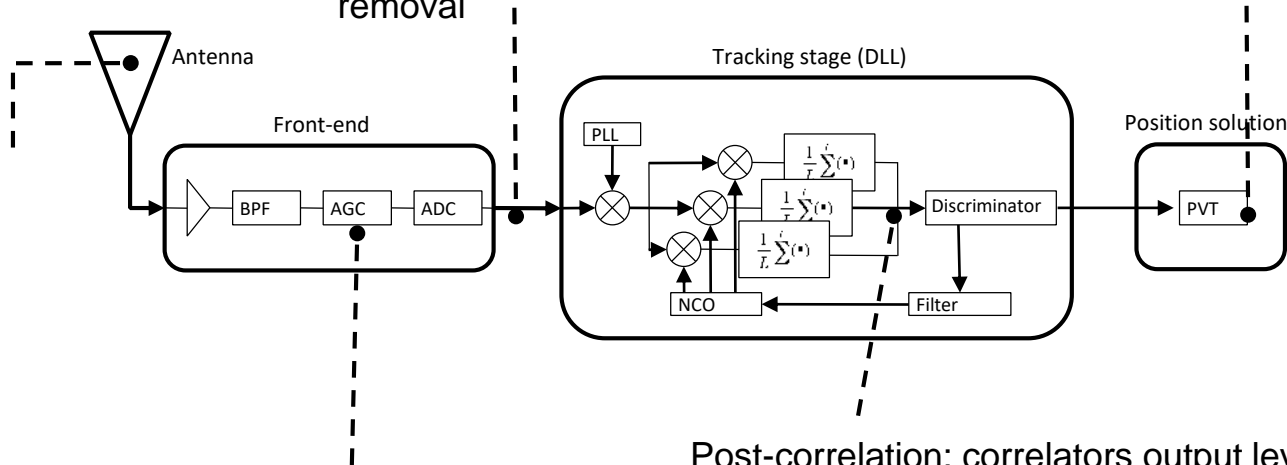
GNSS INTERFERENCE MITIGATION

Pre-correlation: Raw signal samples after ADC

- Notch filter, for CW removal
- Pulse blanking, for pulsed interference removal

Measurements level

Antenna:
 - Beamforming,
 - diversity processing,
 - Null steering (antenna array)



Exploiting properties of the Automatic Gain Control (AGC) and Analog-to-Digital Converter (ADC)

Post-correlation: correlators output level

- C/N_0 monitoring
-



EXAMPLES

INTERFERENCE FROM DVB-T AND ANALOG TV

In the broadcast TV signal, VHF and UHF bands are used. Both bands, in their sub channels, could represent interferences sources for a GNSS receiver.

Real Case: secondary harmonics from DVB-T might fall in the bands of interest:

Torino Eremo, RAI

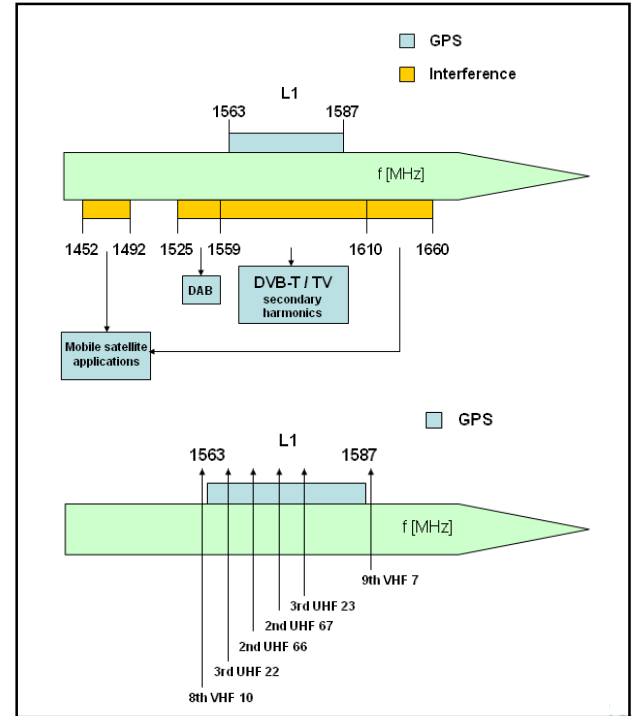
DVB-T Channel 28 and 66

modulation: 16 QAM for Ch 28 and 64 QAM for Ch 66

ERP: 200 W for Ch 28 and 3000 W for Ch (66)

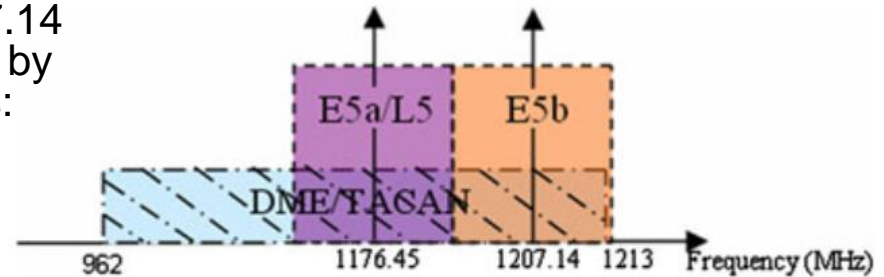
Central frequency: 530 MHz for Ch 28 and 834 MHz for Ch 66

Motella, B., Pini, M. & Dovis, F. GPS Solut (2008) 12: 77.
<https://doi.org/10.1007/s10291-007-0085-5>



DME/TACAN INTERFERENCE IN E5

E5 and L5 signals at 1176.45 MHz and 1207.14 MHz are exposed to RF **pulse interference** by existing aeronautical system pulsed emitters:
Distance Measuring Equipment (DME)
Tactical Air Navigation (TACAN)



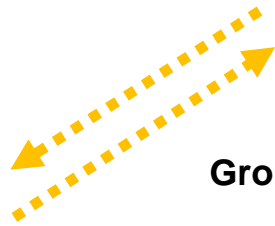
DME provides distance measurement between aircraft and a ground station.

Interrogation based on pulse pair sequence transmission towards the ground

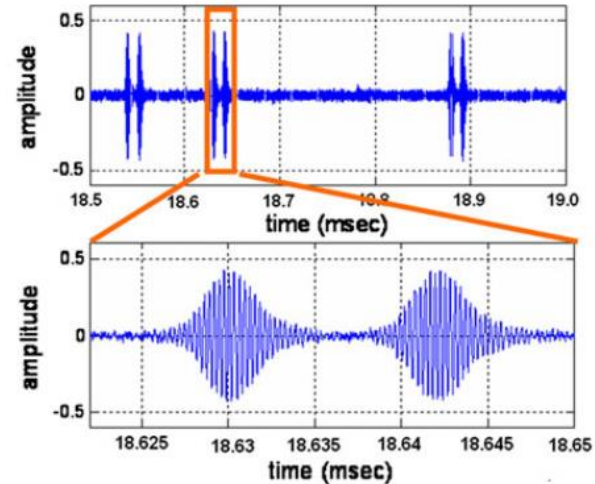
Replies are the same pulse pair sequence delayed of 50 μ s

PULSED INTERFERENCE

Airborne
interrogator



Ground beacon



Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Artech House.

Grace Xingxin Gao et al. DME/TACAN interference mitigation for GNSS: algorithms and flight test results, GPS SOLUTIONS, 2012, 10.1007/s10291-012-0301-9

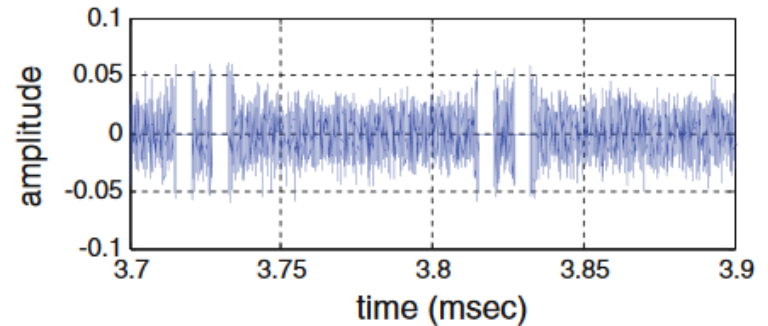
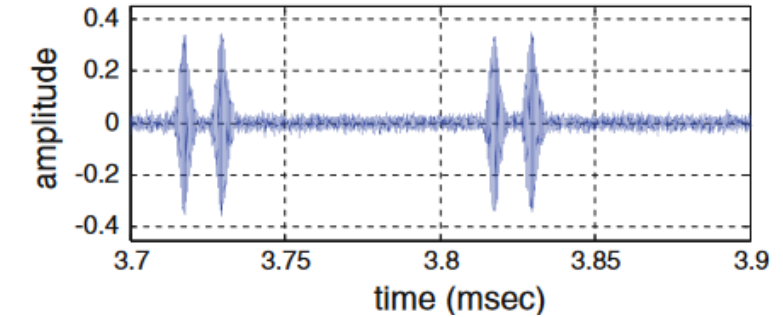
DME pulses are pairs of Gaussian pulses with pulse width of $3.5 \mu\text{s}$ and inter-pulse interval of $12 \mu\text{s}$

MITIGATION THROUGH PULSE BLANKING

Pulse banking

Advanced time-frequency mitigation

Transformed domain mitigation



Dovis, F. (2015). GNSS Interference Threats and Countermeasures. Artech House.



GNSS JAMMING

Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.

Figure credits: C4ADS report



NORTH KOREA

April 1, 2016

According to South Korean officials,
near the borders

110 planes and ships affected

70 fishing vessels had been forced
to return to port after GPS navigation issues



<https://www.bbc.com/news/world-asia-35940542>

<https://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html>

THE NATO DRILL

Norway, November, 2018

NATO's largest military exercise since the Cold War

“Norway has determined that Russia was responsible for jamming GPS signals in the Kola Peninsula during Exercise Trident Juncture”
NATO spokesperson Oana Lungescu

“It is possible that Russia has been the disrupting party in this. Russia is known to possess such capabilities.”
Finland's Prime Minister Juha Sipilä.

Norway-based airline pilots were reporting the loss of GPS signals when flying to airports in northern Norway

<https://www.bbc.com/news/world-europe-46178940>

<https://www.gpsworld.com/norway-finland-suspect-russia-of-jamming-gps/>

<https://insidegnss.com/russia-jammed-gps-signals-during-nato-military-exercise-involving-us-troops/>



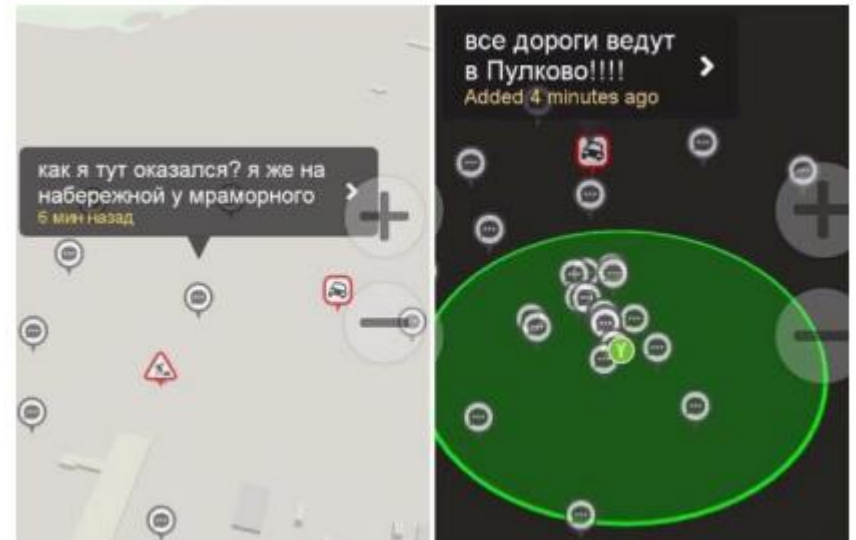
RUSSIA AND SPOOFING

Reported in press already 27 December 2016

Car drivers experience “strange problems” in St Petersburg

Car Sat navigation systems show location near Pulkovo airport when they are actually in city centre

Credits: W. De Wilde, J-M. Sleewaegen, Septentrio



PUTIN IN A GNSS BUBBLE

Close correlation between movements of the Russian head of state and GNSS spoofing events

“Russia regularly demonstrates that GNSS jamming and spoofing can be a useful tool for internal security and an effective method of power projection”



<https://www.bbc.com/news/technology-47786248>

<https://www.wired.co.uk/article/russia-gps-spoofing>

<https://www.gpsworld.com/jammers-at-dachas-add-to-russias-ability-to-silence-gps/>

COMMERCIAL AVIATION

Since 2013, over **90 incidents** of GPS jamming reported by pilots through NASA's Aviation Safety Reporting System (ASRS) since 2013

- Clark Regional Airport: Android tablet frozen showing the aircraft approx. 10 nm to NW of JV. The PIC visually identified what he mistakenly thought was JYV and proceeded to fly Southbound towards the field.
- Complete GPS loss of signal as we crossed the coast in point to RPLL (Manila). Signal was lost for remainder of flight.
- Mexico City: several reports of GPS receiver outages whilst on final approach to the international airport. thought to be caused by jamming
- ...

Source: GNSS Threats, Attacks and Simulations, Guy Buesnel and Mark Holbrow, PNT Advisory Board, Baltimore, 28-29 June 2017

SALT LAKE CITY

July 8, 2019

A passenger aircraft flew off course during a period of GPS jamming and nearly crashed into a mountain

“Had the Radar Controller not noticed, that flight crew and the passengers would be dead”.

NASA report: Passenger aircraft nearly crashes due GPS disruption

July 8, 2019 - By Dana Goward

0 Comments

Est. reading time: 1 minute



Photo: IlkerErgun/Shutterstock.com



<https://www.gpsworld.com/nasa-report-passenger-aircraft-nearly-crashes-due-gps-disruption/>

PHILADELPHIA AIRPORT

2015

Philadelphia North East Airport

Pilots flying to the Northeast Philadelphia Airport kept reporting losing their GPS navigational signals as they approached the runway.

FCC Agents detected a GPS jammer operating in a nearby car park and causing intermittent jamming of a GPS approach procedure.

The truck driver said that he was using a GPS jammer to disable a tracking device in his vehicle, and that he hadn't realized the jammer was illegal

NEWARK AIRPORT

Aug. 4, 2012, Newark Liberty International Airport

Investigator from the FCC's enforcement division, using radio monitoring equipment, located a pickup on airport property that was emanating signals within **GBAS frequency band**.

"The signals emanating from the vehicle were blocking the reception of GPS signals used by the air traffic control system"

"He claimed that he installed and operated the jamming device in his company-supplied vehicle to block the GPS system that his employer installed in the vehicle," the FCC decision stated.

N.J. man fined \$32K for illegal GPS device that disrupted Newark airport system

Posted Aug 8, 2013



The FCC said an aircraft tracking system at Newark Liberty International Airport experienced interference from a GPS jamming device used by a Readington man who claimed he was simply trying to hide his whereabouts from his employer. The FCC fined the driver \$31,875.



https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html

<https://insidegnss.com/fcc-fines-operator-of-gps-jammer-that-affected-newark-airport-gbas/>

WASHINGTON DC



Surprising used of jammers.

While he was at the Washington Hilton in D.C. for the security conference Shmoocon in January, Gostomelsky's station picked up on GPS interference in the area. Gostomelsky mounted the 20 pounds of hardware on his back and tracked the signal to a high school gym, inside of which kids were flying drones.

After someone landed a drone on the White House lawn in 2015, drone manufacturers like DJI began programming their flying machines to refuse to operate if they were in a “no drone zone” with a 30 mile radius around D.C.

The kids apparently used a jammer to trick their drones into assuming they were outside the nation's capital.



<https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955>
<https://forum.dji.com/thread-42423-1-1.html>

HIGHWAY GANTRIES

Multi-antenna GNSS receiver with built-in RF spectrum monitor and adequate processing tool to efficiently detect and classify jamming events and identify the offending car or truck.

Two Septentrio AsteRx-U dual-antenna receivers installed on an overhead structure above a busy **highway**

Possibility to perform lane detection by cross-correlating the jamming signal received by the two antennas and driving direction

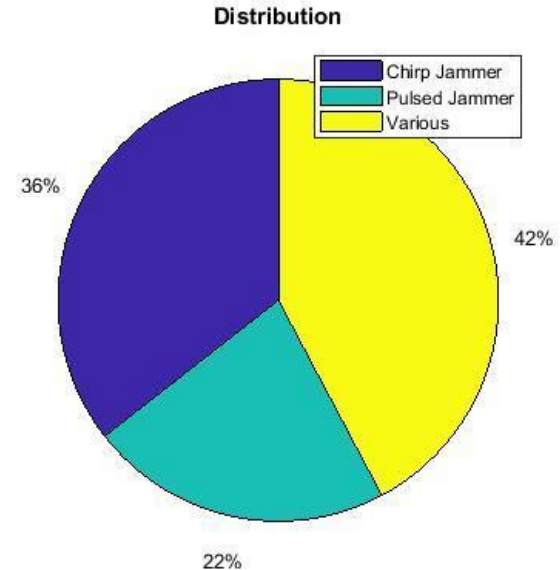
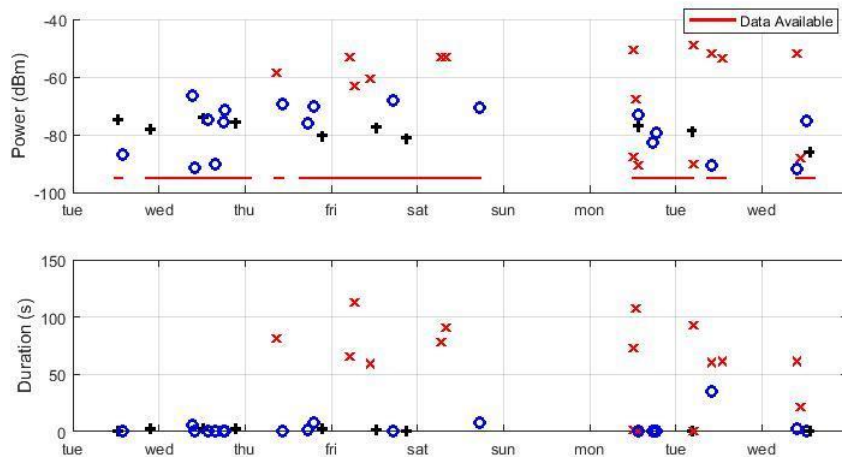


<https://www.gpsworld.com/highway-gantries-identify-jammers/>

RESULTS

Over five days of experiment, **45 jamming events** were recorded and analyzed, most of them intentional: continuous wave, chirp or even less-known pulse jammers

Pattern recognition to distinguish between intentional harmful events and unintentional interferences



Wim De Wilde et al., "Authentication by Polarization: A Powerful Anti-Spoofing Method," Proceedings of ION GNSS+ 2018, Miami, Florida, September 2018, pp. 3643-3658.

<https://doi.org/10.33012/2018.15917>

Wim De Wilde, J.-M. Sleewaegen, "Effective Jammer Detection and Classification using GNSS Receivers on a Highway Overhead Structure," Proceedings of ION GNSS+ 2018, Miami, Florida, September 2018, <https://doi.org/10.33012/2018.16005>

OCCURRENCE OF JAMMING

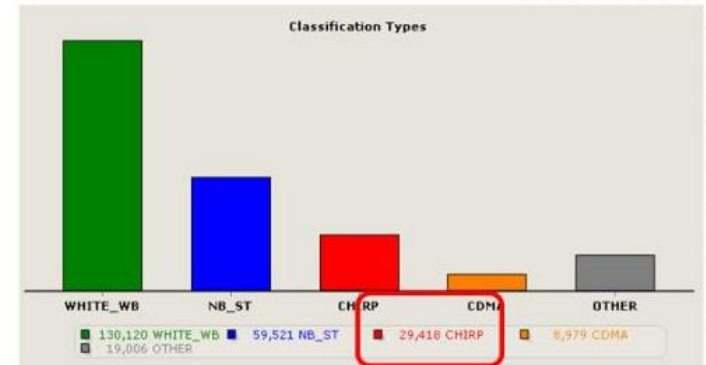
Monitoring during 21 months (Feb 16 to Oct 17)

Most were low power, short duration, wideband. No impact

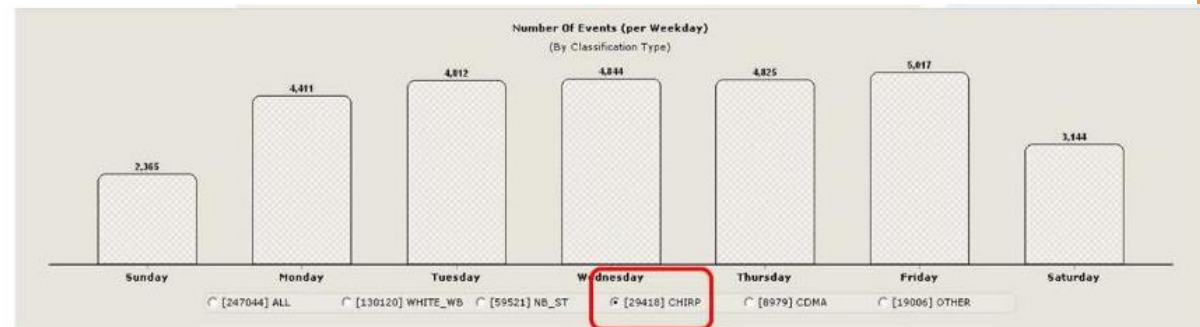
30000 chirp interference from PPD/jammers

Pattern follows working week/hours

Non doubt that this is man-made interference



Ignacio Fernández Hernández, Resilient
Position, Navigation and Timing, ITSNT –
Toulouse, 17 Nov 2017



GNSS SPOOFING

Spoofer mimics authentic GNSS satellites to hijack GNSS receiver tracking loops.

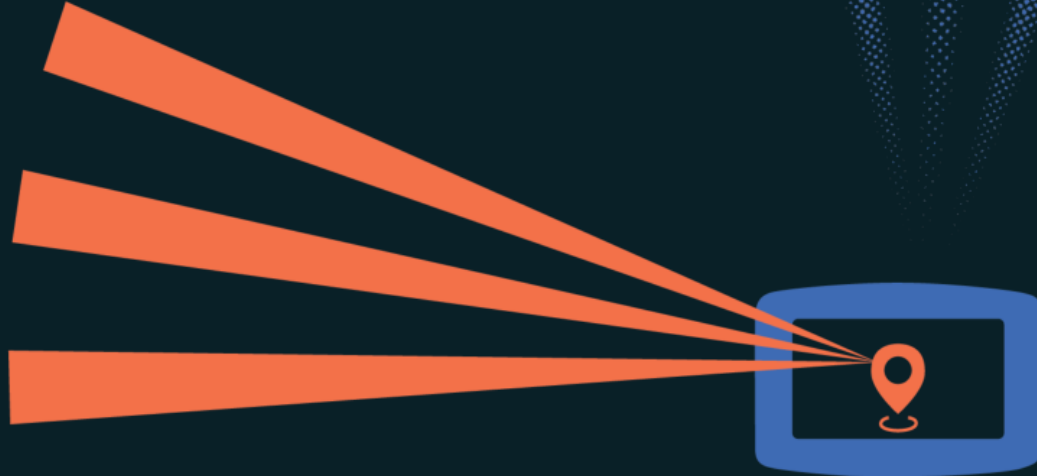


Figure credits: C4ADS report

FROM RESEARCH MANIA TO REAL THREAT

Leaders in the public and private sectors have paid **little attention** to the threat of GNSS spoofing.

Until recently, for good reason: signal generators capable of conducting a spoofing attack cost of **tens of thousands of dollars** and required **expert knowledge** to operate.

But this all began to change over the past decade with the advent of cheap, commercially available, and portable **SDR** (software defined radios) and open-source code capable of transmitting spoofed GPS signals.

These devices are capable of mimicking authentic, multimillion-dollar GPS satellite signals and can be produced for under \$300.

IRAN, 2011

15 December 2011

Probably the first reported spoofing attack ever.

“The US stealth drone broadcast last week on Iranian state television was captured by spoofing its GPS coordinates, a hack that tricked the bird into landing in Iranian territory instead of where it was programmed to touch down”



https://www.theregister.co.uk/2011/12/15/us_spy_drone_gps_spoofing/
https://www.theregister.co.uk/2011/12/08/iran_footage_captured_us_spy_drone/
<https://www.securityweek.com/reports-say-us-drone-was-hijacked-iran-through-gps-spoofing>

UT AUSTIN YACHT SPOOFING

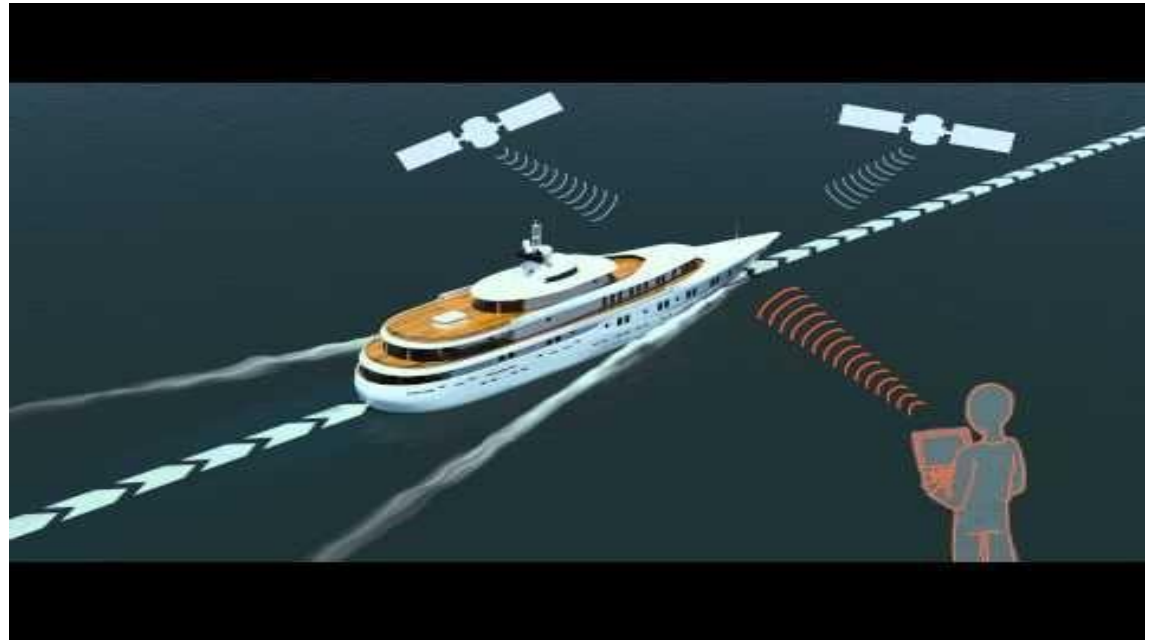
Summer 2011

A research team from the University of Texas at Austin (UT Austin) successfully hijacked the GPS navigation systems onboard an 80 M\$ superyacht using a 2000 \$ device the size of a small briefcase.

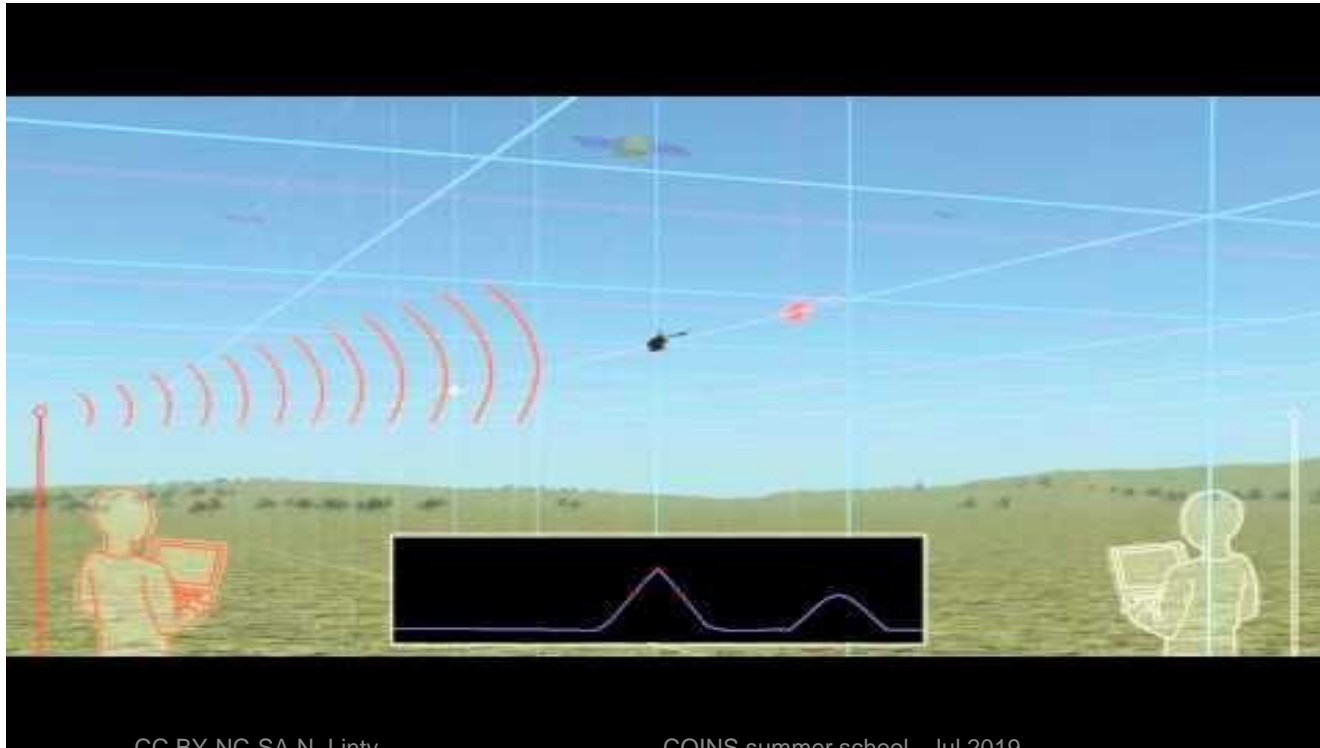
<https://youtu.be/ctw9ECgJ8L0>

Full story:

<http://www.engr.utexas.edu/news>



UT AUSTIN DRONE SPOOFING



University of Texas,
Austin
Prof Todd Humphreys

<https://youtu.be/6qQXVUze8oE>

THE BLACK SEA CASE

June 22-24, 2017

A number of ships in the Black Sea reported **anomalies** with their GPS-derived position, and found themselves apparently located more than 32 km inland, at Gelendzhik Airport.

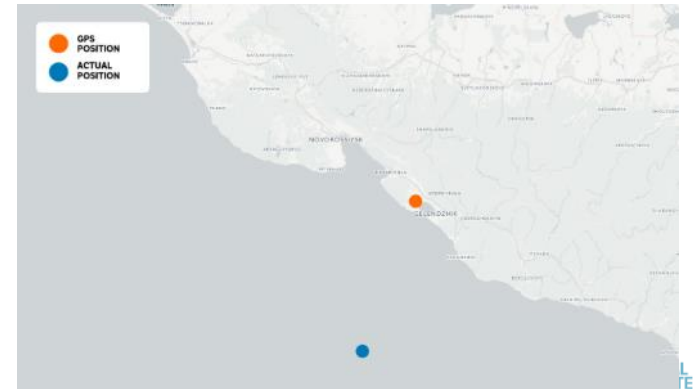
“Good HDOP, accuracy within 100 m, but location 25 nautical miles off”



<https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>

<https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/>

<https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/>



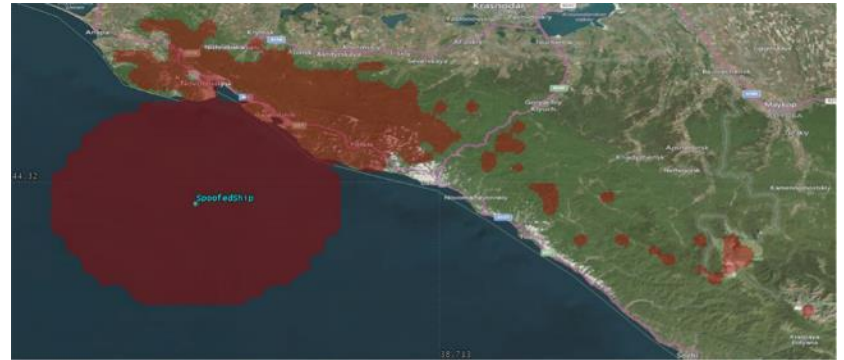
WHAT REALLY HAPPENED

“[...] basing this discussion solely on public domain information and anecdotal evidence, I would say this was almost certainly a spoofing incident.”

“The first thing we might conclude from this is that the spoofing indeed originates from Russian territory, close to the Black Sea coast”

“There’s one explanation that fits very nicely: drone defense”

“Some worry that this means that spoofing is getting easier”



Possible spoofing source locations

WHY AIRPORTS?

October 24, 2016

Modern drones have **geofencing rules**, a map of zones they are forbidden to fly over, which include airports and other restricted areas.

So, if you were trying to perform aerial surveillance of the Russian border, your drone may suddenly think it was over an airport, and take action accordingly.

Problems with taxi apps: taxi customers had their journeys recorded as airport transfers, which cost them much more



https://www.rbth.com/politics_and_society/2016/10/24/why-is-the-kremlin-transporting-gps-users-to-vnukovo-airport_641665

RUSSIA BEYOND English

Lifestyle Culture Travel Education Bu

Why is the Kremlin 'transporting' GPS users to Vnukovo airport?

LIFESTYLE · OCT 24 2016 · YEKATERINA SINELSHIKOVA · RBTH

The Moscow Kremlin and the Kremlin Embankment.
Evgeny Biryakov/RIA Novosti

Moscow residents have been recording a strange GPS anomaly near the Kremlin. From time to time, the signal there disappears and users are "transported" many miles from the place – to one of the city's airports. What is going on?

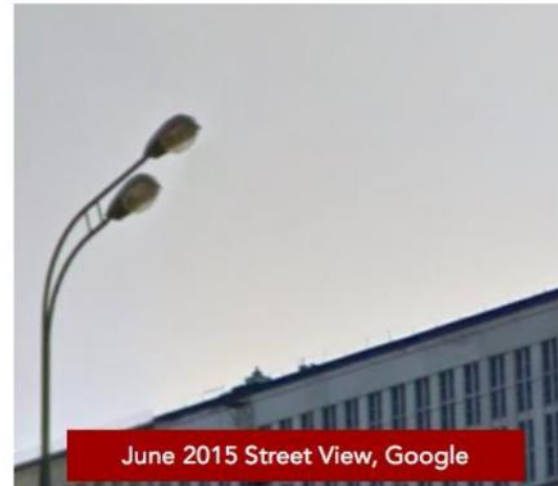
AROUND THE KREMLIN

June 2016

First public reports of GNSS spoofing near the Kremlin

Source: GNSS Spoofing – A Technology Re/evolution, The Resilient Navigation and Timing Foundation, C4ADS

CC BY-NC-SA N. Linty



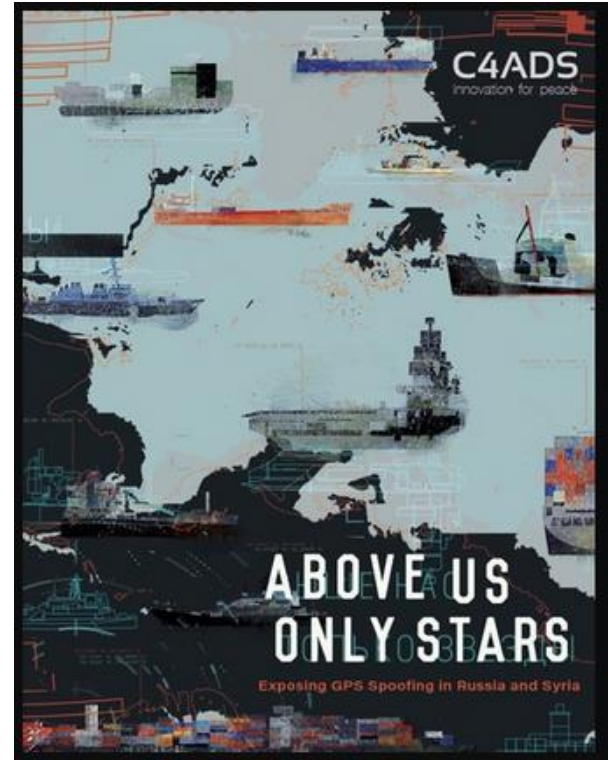
THE C4ADS REPORT

C4ADS: Center for Advanced Defense Studies is a nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security

Year-long, Worldwide investigation

Shows evidence for spoofing pointing to consistent, widespread GNSS disruptions and geolocation errors in and around the Russian Federation, Crimea, and Syria

- 9883 separate cases of GPS spoofing
- 1311 commercial ships affected, in and around Russian waters since February 2016
- `spoofing for very important person (VIP) protection



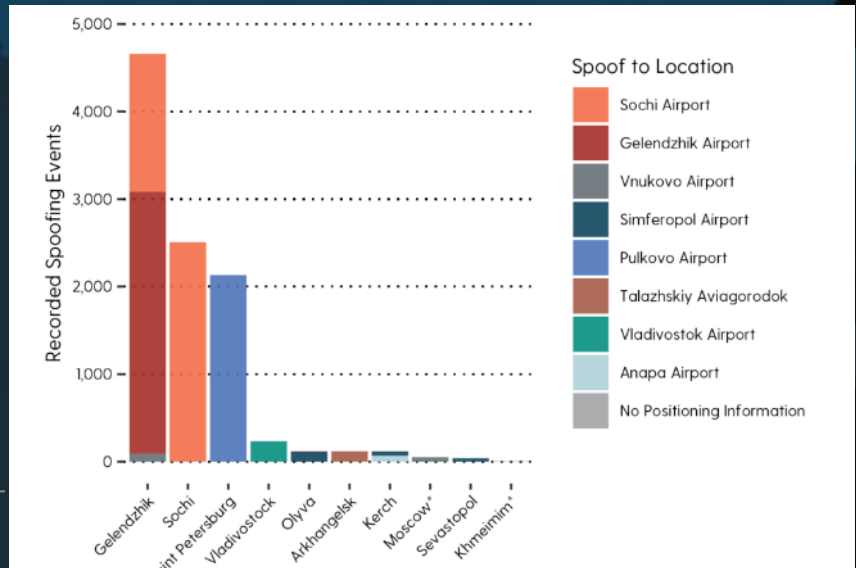
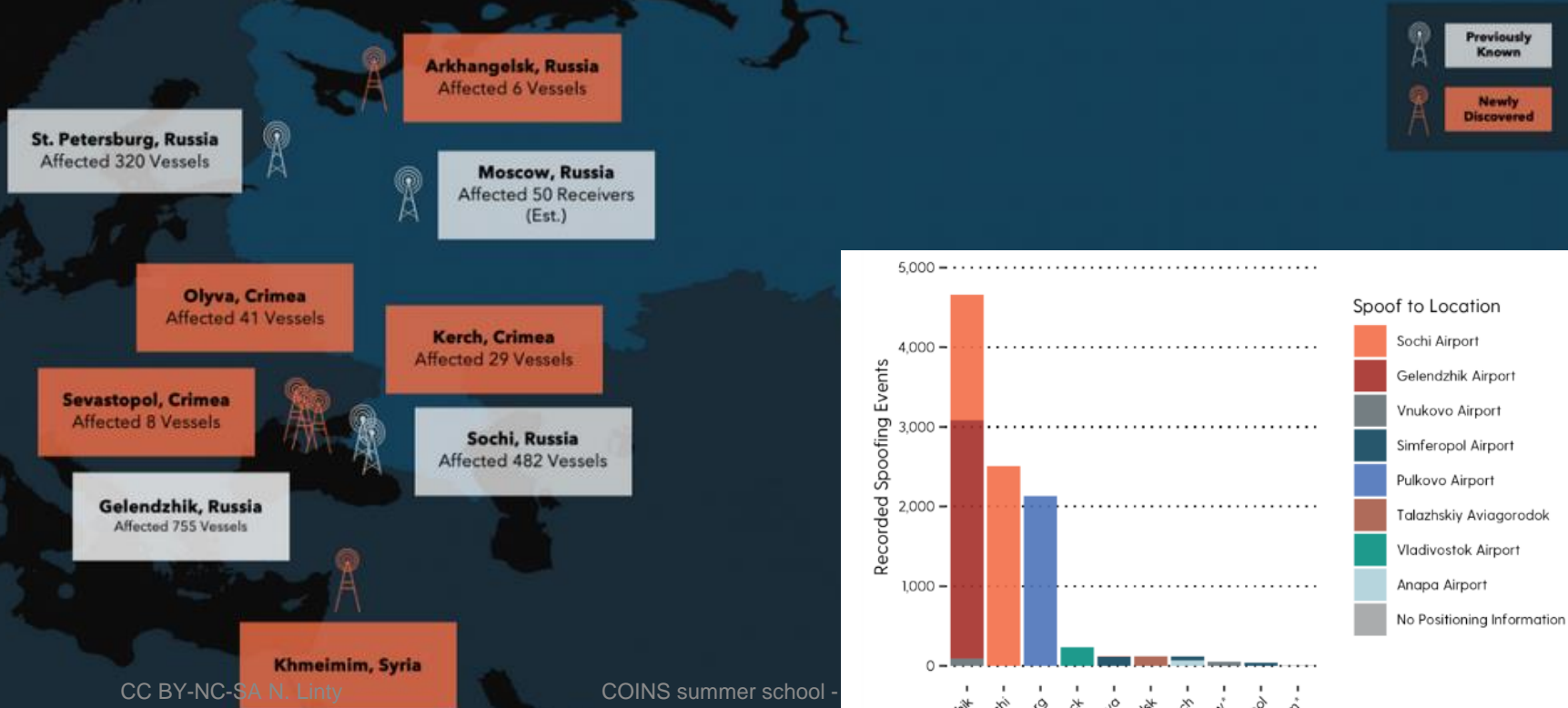
www.c4ads.org



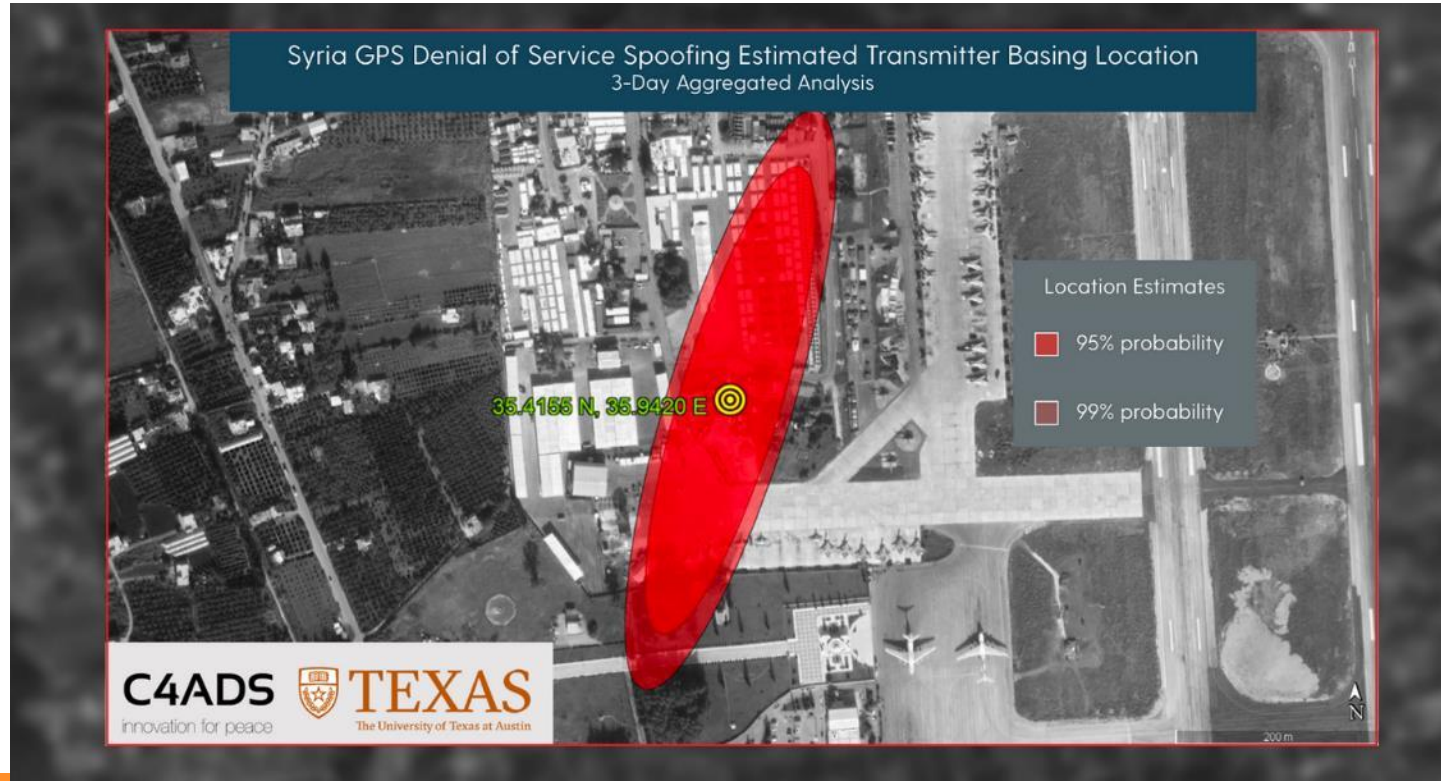
<https://www.c4reports.org/aboveusonlystars>

<https://insidegnss.com/new-report-details-gnss-spoofing-including-denial-of-service-attacks/>

DETECTED GNSS SPOOFING



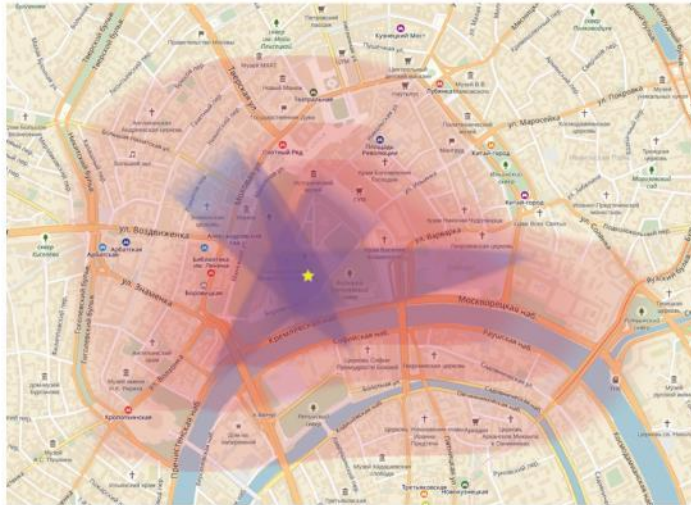
GNSS DATA FROM ISS



MORE TESTS

Grigory Bakunov, popular blogger

“there is a powerful transmitter operating at random times inside the Kremlin, spoofing geolocation signals on L1”



Geolocation spoofing around the Kremlin.

Grigory Bakunov / Telegram

The Kremlin Eats GPS for Breakfast

Why geolocation in central Moscow has become a real headache

By Kevin Rothrock
Oct. 21, 2016



in blue and red, where his GPS and GLONASS devices succumbed to location-spoofing



<https://www.themoscowtimes.com/2016/10/21/the-kremlin-eats-gps-for-breakfast-a55823>

IRAN, 2019

“We have had several members suggest that before the US drone was shot down by Iran last week, it was spoofed into violating Iranian airspace.”

Still, it is unlikely that a 200 M\$ drone is not equipped with anti-spoofing measures and with backup navigation systems



<https://rntfnd.org/2019/06/22/drone-shoot-down-did-iran-spoof-it-then-shoot-it/>

<https://www.wired.com/story/iran-global-hawk-drone-surveillance/>

ION GNSS+2017 CONFERENCE

28 September 2017

Portland Convention Center, Exhibition Hall

Numerous smartphones began exhibiting abnormal behavior (Inability to fetch e-mail, very old text messages, wrong time & date

A spoofing event was in progress

GNSS Simulator running a demonstration. 1 port attached to a device, 5 not properly terminated (plastic caps).

Energy leakage sufficient for phones to lock onto the false signal set for a two booth block radius (January 12, 2014, somewhere in Europe)

The incident shows really how vulnerable many receivers are to spoofing.

ION GNSS+ Exhibit Hall Map and Information

	118	119	218	217	318	319	418	419	518	519	HALL HOURS Wednesday: 10:00 a.m.–8:00 Exhibit Hall Open 6:00 p.m.–8:00 Exhibitor Hosted Reception Thursday: 9:00 a.m.–6:00 Exhibit Hall Open
	116	117	216		316	317	416	417	516	517	
	114	115	214	215	314	315	414	415	514	515	
										513	
Attendee Lounge	108	109	208	B		E		409	508	511	
										509	
										505	



CC BY

<https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/>

Logan Scott, «The Portland spoofing incident», presentation to PNT Advisory Board

<https://www.gps.gov/governance/advisory/meetings/2017-11/scott2.pdf>

POKEMON GO

These are actually mainly developer applications that do spoofing at **application layer**.

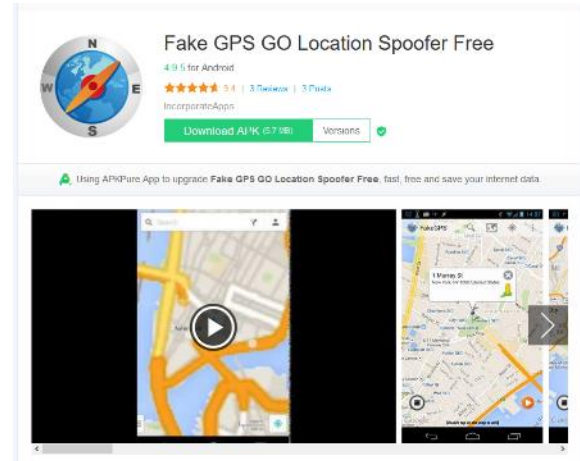
Pokemon Go Developers were quick to implement checks to ensure only “real” GPS locations were used

So people started looking at spoofing GPS, quick and dirty using HackRF front-end and **SDR**

Spoofing becoming available to a new generation of hackers...



GNSS Threats, Attacks and Simulations Guy Buesnel and Mark Holbrow, June 2017
<https://www.gps.gov/governance/advisory/meetings/2017-06/buesnel.pdf>



POKEMON GO

Report on Reddit about the use of jammers to cheat Pokemon Go.

a guy in his neighborhood” bought a bunch of jammers and set them up near the real-life locations of the virtual gyms he had conquered in the game. That meant that when other players approached the gyms, the GPS on their phones would be blocked and their locations couldn’t be registered in the virtual space—which meant “nobody could conquer his gyms.”



https://www.reddit.com/r/pokemongo/comments/5064rn/is_there_such_a_thing_as_a_gps_jamming_device/d71fsut/

LONDON STOCK

2013

The London Stock exchange was periodically affected by a jammed GPS signal.

The jamming was not thought to be malicious, but the result of a **local driver** using an off-the-shelf jammer to elude his employer's tracking.

But what if a more sophisticated user with bad intentions conducts a complex timing attacking on a stock exchange?

In today's world of high-speed stock trades, millions of dollars can quickly be lost if timestamps are corrupted and panic sets in.



<https://www.economist.com/international/2013/07/27/out-of-sight>

FURTHER READS ON THE TOPIC



<https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>

<https://blog.bliley.com/radar-jamming-deception-electronic-warfare>

<https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955>

<https://inhomelandsecurity.com/gps-jammers-problems-worldwide/>

<https://nrkbeta.no/2017/09/16/over-20-skip-gps-hacket-i-svartehavet/>

Dana Goward - President of the Resilient Navigation and Timing Foundation

<https://www.linkedin.com/in/dana-a-goward-3631bb51>



OTHER VULNERABILITES

TIMING

GNSS also provides consistent, global, extremely accurate **time** and **frequency**.

The **Telecommunications** sub-segment uses the GNSS timing function for handover between base stations in wireless communications, time slot management purposes and event logging (4G/5G networks, network time protocols).

The **Energy** sub-segment, including power transmission, (smart) electricity grids, uses GNSS timing in systems providing frequent measurements relevant to the network status and to determine the location of faults along a transmission line.

The **Finance** sub-segment (Banks and Stock Exchanges) uses GNSS to timestamp financial transactions, allowing one to trace causal relationships and synchronize financial computer systems.



GNSS Market Report, Timing & Synchronization

https://www.gsa.europa.eu/sites/default/files/GNSS_timing.pdf

CC BY-NC-SA N. Linty

COINS summer school - Jul 2019



181

INTERNET TIME

Time in an example of often-overlooked area that degrades security.

NTP over the internet is not secure, due to network load, variable path delays, firewalls.

Time from GPS/GNSS signals is recognized as the most accurate, available and traceable time source.

When there is a business-critical need to trace time to an accurate source, a GPS/GNSS-based time server should be deployed on the local network.



<https://www.gpsworld.com/is-internet-time-good-enough-for-cybersecurity/>

SIGNAL-LEVEL PROTECTION

Two different protection layers:

signal-level protection (encryption)

data-level protection (authentication)



ENCRYPTION

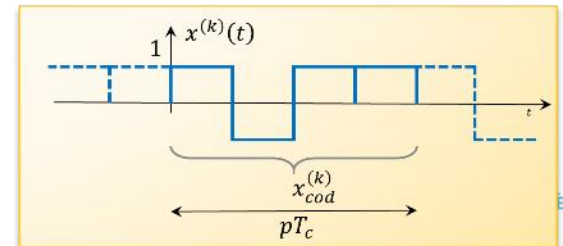
To keep the more powerful signal available at all times, and make it harder to spoof.

As long as the encryption key is kept unavailable to the general public it is near impossible to intercept/replicate/interfere with authorized user signals.

When encrypted, the **spreading codes** are replaced by an unpredictable bit-stream generated through a secret key

→ the signal indistinguishable from noise for unauthorized receivers

→ the signal is not reproduceable by anybody



GPS P(Y) CODE

The P code is public

GPS has the option to replace the P-Code with a secure P(Y)-Code (for authorized U.S. Government users)

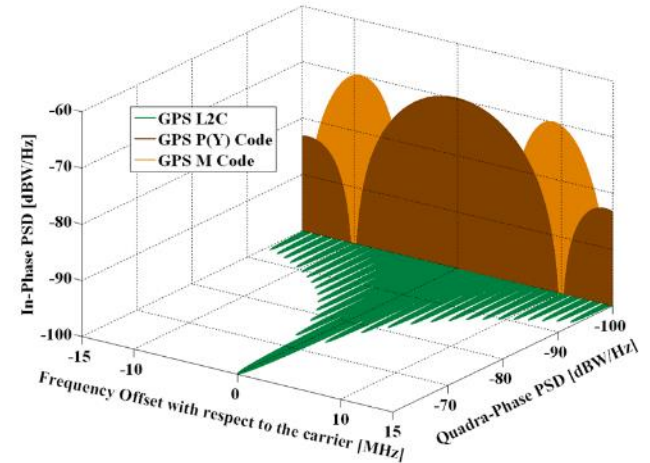
XOR between P code and a W encrypted sequence

W code details are secret, but it has been discovered that it is applied at approximately 500 kHz (20 times slower) → semicodeless techniques to track P(Y) signal.

Encryption

When encrypted, the P code becomes Y-Code and can only be interpreted by receivers with the encryption key.

The main purpose of the Y-Code is to assure that an opponent cannot spoof the Y-Code signal generating a Y-Code replica



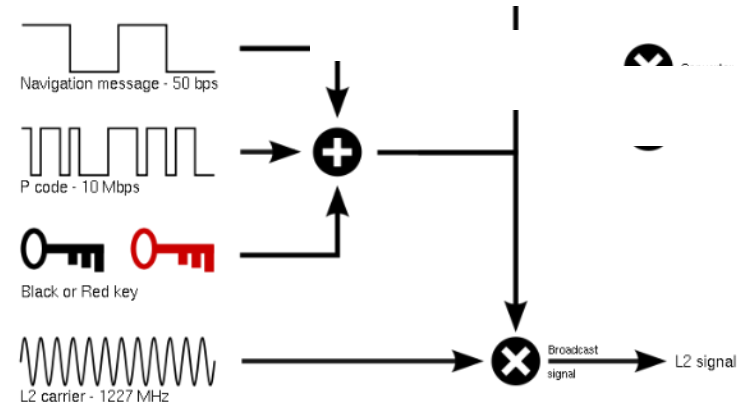
GPS P SIGNAL

P stands for **precision**

It is the original legacy GPS signal, C/A was conceived as an assistance for P processing

Shorter chip time means higher precision in range measurements w.r.t. C/A codes

Code length	Unique segment of an extremely long PRN sequence ($\sim 10^{14}$ chips lasting 267 days, split into 37 sections of 7 days each)
Chip rate	$R_C = 10.23 \text{ MChip/s}$
Code duration	$T_{\text{code}} = 1 \text{ week}$
Carrier	$f_{L1} = 1575.42 \text{ MHz}$ and $f_{L2} = 1227.60 \text{ MHz}$

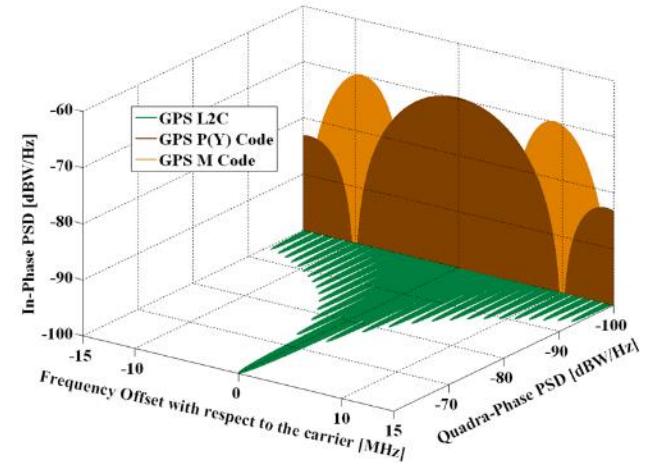


Source: Wikimedia commons

GPS M CODE

Part of GPS modernization process

intended to be broadcast from a high-gain directional antenna, in addition to a full-Earth antenna.



Code length	Unknown
Chip rate	$R_C = 5.115$ MChip/s
Code duration	Unknown
Carrier	$f_{L1} = 1575.42$ MHz and $f_{L2} = 1226.70$ MHz
Bandwidth	24 MHz (separated sidebands lobes)
Modulation	BOC

GALILEO PRS

The Galileo Public regulated service (PRS) is an **encrypted** navigation service for governmental authorised users and sensitive applications that require high continuity

Differences with OS:

- resilience: PRS will ensure better continuity of service when access to other navigation services may be degraded
- robustness: in cases of malicious interference, PRS increases the likelihood of the continuous availability of the SIS

The PRS will make more costly and more difficult to attack the Galileo signal

Jammers will require more power, they will be more expensive and easier to locate when in use. At the same time, robust encryption mechanisms within the PRS signal will enable positive protection against spoofing.



<https://www.gsa.europa.eu/security/prs>

PRS USERS

PRS is primarily intended for use by EU Member State government authorised users. Access to PRS is controlled through operational and technical means, including governmental grade encryption. Users not granted access to the service will be unable to access any information from the signal.

PRS can provide support to a range of European public safety and emergency services, including: fire brigades, health services (ambulance), humanitarian aid, search and rescue, police, coastguard, border control, customs, civil protection units.

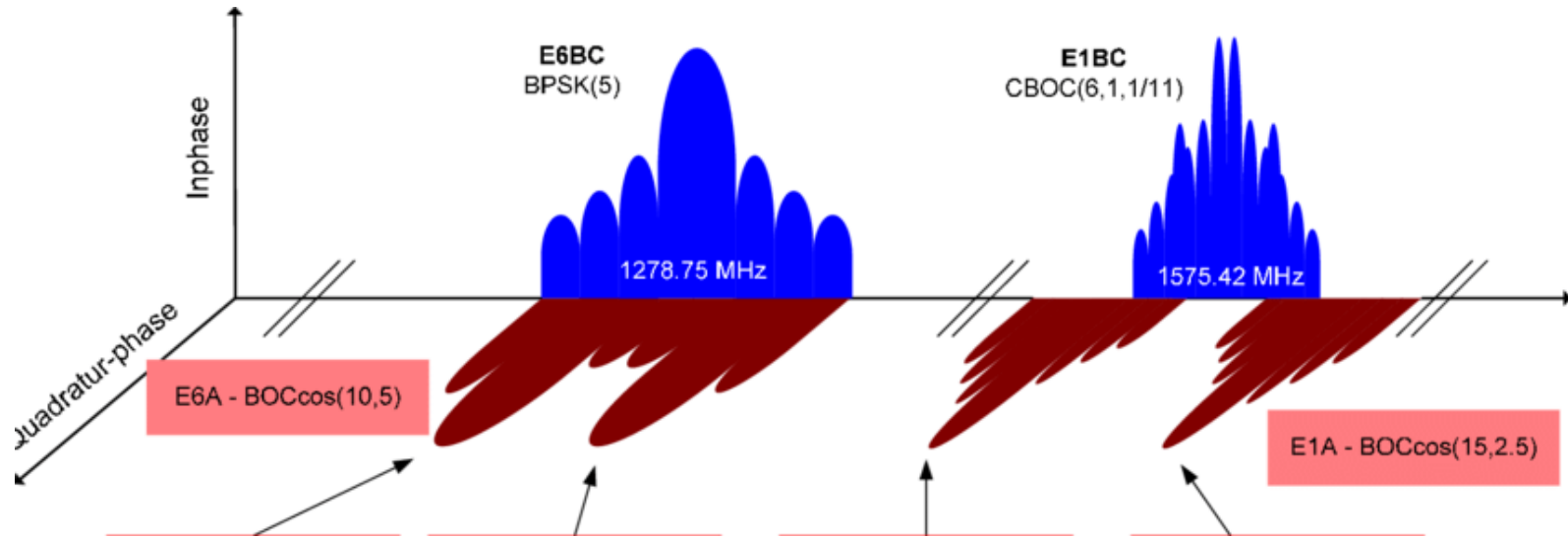
And to security and strategic infrastructure:

energy, telecommunications and finance

Technical features:

- Wide bandwidth
- Two signals (E1, E6)

WHERE IS PRS TRANSMITTED?

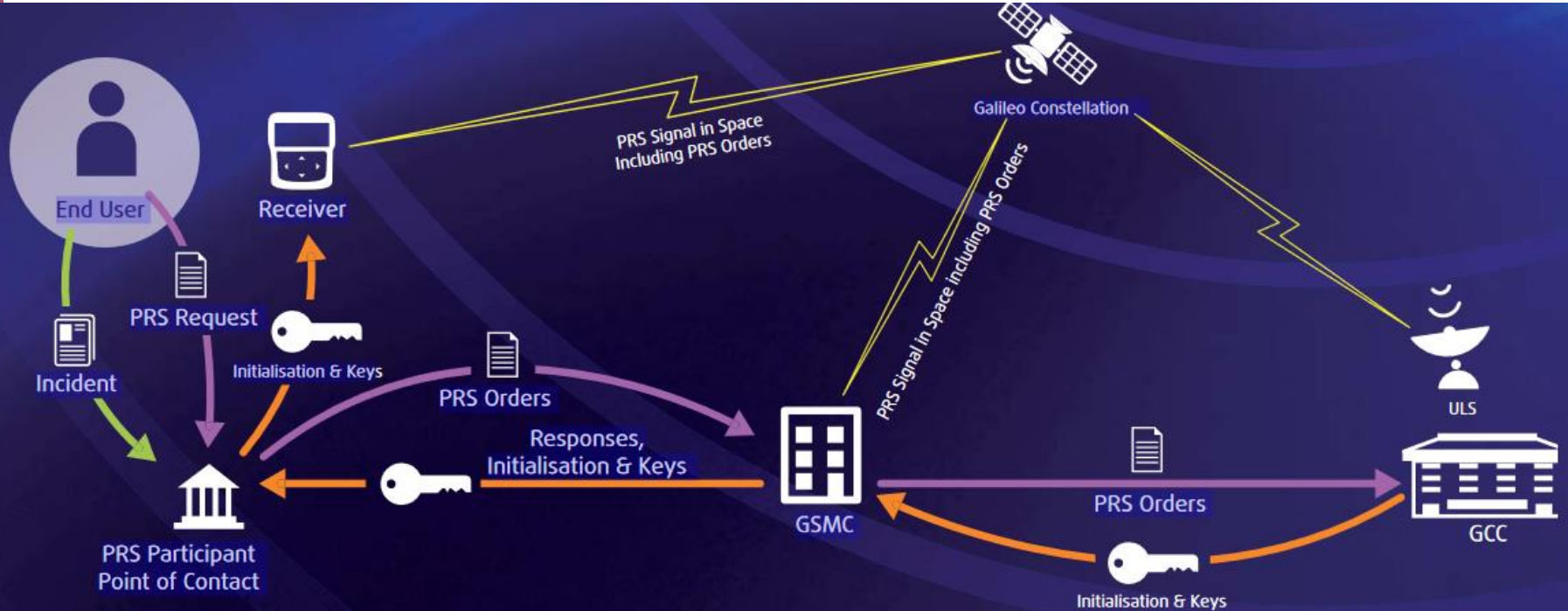


Source: Rügamer, Alexander et al. (2011). A Bavarian Initiative towards a Robust Galileo PRS Receiver. Proceedings of ION GNSS 2011.

HOW THE PRS WORKS

Source:

<https://www.dlr.de/Portaldata/28/Resources/dokumente/rnSource:/satnav/GSA10001015flyer8.pdf>



FURTHER INFO

Say 'Hello' to Galileo's PRS

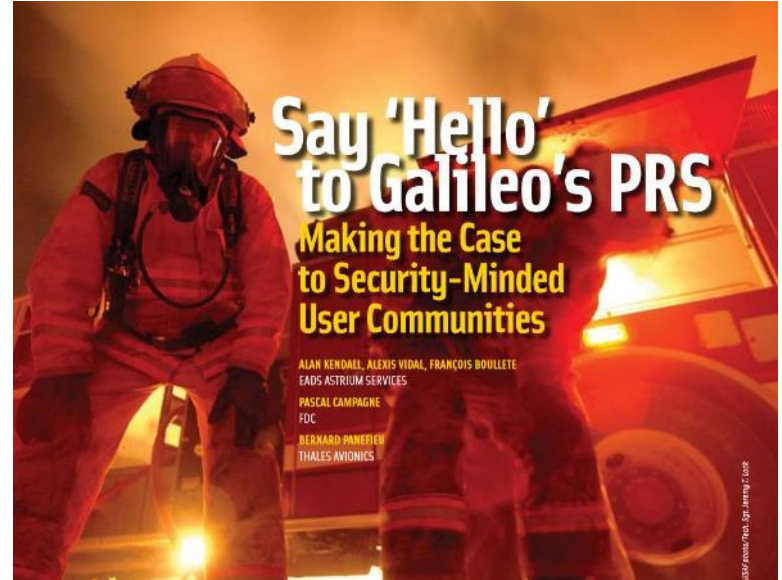
https://insidegnss.com/wp-content/uploads/2018/01/igm_050-054.pdf

Public Regulated Service (PRS) equals public security

<https://www.gsc-europa.eu/news/public-regulated-service-prs-equals-public-security>

The Galileo PRS, Public Regulated Service

<https://galileognss.eu/the-galileo-prs-public-regulated-service/>



AUTHENTICATION

As of today, all open civil GNSS signals are transmitted in the clear.

To limit spoofing, we need to be able to trust received signal.

Message Authentication is a concept that has a long history in digital communications, the basic idea being that the receiver of a message would like to ensure that the message they receive:

- 1) is **identical** to the message that was transmitted;
- 2) was generated by a **trusted** source.

NAVIGATION MESSAGE AUTHENTICATION

2003, Logan Scott proposed a number of techniques that could be implemented at the satellite level to “harden” the civil GNSS signals against spoofing attacks.

The first and most straightforward amongst these was NMA.

NMA is, unsurprisingly, the application of the Message Authentication concept to the navigation messages generated by GNSS satellites.

Using **asymmetric key** techniques in which the secret key is split into two parts, a “private” key, known only to the transmitter, and a public key which can be distributed publicly. The private key is used to generate the authentication message, while the public key is used in the verification step.



Generated by a trusted source does not necessarily means transmitted by a trusted source!



Scott, L. (2003) “Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems”, *ION GNSS 2003*.

AUTHENTICATION AND GNSS

GPS L1C: CHIMERA

asymmetric elliptic curve digital signature algorithm (ECDSA) P-224

At most every 3 minutes

Galileo E1 OS / E6 HAS:

hybrid symmetric/ asymmetric key approach known as the Timed Efficient Streamed Loss-Tolerant Authentication (TESLA) scheme.

40 bits every two seconds of the Galileo E1b I/NAV

cross-satellite and even cross-system authentication



<https://insidegnss.com/what-is-navigation-message-authentication/>

TESLA OSNMA

symmetric key distribution:

- 1) Message Authentication Code (MAC) is generated using the message and the private key
- 2) The message and the MAC are transmitted
- 3) Sometime later, the private key is broadcast, to ensure that the key used to generate the MAC is not known until after the message and MAC are already received

chain of keys

- 1) An initial key K_0 is randomly selected
- 2) Each subsequent key in the chain K_{i+1} is generated from the previous key K_i using a one way function: $K_{i+1} = f(K_i)$.
- 3) The system generates a chain of length N , then transmits the N th key (called the root key) along with a digital signature generated using a standard asymmetric scheme, such as ECDSA
- 4) The chain keys are then used in reverse order to generate the MACs
- 5) Knowing the one-way function, the receiver can verify that each chain key is from the same chain as the digitally signed root key, but cannot predict “future” chain keys

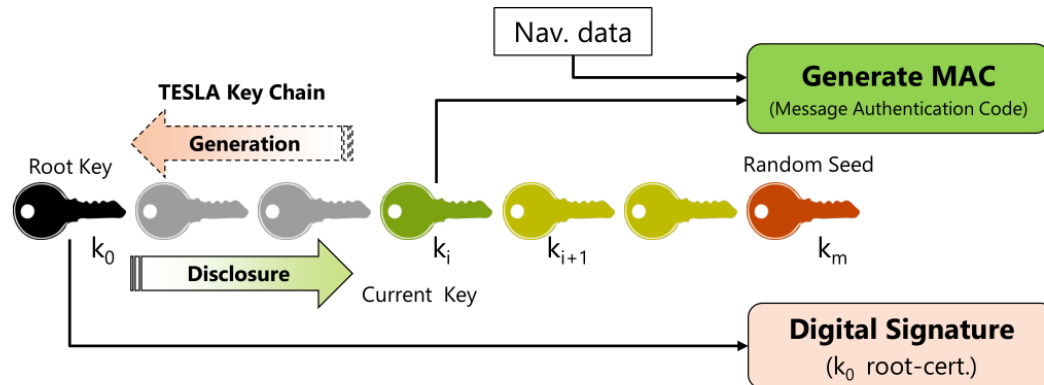
TESLA OSNMA

Once a TESLA chain has been established by asymmetric cryptographic means, the satellites begin transmitting messages, MACs and keys using the delayed release mechanism

The receiver extracts the messages and MACs and stores them until the key is received

The key is first checked to ensure that it is part of the TESLA chain in force using the known one way function

If the key passes this test. it is then used to verify that the MAC and the message correspond



TESLA

TESLA key chain:

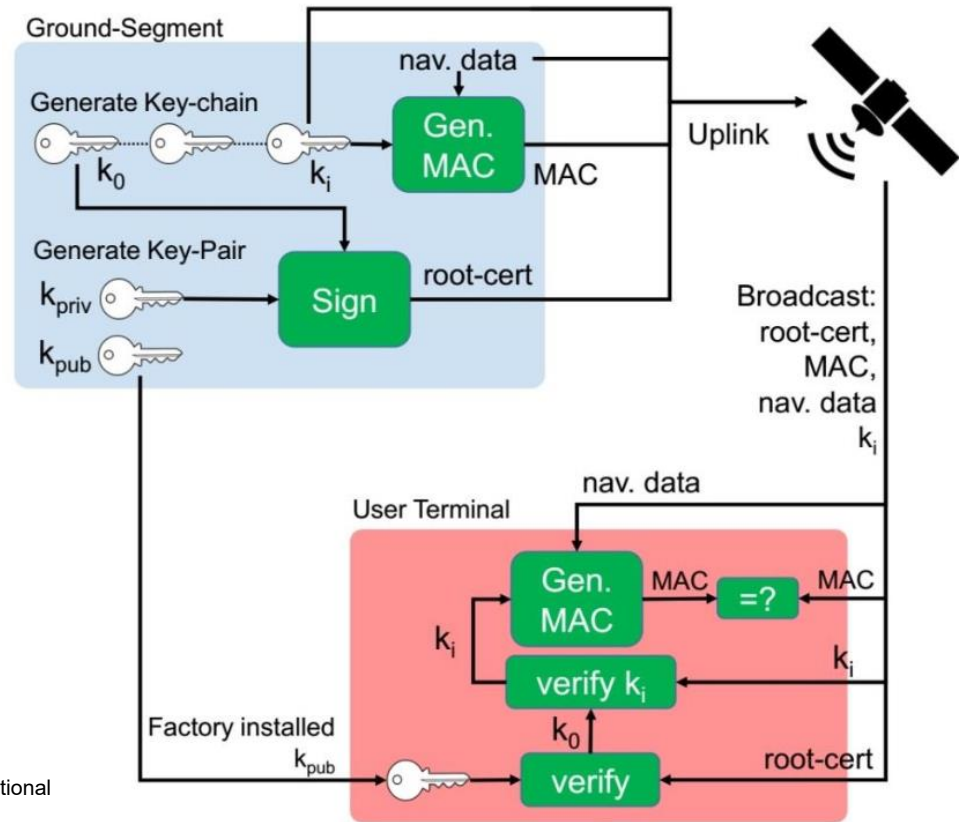
- $k_0 \dots k_i k_{i+1} \dots k_m$
- SYMMETRIC approach

Public-private pair:

- k_{priv} used to sign k_0 (root-cert.)
- k_{pub} to verify k_0 root-cert. (e.g. k_{pub} factory installed in the receivers)
- ASYMMETRIC approach

Strict requirement on receiver synchronization:

- MAC must be received before k_i is released



OSNMA

NMA is not a panacea, and by itself does not solve the spoofing problem

Also **range measurements** should be authenticated

However, certain types of spoofing attack are detectable when NMA is implemented



GNSS Authentication: Design Parameters
and Service Concepts
I. Fernández-Hernández

GPS ROLLOVER



<https://www.gpsworld.com/schriever-air-force-base-releases-gps-week-number-rollover-guidelines/>

In GPS time is counted combining

- **GPS week**, in weeks
- Time of the week (**TOW**): number of 1.5-second intervals since Sunday midnight

Both transmitted in the navigation message

The GPS Week Number count began at midnight on Jan. 5, 1980. It is increments by 1 each week.

Problems: 10 bits reserved for this field. → roll from 1023 to 0 every 1024 weeks (about 19.7 years)

- Aug 21, 1999
- **Apr 6, 2019**

GPS ROLLOVER GONE WRONG

GPS Week Number Rollover was supposed to pass without a hitch. Plenty of notice that updates might be required for legacy receivers.

Instead, several systems crashed.

- 15 Boeing 777s and 787s grounded in China, pending a GPS update (the receivers gave the date as August 22, 1999)
- Part of the wireless grid faulted in New York City, cutting information feeds to the NYPD (license plate cameras) and remote worksite communications
- Weather balloons grounded In Australia
- US NOAA autonomous monitoring stations went offline



<https://www.gpsworld.com/seen-heard-measuring-everest-gps-rollover-boo-boos>

THE STRAVA CASE

29 January 2018

Online fitness tracker Strava has published a "heatmap" showing cycle.

Nathan Ruser, a 20-year-old international security student at the , across the map while browsing a cartography blog.

A large number of military personnel on active service had been publicly sh



<https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/?verso=true>

<https://www.bbc.com/news/technology-42853072>

<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

● Latest: Strava suggests military users 'opt out' of heatmap as row deepens



▲ A military base in Helmand Prov
Strava Heatmap

Fitness app Strava lights up staff at military bases

© 29 January 2018



The movements of soldiers within Hagram air base - the largest US military facility in Afghanistan

Security concerns have been raised after a fitness tracking firm showed the exercise routes of military personnel in bases around the world.

GPS NSC

Ma 17, 2017

Main lobe of the GNSS L1 signals spectrum

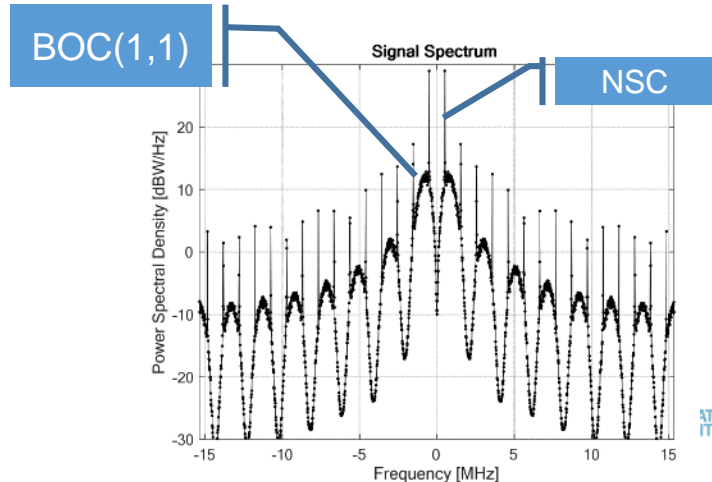
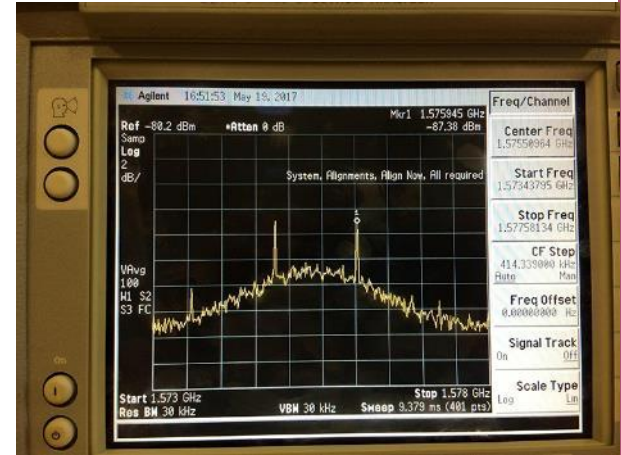
Two spikes, at approximately
 $f_{L1} = 1575.42 \text{ MHz} \pm 0.5 \text{ MHz}$

Coming from GPS satellite **SVN49** transmitting a **NSC**: BPSK sequence with alternating logical 0s and 1s, transmitted at the C/A code chipping rate



<https://www.gpsworld.com/anomalous-gps-signals-reported-from-svn49>

Dovis, F., Margaría, D., & Motella, B. Analysis of the impact of a Non-Standard GPS C/A code on Galileo signals. *IEEE/ION PLANS 2018*, pp. 945-955



#GLONASSDOWN

April 2 2014

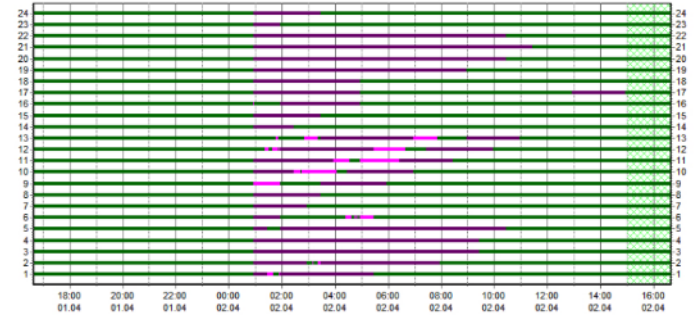
Unprecedented total disruption of a fully operational GNSS

All satellites GLONASS broadcast corrupt information for 11 hours.

This rendered the system completely unusable to all worldwide GLONASS receivers.

Bad ephemerides were uploaded to satellites and became active at 1:00 a.m. Moscow time. The GLONASS fix could not take effect until each satellite in turn could be reset, during its pass over control stations in Russian territory, thus taking nearly 12 hours.

Состояние КА ГЛОНАСС с 16:39:00 01.04.14 по 16:39:00 02.04.14 UTC+4



<http://gpsworld.com/the-system-glonass-fumbles-forward/>

#GALILEODOWN

July 11-15, 2019

Starting 1 p.m. CET, users noticed that all ephemeris stopped broadcasting, and then a [Notice Advice to Galileo Users \(NAGU\)](#) appeared: “signals may not be available and should be employed at users’ own risk”

“The technical incident originated by an equipment malfunction in the Galileo ground infrastructure, affecting the calculation of time and orbit predictions, and which are used to compute the navigation message. The malfunction affected different elements on the ground facilities.



<https://www.gpsworld.com/galileo-down-over-weekend/>
<https://www.gpsworld.com/galileos-initial-services-rocky-patch-continues/>
<https://www.gpsworld.com/galileo-picks-itself-up-and-moves-on/>
<http://www.navsas.eu/node/610>
<http://www.navsas.eu/node/614>
<https://www.wired.com/story/galileo-satellite-outage-gps/>
https://www.maanmittauslaitos.fi/en/topical_issues/galileo-incident-july-11th-17th

GPS BACKUP SYSTEMS

Space Development Agency Plans to Create an Alternative GPS Constellation

LORAN-C became obsolete once GPS was widely adopted (South Korea is developing something similar)

Ground-based fiber optic cables: UTC can be transferred with a stability of less than 100 ns



<https://insidegnss.com/space-development-agency-plans-to-create-an-alternative-gps-constellation/>



OTHER RESOURCES



TODD HUMPHREY'S TED TALK



<https://youtu.be/r4UdHE3JNnU>

WHAT YOU CAN FIND ON YOUTUBE...



**(Short Range) GPS
Signal Blocker ~ Ensure
Your Right To Privacy**
[https://youtu.be/GavkPyhX
GKU](https://youtu.be/GavkPyhXGKU)

TUTORIALS...



<https://youtu.be/VAmbWwAPZZo>

PARTIAL BIBLIOGRAPHY

Kaplan, E. D., Hegarty C.H. Understanding GPS: principles and applications (II edition), Artech House, Norhood, MA, 2006

Parkinson B., Spilker J. J. , Global Positioning System: theory and applications, Vol. I e Vol. II, American Institute of Aeronautics, 1996.

Misra P., Enge P. Global Positioning System: Signals, Measurements, and Performance (II edition), Ganga-Jamuna press

Misra P., GPS for Everyone: You are Here, Ganga-Jamuna press

Tsui, J. B. Y., Fundamentals of Global Positioning System (II edition), John Wiley & Sons, New York, 2006.

Zekavat S. A. , Buehrer R. M. (ed), Handbook of Position Location: Theory, Practice, and Advances, John Wiley & Sons, Inc., Hoboken, NJ, USA

Fabio Dovis, et al. *Classification of interfering sources and analysis of the effects on GNSS receivers*, Artech House, 2015

www.navipedia.net

CREDITS AND DISCLAIMER

A part of the material contained in these slides is taken from the classes I had at Politecnico di Torino, in the frame of the “Satellite Navigation Systems” class at the *Master of Science in Communication and Computer Networks Engineering* and of the classes at the *Second Level Specializing Master in Navigation and Related Technologies*.

A part of the material is taken from the classes I had in the frame of the e-KnoT project, lead by Politecnico di Torino. <http://www.eknotproject.eu/>

I would like to acknowledge prof. Fabio Dovis, who contributed to the preparation of the first version of some of the slides.

A part of the material contained in these slides was freely collected along the years, from websites, presentations, papers... When possible, the source has been acknowledged. In all the cases where it applies, I do not own the copyright of images, content, figures, etc.

Nicola Linty

PhD, Associate professor

Navigation and Positioning Department
Finnish Geospatial Research Institute (FGI)
National Land Survey of Finland (NLS)

www.fgi.fi



@nicolalinty



<https://github.com/nicolalinty>



linkedin.com/in/nicolalinty



nicolalinty.wordpress.com



nicola.linty@nls.fi

ΕΥΧΑΡΙΣΤΩ!