Università degli Studi di Padova

Department of Information Engineering

Master Thesis in ICT for Internet and Multimedia

Parametric models for a database of realistic threats to GNSS receivers

Supervisor
Nicola Laurenti
Università di Padova

Master Candidate
Nicola Boscaro

Academic year: 2019/2020

March 2^{nd}*, 2020*

To my Parents, my Girlfriend and my Friends.

Abstract

Threats to GNSS receivers are becoming increasingly complex and easier to implement due to technological advancement. So, these attacks have become now a serious problem for any user, not only, for example, for military or safety-of-life purposes anymore. In this context, Testbed for Attacks and Mititgations has been created to collect data about these attacks and possible mitigations.

This thesis describes how tested threat scenarios to GNSS signals have been parameterized to be inserted in the TAM database.

Contents

Listing of figures

Listing of tables

Listing of acronyms

ADC	Analog to Digital Conversion
AGC	Automatic Gain Control
AR	Axial Ratio
AS	Authorized Service
AWGN	Additive White Gaussian Noise
BDS	BeiDou Navigation Satellite System
BGD	Broadcast Group Delays
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
CNSA	China National Space Administration
CRC	Cyclic Redundancy Check
CS	Commercial Service
CW	Continuous Wave
DEI	Department of Information Engineering
DLL	Delay Lock Loop
DoS	Denial of Service
EGNOS	European Geostationary Navigation Overlay Service
EC	European Commission
ESA	European Space Agency

EU ..... European Union

FLL ..... Frequency Locked Loop

GAGAN ..... GPS Aided Geo Augmented Navigation

GEO ..... GEostationary Orbits

GIS ..... Galileo Initial Services

GLONASS ..... GLObal'naja NAvigacionnaja Sputnikovaja Sistema

GNSS ..... Global Navigation Satellite System

GST ..... Galileo System Time

HAS ..... High Accuracy Service

ICG ..... International Committee on Global Navigation Satellite Systems

IF ..... Intermediate Frequency

IGSO ..... Inclined GeoSynchronous Orbits

LHCP ..... Left-Hand Circular Polarization

LO ..... Local Oscillator

MEO ..... Medium Earth Orbiting

MSAS ..... Multi-functional Satellite Augmentation System

NAVSTAR GPS . NAVigation Signal Timing And Ranging Global Position System

OS ..... Open Service

PLL ..... Phase Lock Loop

PNT ..... Positioning, Navigation, Timing

PVT ..... Positioning, Velocity, Timing

PPS ..... Precise Positioning System

PRS ..... Public Regulated Service

QZSS ..... Quasi-Zenith Satellite System

RF ..... Radio Frequency

RFI ..... Radio Frequency Interference

RHCP ..... Right-Hand Circular Polarization

SA ..... Selective Availability

SaR ..... Search-and-Rescue

SBAS ..... Satellite-Based Augmentation Systems

SDR ..... Software Defined Radio

SIS ..... Signal-in-Space

SISA ..... Signal-in-Space Accuracy

SMS ..... Short Message Service

SPS ..... Standard Positioning System

SQM ..... Signal Quality Monitoring

SV ..... Space Vehicle

SVID ..... Space Vehicle IDentifiers

TAM ..... Testbed for Attacks and Mitigations

TOA ..... Time of Arrival

TOW ..... Time-of-Week

USSR ..... Union of Soviet Socialist Republics

UTC ..... Coordinated Universal Time

WAAS ..... Wide Area Augmentation System

WADS ..... Wide Area Differential Service

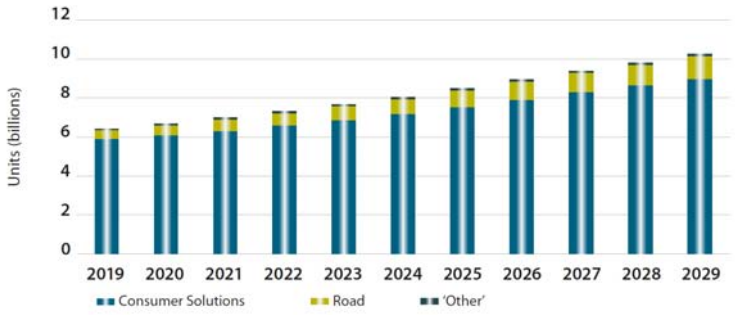
1 Introduction

A Global Navigation Satellite System (GNSS) is an infrastructure that allows users with a compatible device to determine their position, velocity and time by processing signals from satellites. Altough it was born for military purposes decades ago, nowadays, it is used globally for a wide range of services, as we can see in Fig. 1.1, to the point where its absence would be inconceivable.

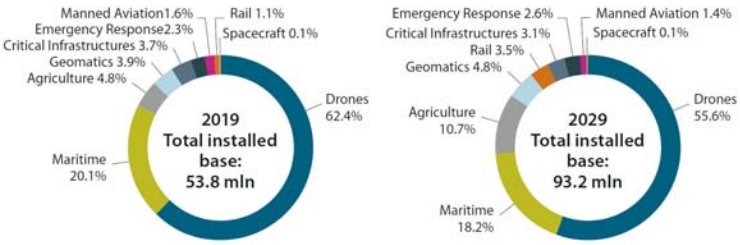
Right now there is a digital revolution that is influencing our lives, but also the business models of companies that are constantly trying to keep up with "macrotrends" (*i.e.* climate change and sharing economy just to name a few) in technological development. Indeed, when these services require positioning and timing data, the adoption of GNSS solutions is needed, so that we may have environmentally friendly transport solutions, sustainable agriculture, meteorology and climate change monitoring or ride sharing services.

Of course, with more and more people that are growing concerns about security over the years, GNSS threats may now be considered hot topic given the spreading of GNSS services. The low power of the signals that reach the Earth surface from satellites, in fact, makes it easier to perform denial of service (*jamming*) or forging of GNSS signal (*spoofing*) attacks. The impact of such threats may be so disruptive - just imagine businesses that base their activities on GNSS, or safety of life services - that the study of countermeasures to these problems is truly significant.

This thesis was developed as part of the project *Testbed for Attacks and Mitigations* (TAM)



(a) Global installed base by segment



(b) Installed base of "Other" segments

Figure 1.1: GNSS global installed base by segment (1.1a) and detailed view of "Other" segment (1.1b). [1]

during an internship carried out between August 2019 and February 2020, and it is about the laboratory testing of several threat scenarios to GPS and Galileo signals and the following insertion, based on specific parameters, of the results in a database needed for the services offered by TAM. This thesis is composed as follows:

Chapter 2 a brief overview of GNSS technologies with regards to different systems services and architecture, and the description of the GNSS signal.

Chapter 3 a description of GNSS threats jamming and spoofing, with some more details about some of the most common attacks and their detection.

Chapter 4 a report about the results achieved from the tests performed during the internship with also a description of what has been done in those months.

Conclusion conclusions from the work carried out and suggestions concerning possible future research topics.

Appendix few more details about GNSS error sources.

2

GNSS technologies

Satellite navigation systems have history that starts during what is now called Space Race*, starting with the first system deployed in the 1960s, Transit by the US military, which was based on the Doppler effect. To achieve enough accuracy this system needed constant monitoring from the base station which would send information about the deviation in satellites orbit so that next satellite broadcast would have had updated ephemeris.

What we have, about 60 years later in the modern GNSS, (*e.g.* such as GPS or Galileo just to name a few), is a more direct situation, where the satellite broadcasted signals directly contains orbital data and the precise time the signal was transmitted.

The description in this chapter is based on [3], [4], [5] and [6] and is not intended to be comprehensive, but only the basic concepts of modern GNSS and everything that will be needed in the following chapters to better understand this thesis work.

2.1 Systems overview

Global Navigation Satellite System (GNSS) is the name used to refer to a constellation of satellites, usually composed of 18-30 units in medium Earth orbit (MEO) spread between several orbital planes, providing signals from space that transmit positioning and timing data

*The competition between URSS and US, that began on August 2, 1955 during the Cold War, to achieve firsts in spaceflight capability. [2]

System	GPS	Galileo	GLONASS	BeiDou
Orbit	MEO	MEO	MEO	MEO, IGSO, GEO
Nominal number of satellites	24	30	24	27, 3, 5
Constellation	6 planes, 56° inclination	Walker (24/3/1), 56° inclination	Walker (24/3/1), 64.8° inclination	Walker (24/3/1), 55° inclination
Services	SPS, PPS	OS, HAS, PRS, SaR	SPS, PPS	OS, AS, WADS, SMS
Initial service	Dec 1993	Dec 2016	Sep 1993	Dec 2012
Origin	USA	Europe	Russia	China
Frequency (MHz)	L1 1575.42 L2 1227.60 L5 1176.45	E1 1575.42 E5a 1176.45 E5b 1207.14 E6 1278.75	L1 1602.00 L2 1246.00 L3 1202.025	B1 1561.098 B2 1207.14 B3 1268.52

SPS: Standard Positioning Service; *PPS*: Precise Positioning Service; *OS*: Open Service; *HAS*: High Accuracy Service; *PRS*: Public Regulated Service; *SaR*: Search-and-Rescue service; *AS*: Authorized Service; *WADS*: Wide Area Differential Service; *SMS*: Short Message Service
Galileo services and initial service date were changed based on [7] and [8]

Table 2.1: Overview of GNSS. [6]

to GNSS receivers. The actual systems vary, but use orbital inclinations of about 55° and have orbits, at an altitude of about 20,000 kilometres, with periods of roughly twelve hours (see Table 2.1).

Currently there are four active navigation satellite systems that provide global coverage which are the American GPS, the European Galileo, the Russian GLONASS and the Chinese BeiDou. Since a GNSS signal has to satisfy four performance parameters (accuracy, integrity, continuity and availability), several regional Satellite-Based Augmentation Systems (SBAS) come to help GNSS by correcting signal measurement errors (see Appendix A for different GNSS error sources). Some examples are the American Wide Area Augmentation System (WAAS), the European Geostationary Navigation Overlay Service (EGNOS), the Japanese Multi-functional Satellite Augmentation System (MSAS) or Quasi-Zenith Satellite System (QZSS), and the Indian GPS Aided Geo Augmented Navigation (GAGAN).

2.1.1 GPS

The Global Positioning System (GPS) is the American GNSS, implemented and operated by the US Department of Defense (DoD), which was declared fully operational from April 1995 with the baseline GPS being specified for 24 satellites, even if, currently [9], the system employs 31 Block IIA/IIF/IIR/IIR-M satellites[†].

The GPS, originally NAVSTAR GPS, is a line-of-sight, all weather, world-wide continuously available satellite-based RF positioning system that provides 3-dimensional position, velocity and time data to an end-user with an appropriate receiver. There are two different services provided by the GPS: the Standard Positioning Service (SPS) and the Precise Positioning Service (PPS). SPS is the service available for the civilian use which use the public C/A code on the L1 carrier. On the other hand, PPS is the service used by the military, and other authorized parties, which uses the encrypted P(Y) codes on both L1 and L2 carriers. Anyway, after the deactivation of the Selective Availability (SA) technique on 2 May 2000 by the administration Clinton, which was done in order to make GPS more responsive to civil and commercial users world-wide [11], the signals that the civilian receives are not so degraded anymore and the differences between the two services are that the PPS also features increased robustness, higher resistance to jamming, improved accuracy regarding signal distortion caused by ionosphere and multipath propagation. It must be said anyway that nowadays, even if the encrypted code P(Y), which will be replaced by the new more powerful M-code, is still available only for military use, there exists dual-frequency GPS equipment which is available for civilian use, that significantly improves the obtained results, but its cost and size has limited it to professional applications.

The modern GPS receivers also have the possibility to use an extra civilian safety-of-life signal on L5 band which can have much higher accuracy, pinpointing to within 30 centimetres. [12]

2.1.2 Galileo

The European GNSS Galileo is, as opposed to GPS, GLONASS or BeiDou, under civilian control. This means that, while the formers may be switched off or made less precise when desired (*e.g.* in case of conflict [13]) causing a very costly disruption, this situation should not happen for the Galileo system.

[†]From 22 August 2019, 2 third generation GPS Block IIIA satellites are also in orbit [10]

In the 1990s the European Union (EU) saw the need for Europe to have its own GNSS so, together with private investors, they started the Galileo project for a civilian GNSS. This project had many problems over the years, such as the nationalisation of the system in 2006 due to the falling apart of the public/private partnership and the subsequent funding problems, but in the end European Commission (EC) together with the European Space Agency (ESA) made it and the European GNSS went live in the end of 2016.

The Galileo space segment has right now 26 satellites in space, of which 5 are not usable for the services offered by this GNSS [14], but will include, once fully deployed, a constellation of 30 MEO satellites (including 6 spares).

The Galileo Initial Services (GIS) which are currently available and offered are the Open Service (OS), the Public Regulated Service (PRS) and the Search-and-Rescue service (SaR) [7]. OS is the freely accessible service that targets the mass market and is intended for motor vehicle navigation and location-based mobile telephone services in high-volume satellite radio navigation applications scenarios. It requires no authentication and it is expected that this service is used along with GPS to improve performance in severe environments, or with GNSS Augmentation techniques if one needs to achieve higher precision without the necessity of integrity. For sensitive applications there is PRS which, like PPS for the GPS, is restricted to government or otherwise authorised users. The last service of GIS is SaR, a service that is the European contribution to the international COSPAS-SARSAT co-operative effort on humanitarian search and rescue activities. SaR helps to forward distress signals to a rescue coordination centre by detecting emergency signals transmitted by beacons and relaying messages to them. Moreover, since for Galileo system there is always at least one satellite which is in view of any point on Earth, we can achieve near real-time distress alerts.

Once the satellite constellation and the ground infrastructure will be completed, another service will also be available, the High Accuracy Service (HAS)[‡]. The HAS is complementary to OS and it provides an additional navigation signal and added value services in a different frequency band, allowing the user to obtain an accuracy to the nearest centimetre. Like OS, this service does not offer integrity information, but, in addition to high accuracy, it can offer the authentication of the information encoded in the signal and the signal Time of Arrival (TOA)[§]. [8]

[‡]It is a rescope of the former Galileo Commercial Service (CS).

[§]While integrity protection protects a receiver from, for example, satellite failures (orbit or clock), this one provides a defense against threats, such as jamming and spoofing, due to the use of encryption.

2.1.3 GLONASS

The former Soviet Union developed in the 1980s the GLObal'naja NAvigacionnaja Sputnikovaja Sistema (GLONASS), its own GNSS operated by Russian military but also available for civilian use, with the first test satellite launched on 12 October 1982. GLONASS was then finally deployed with full operational capability (24 satellites) in 1995. However, due to the dismantling of the USSR, by 2002 the constellation had dropped to as few as seven satellites. It is because of the support by the Russian government that GLONASS was reborn and reached full operational capability again on 8 December 2011.

The services offered by GLONASS are the same given by the GPS, SPS and PPS.

2.1.4 BeiDou

Started as a regional navigation satellite system with a program of research and development that began in 1980, also the Chinese BeiDou Navigation Satellite System (BDS, formerly known as COMPASS) is now a GNSS operated by the Chinese Spacial Agency CNSA.

There were 3 stages in the development of this GNSS that has brought us to the present BeiDou. The first, which was from 2000 to 2006, was the BeiDou-1 and it was a regional navigation satellite system. It consisted of 4 satellites in geostationary orbit (GEO), which means that the system did not need a large constellation of satellites, but obviously it limited the coverage to areas on Earth where the satellites were visible. From 2007 to 2019, the second version of BDS, the BeiDou-2, which planned to have a constellation of 35 satellites: 5 in GEO for backward compatibility with BDS-1, 27 in MEO and 3 in inclined geosynchronous orbit (IGSO), was the first Chinese test for a GNSS. It reached the full operational capability at the end of 2012 with 16 satellites in orbit of which 14 were in service and it covered China and its surrounding regions. To achieve full global coverage, from 2015 CNSA started the new GNSS project, BeiDou-3, and planned for it to include 5 GEO satellites, 3 IGSO satellites and 24 MEO satellites. It is expected to become operational by 2020 and it will offer 2 global services, Open Service (OS, similar to the GPS one) and Authorized Service (AS), and 2 regional services, Wide Area Differential Services (WADS) and Short Message Service (SMS).

Currently there are in space: no operational BDS-1 satellites, 15 operational BDS-2 satellites and 28 BDS-3 satellites of which 19 operational and 9 in testing. [15]

2.1.5 Compatibility and Interoperability

As we have just seen, there exist more global navigation satellite systems and, without taking into consideration possible political reasons behind this situation, the technical cause for it is that a single GNSS may not be enough to guarantee user performances. This leads us to two main problems [16]:

- *Compatibility*: different systems should not interfere with each other.
- *Interoperability*: we would like to use these systems, that are independent by design, together to provide better capabilities at user level.

The United Nations' International Committee on Global Navigation Satellite Systems (ICG), which promotes voluntary cooperation on matters of mutual interest related to civil satellite-based positioning, navigation, timing (PNT) and value-added services, has encouraged coordination among providers of GNSS, but also regional systems and augmentations, about these topics for years.

The compatibility issue was addressed, specifically between GPS and Galileo but then also for other systems, by the EU-US Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications in 2004 [17]. This document has set up the models and methodology for the radio frequency compatibility of satellite navigation systems.

As regards interoperability, Galileo was designed to be interoperable with GPS and BeiDou achieved it in 2017. As regards GLONASS, even if a working group about this topic was established in 2004 and had a "successful meeting" in 2006, everything about this collaboration seems on hold from April 2014. It should be said that it is anyway possible to use a receiver that uses GLONASS and other GNSS constellations to achieve better results. This is because the Russian GNSS is considered system interoperable, so, from GPS and GLONASS, we will obtain the same measurements within the specified accuracy of each individual system, and those may be used together to achieve higher accuracy. [18]

2.2 GNSS signals

GNSS satellites continuously transmit navigation signals at two or more frequencies in L band. These signals contain ranging codes and navigation data to allow users to compute both the travel time from the satellite to the receiver and the satellite coordinates at any epoch. The main signal components are described as follows:

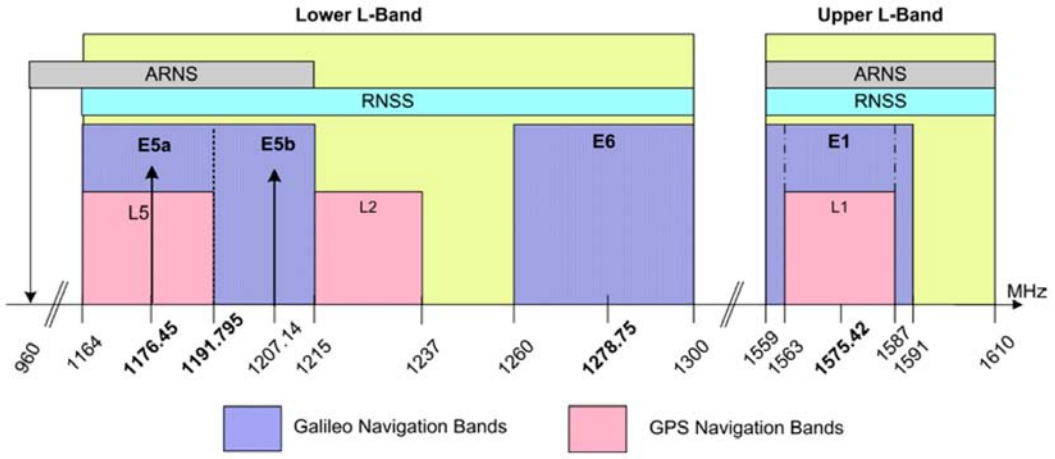


Figure 2.1: GPS, Galileo navigational frequency bands. [20]

- *Carrier*: radio frequency sinusoidal signal at a given frequency f_{RF}.
- *Ranging code*, $C(t)$: sequences of zeros and ones which allow the receiver to determine the travel time of the radio signal from the satellite to the receiver. They are called PRN sequences or PRN codes.
- *Navigation data*, $D(t)$: a binary-coded message providing information on the satellite ephemeris (pseudo-Keplerian elements or satellite position and velocity), clock bias parameters, almanac (with a reduced-accuracy ephemeris data set), satellite health status and other complementary information.

GNSS signals are usually transmitted with quadrature modulation using Right-Hand Circular Polarization (RHCP), and the overall transmitted signal, the Signal-in-Space (SIS), can be expressed as:

$$s(t) = \sqrt{2P}C(t)D(t)\cos(2\pi f_{RF}t + \varphi_0), \tag{2.1}$$

where P is the average power of the sinusoidal signal and φ_0 is the initial phase. C and D have an amplitude of ± 1 varying with time. [19]

In the next sections I will focus on GPS and Galileo signals description, since those are the system with which I have made the tests for this thesis.

2.2.1 The GPS signal

Legacy GPS signals are transmitted on two radio frequencies, L1 and L2, and their frequencies are derived from a fundamental frequency, $f_0 = 10.23MHz$, generated by onboard

atomic clocks:

- $f_{L1} = 154 \times 10.23MHz = 1575.420MHz$
- $f_{L2} = 120 \times 10.23MHz = 1227.600MHz$

where L1 is used by SPS while PPS is a dual frequency service that uses both L1 and L2.

To send different signals on the same radio frequency, GPS uses the Code Division Multiple Access (CDMA) technique and the Binary Phase Shift Keying (BPSK) as modulation method.

The following types of PRN codes and messages are modulated over the two carriers

- *Coarse/Acquisition (C/A) code*, also known as *civilian code*, $C(t)$: this sequence contains 1023 bits and is repeated every millisecond (*i.e.* a chipping rate of 1.023 Mbps). Then, the duration of each C/A code chip is 1 μs, which means a chip width or wavelength of 293.1 m. This code is modulated only on L1. The C/A code defines the SPS.
- *Precision code*, $P(t)$: This is reserved for military use and authorised civilian users. The sequence is repeated every 266 days (38 weeks) and a weekly portion of this code is assigned to every satellite, called the PRN sequence. Its chipping rate is 10 Mbps, which leads to a wavelength of 29.31 m. It is modulated over both carriers L1 and L2. This code defines the PPS.

  In order to protect military receivers against an adversary transmitting a faulty copy of the GPS signal to mislead the receiver, and to deny access of non-authorized users to the precise ranging code P, the latter is encrypted by combining it with a secret W code (called security code), resulting in the Y code, which is modulated over the two carriers L1 and L2.

So, the SIS transmitted by a GPS satellite takes the following form:

$$s(t) = s_{L1}(t) + s_{L2}(t), \tag{2.2}$$

where

$$\begin{aligned} s_{L1}(t) =& \sqrt{2P_{P,1}} W(t) C(t) D(t) \sin(2\pi f_{L1} t + \varphi_{L1}) + \\ &+ \sqrt{2P_C} C(t) D(t) \cos(2\pi f_{L1} t + \varphi_{L1}), \end{aligned}$$

$$s_{L2}(t) = \sqrt{2P_{P,2}} W(t) P(t) D(t) \sin(2\pi f_{L2} t + \varphi_{L2}).$$

Link	Carrier freq. (MHz)	PRN code	Modulation type	Code rate (Mcps)	Data rate (bps)	Service
L1	1575.420	C/A	BPSK(1)	1.023	50	Civil
		P	BPSK(10)	10.23	50	Military
		M	BOCsin(10,5)	5.115	N/A	Military
		L1C-I data	MBOC(6,1,1/11)	1.023	50	Civil
		L1C-Q pilot			-	
L2	1227.600	P	BPSK(10)	10.23	50	Military
		L2C M	BPSK(1)	1.023	25	Civil
		L2C L			-	
		M	BOCsin(10,5)		N/A	Military
L5	1176.450	L5-I data	BPSK(10)	10.23	50	Civil
		L5-Q pilot			-	

Table 2.2: GPS navigation signals. [4]

Recently there was a GPS modernisation which brought to us an additional frequency L5 ($f_{L5} = 115 \times 10.23MHz = 1176.450MHz$), for life critical applications, and several new ranging codes on the different carrier frequencies (civilian signals L2C, L5C, L1C and the military M-code, which have different modulation methods). For more details about GPS signals and frequencies see Table 2.2.

Since a receiver needs to know the time and position of each active satellite, GPS encodes this information into the navigation message and modulates it over both carriers at 50 bps. In particular, what are contained in the navigation message are 25 frames of 30 s each, for a total of 12.5 min of transmission, which in turn is subdivided in five sub-frames of 6 s each. Every sub-frames, then, consists of 10 words with 30 bits per word.

Every sub-frame always starts with the telemetry word TLM, for synchronisation, and the transference word (HOW), which provides the seconds of the GPS week that allow the receiver to acquire the week-long $P(Y)$ code segment. Except for these fixed elements, the contents of every sub-frame are as follows:

- *Sub-frame 1 – Satellite Clock and Health Data*: contains, first of all, clock information, which is needed to compute at what time the navigation message is transmitted from the satellite. Additionally, this sub-frame also contains health data indicating whether or not the data should be trusted.

- *Sub-frames 2 and 3 – Satellite Ephemeris Data*: contain the satellite ephemeris data. The ephemeris data relate to the satellite orbit and are needed to compute a satellite position.

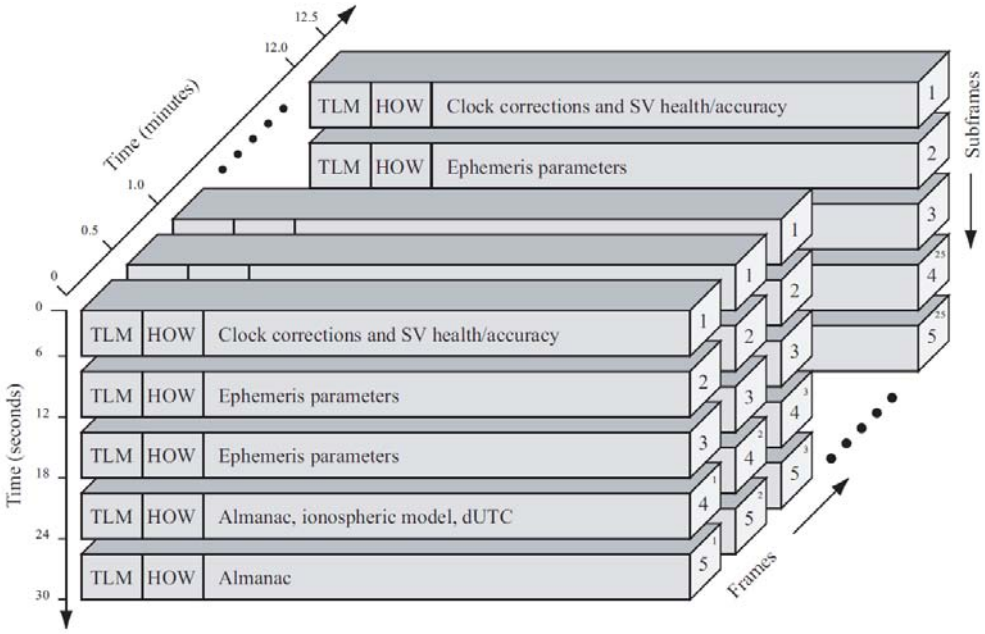


Figure 2.2: GPS navigation message. [3]

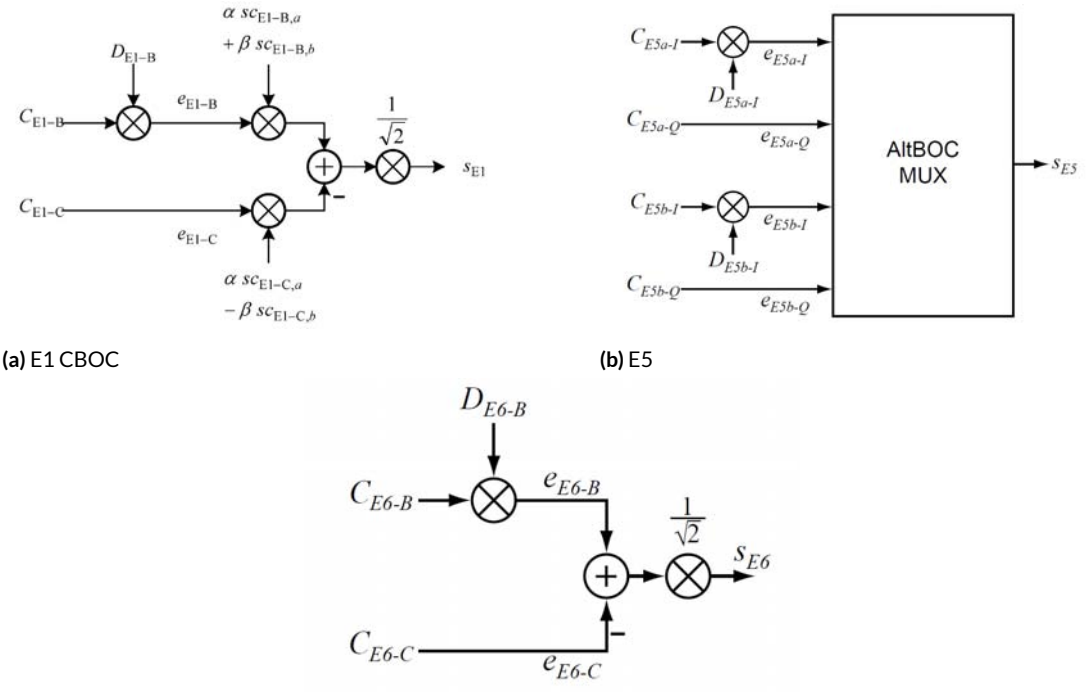
- *Sub-frames 4 and 5 – Support Data*: the last two sub-frames contain almanac data, which are the ephemerides and clock data with reduced precision. Additionally, each satellite transmits almanac data for all GPS satellites while it only transmits ephemeris data for itself. The remainder of sub-frames 4 and 5 contain various data (*e.g.* UTC parameters, health indicators, and ionospheric parameters).

2.2.2 The Galileo signal

The Galileo system transmits three signals: E1, E5 (consisting of E5a and E5b) and E6:

- $f_{E1} = 1575.420 MHz$
- $f_{E5a} = 1176.450 MHz$
- $f_{E5b} = 1207.140 MHz$
- $f_{E6} = 1278.750 MHz$

where E1 supports OS and PRS, E5a and E5b only OS, and E6 is used for PRS. When HAS will be available, it will be supported by E1, E5b and E6.



(a) E1 CBOC **(b)** E5

(c) E6

Figure 2.3: Modulation scheme for Galileo signals: E1 CBOC in 2.3a, E5 in 2.3b and E6 in 2.3c [20].

As regards Galileo SIS, it is comparable to GPS one except for the fact that we have more signals[¶]. In Fig. 2.3 you can see more details about Galileo signals.

As in GPS, all satellites share the same frequencies and the signals are differentiated by the CDMA technique. Moreover, some signals can contain data and pilot channels but, while they both provide ranging codes, only the data channel also includes navigation data. So, the pilot channel, which is considered a data-less channel, is needed to help tracking weak signals. For more details see Table 2.3.

Regarding Galileo navigation message, the Galileo SIS data channels transmit different message types according to this subdivision:

- *F/NAV message type*: for the OS on E5a-I.
- *I/NAV message type*: for the OS on E5b-I and E1-B[‖].

As we can see in Fig. 2.4, we have differences in the navigation message size based on the message type.

[¶] Galileo signals are more like the modernised version of GPS signals instead of the original ones.
[‖] E1-B will be also for the HAS in the future

Band	Carrier freq. (MHz)	Channel or sig. comp.	Modulation type	Code rate (Mcps)	Data rate (bps)	Service
E1	1575.420	E1-A data	BOCcos(15,2.5)	2.5575	N/A	PRS
		E1-B data	MBOC(6,1,1/11)	1.023	125	OS, HAS
		E1-C pilot			-	
E5a	1176.450	E5a-I data	BPSK(10)	10.23	25	OS
		E5a-Q pilot			-	
E5b	1207.140	E5b-I data	BPSK(10)	10.23	125	OS
		E5b-Q pilot			-	
E6	1278.140	E6-A data	BOCcos(10,5)	5.115	N/A	PRS
		E6-B data	BPSK(10)		500	HAS
		E6-C pilot			-	

Table 2.3: Galileo navigation signals. [4]

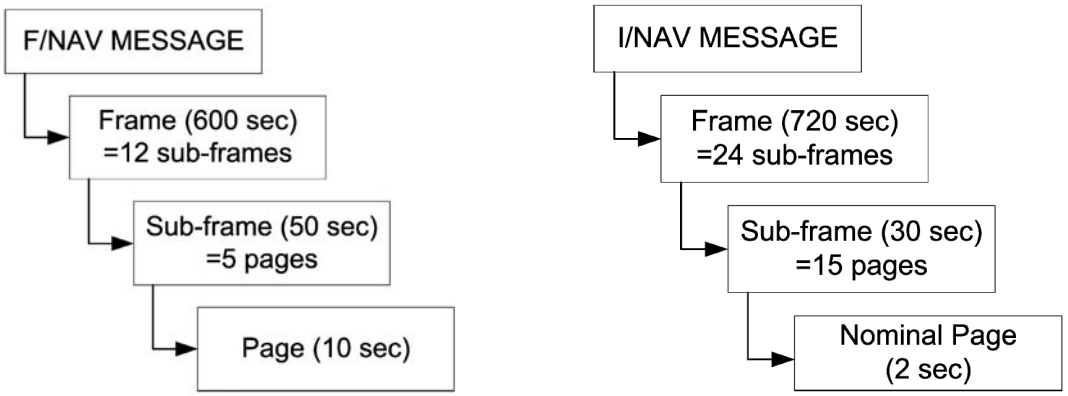
In the F/NAV message, every sub-frame always starts with the page type field (6 bits), which is needed to identify the page content, then there is the navigation data field (208 bits) and a CRC (24 bits). In particular, each sub-frame is composed as follows:

- *Page 1*: contains SVID, clock correction, SISA, ionospheric correction, BGD, Signal health status, GST and Data validity status.
- *Page 2, 3 and 4*: contain ephemeris, GST, GST-UTC conversion, GST-GPS conversion and TOW.
- *Page 5 and 6*: contain almanac of one satellite and part of the almanac of another one.

As regard I/NAV instead, we have two types of pages:

- *Nominal pages*: having a duration of 2 seconds, they are transmitted sequentially in time in two parts of duration 1 second each on each of the E5b-I and E1-B components.
- *Alert pages*: having a duration of 1 second, they are transmitted in two parts of duration 1 second each at the same epoch over the E5b-I and E1-B components. This transmission is repeated at the next epoch but switching the two parts between the components.

The content of each sub-frame, even if in a different order, is the same of the F/NAV message type, clearly with different layout given that the service provided on these frequencies is a dual-frequency service.



(a) F/NAV **(b)** I/NAV

Figure 2.4: Galileo navigation messages: F/NAV in 2.4a, I/NAV in 2.4b. [20]

2.3 GNSS architecture

A GNSS basically consists of three main segments (see Fig. 2.5):

- the *space segment*, which comprises the satellites;
- the *control* (or *ground*) *segment*, which is responsible for the proper operation of the system;
- the *user segment*, which includes the GNSS receivers providing positioning, velocity and precise timing to users.

In the following paragraphs there will be a brief description of the first two segments, but then I will focus more on the receiver part for the remaining part of the section.

2.3.1 Space segment

The main functions of the space segment are to generate and transmit code and carrier phase signals, and to store and broadcast the navigation message uploaded by the control segment. These transmissions are controlled by highly stable atomic clocks onboard the satellites.

The GNSS space segments are formed by satellite constellations with enough satellites to ensure that users will have at least four satellites in view simultaneously from any point on Earth's surface at any time (see Fig. 2.6).

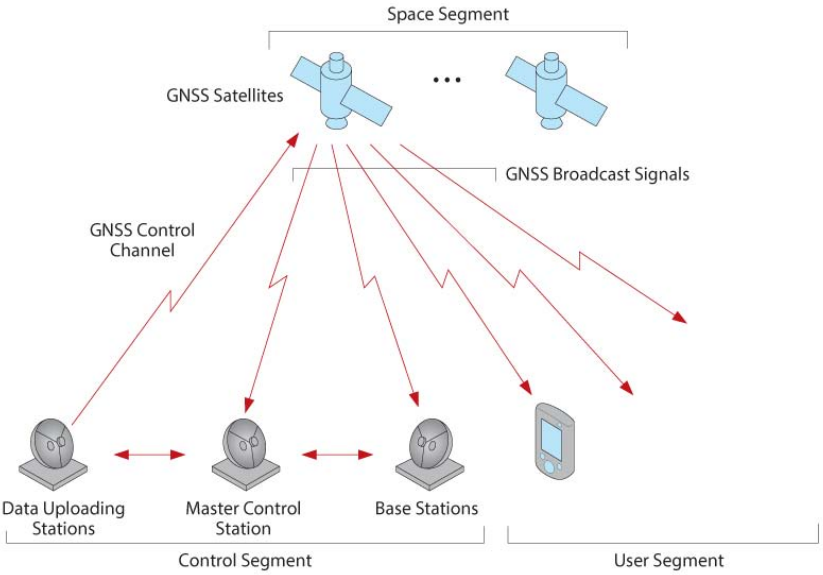


Figure 2.5: GNSS architecture. [21]

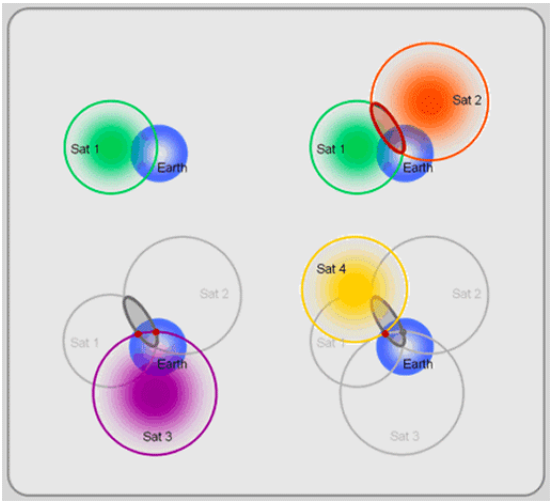


Figure 2.6: GNSS trilateration. [22]

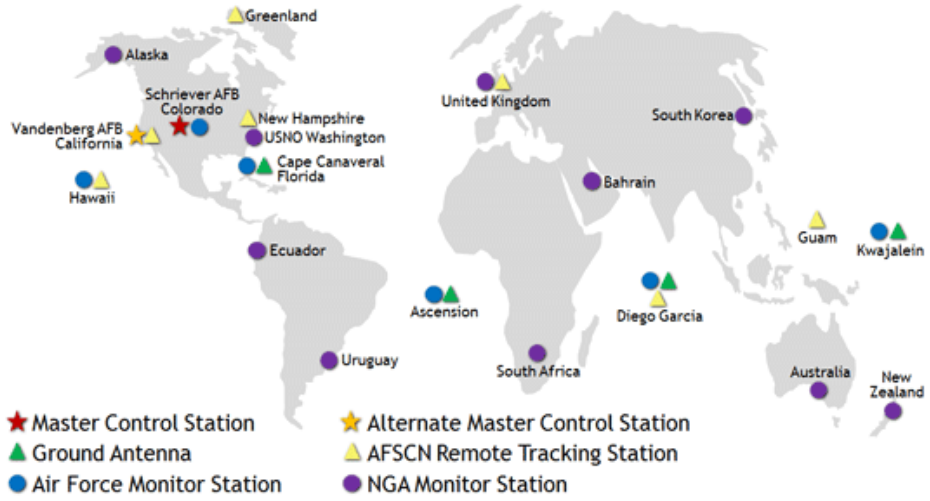


Figure 2.7: GPS control segment map. [23]

2.3.2 Control segment

The control segment (also referred to as the ground segment) is responsible for the proper operation of the GNSS. Its basic functions are:

- to control and maintain the status and configuration of the satellite constellation;
- to predict ephemeris and satellite clock evolution;
- to keep the corresponding GNSS time scale (through atomic clocks);
- to update the navigation messages for all the satellites.

Since the control performed by the ground segment is essential to ensure that the information obtained from the users' receivers are correct, an extensive distribution of monitoring and control stations, and ground antennas are needed to always reach each satellite. See in Fig. 2.7 an example for the GPS control segment.

2.3.3 User segment

The user segment is composed of GNSS receivers. Their main function is to receive GNSS signals, determine pseudoranges (and other observables) and solve the navigation equations in order to obtain the coordinates and provide a very accurate time.

A conventional GNSS hardware receiver is basically composed of the analog part, the digital part including the application processor, and the interfaces for input-output.

Antenna

The basic purpose of a GNSS user antenna, operating in the L-band of the radio frequency spectrum, is the reception of navigation signals from all visible GNSS satellites. Anyway, this is not a simple task since received GNSS signals from satellites are notoriously weak, and also they can arrive from, virtually, any direction with signals from different satellites arriving simultaneously.

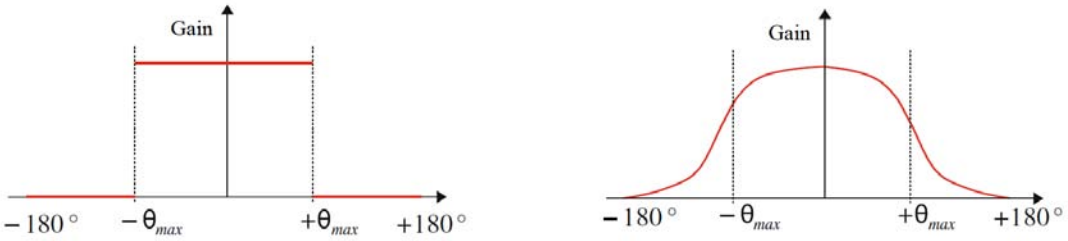
Some parameters that defines, or affects, GNSS antennas functionality are:

- *Frequency coverage*: as we have seen in Table 2.1, there are a lot of frequency bands available for satellite navigation purposes, so the antenna may need to cover some or all of these bands. This, together with size requirements, makes the antenna harder to design.
- *Gain pattern*: the gain is the ratio of the power delivered by the antenna in response to a signal arriving from a given direction compared to that delivered by a hypothetical isotropic reference antenna. The spatial variation of an antenna's gain is referred to as the radiation pattern and, under the antenna reciprocity theorem and by ignoring losses, this is equal to the gain pattern. In a "theoretical world" the antenna should cover the entire hemisphere above it with no variation in gain (see Fig. 2.8a). But, since in the "real world" we also have to consider multipath rejection and antenna noise temperature, we have some roll-off (see Fig. 2.8b).
- *Multipath suppression*: except for the GNSS signals that arrives directly from the satellite to the receiver's antenna, they may also be reflected off the ground, buildings, or other obstacles, and arrive at the antenna multiple times and delayed in time, therefore, degrading positioning accuracy. This is what is called multipath and the problem introduced by it is due to the fact that reflected signals typically contain a large LHCP component. Usually LHCP reflections that arrive at the antenna at high elevation angles are not a problem because the axial ratio (AR)** tends to be quite good at these elevation angles and, therefore, the reflection will be suppressed. On the other hand, at lower elevation angles, to improve the results it makes sense to have some level of gain roll-off towards these elevation angles, even if a good AR is also required.

From equation 2.1, the received signal for a visible satellite at the end of a receiver antenna can be modelled as:

$$r_{RF}(t) = a\sqrt{2P}D(t - t_p)C(t - \tau)\cos[2\pi(f_{RF} + f_D)(t - t_p) + \varphi_0] + n_{RF}(t), \quad (2.3)$$

** Axial ratio is the measure of the polarization ellipticity of an antenna designed to receive circularly polarized signals. It is best when AR is close to 1, or 0, dB.



(a) Theoretical antenna

(b) "real world" antenna

Figure 2.8: Antenna gain (in dBi) patterns. [24]

with

$$f_D = -\frac{f_{RF}}{c}\frac{dt_p}{dt},$$

where a is the path attenuation, t_p is the propagation time, τ is the propagation time modulo the code period, denoted as code delay, f_D is the carrier Doppler frequency shift (Hz) and $n_{RF}(t)$ is the additive noise component at RF.

Front-end

The GNSS signal obtained by the receiver's antenna is then given to the front end. This part is then responsible for the first handling of the received signals for the following signal processing tasks. The different steps performed at the receiver's front-end are the following:

- *Filtering and amplification*: since the received GNSS signal has low power, after the antenna there is a set of filtering and low-noise amplification stages. These are needed to amplify the signal, to compensate for transmission losses, while keeping the noise figure low and rejecting possible out-of-band interference.

- *Down-conversion*: this stage's main objective is to convert the input signal from RF to IF and/or to baseband. This is achieved through the local oscillator (LO) which deals with signal mixing operations. These operations are the mixing of two different frequency signals in order to shift the same information at two different frequencies, where one is the sum of the two frequencies mixed, while the other is their difference.

- *Automatic Gain Control (AGC)*: in this stage, the AGC is responsible for adjusting the gain of the front-end section in order to take benefit from the full dynamic range. The most common implementation is to adjust the signal gain depending on incoming signal levels, for example by estimating the noise standard deviation.

- *Quantization*: after the down-conversion, the incoming signals are digitized through analog to digital converters (ADC), ensuring that quantization errors and dynamic ranges are appropriate to accommodate the signal's characteristics.

From the signal received by the antenna, the signal at the end of the front-end, for a single satellite, can be modelled as

$$\begin{aligned} r_{IF}(t) = r_{IF}(k;\tau;\varphi;f_D;A) =& AD(kT_s - t_p)C(kT_s - \tau)\cos[2\pi(f_{IF} + f_D)kT_s + \varphi] \\ &+ n_{IF}(t) \quad \text{for } k = 0, 1, 2, ..., \end{aligned} \tag{2.4}$$

where T_s is the sampling time interval (s) such that $t = kT_s$ and n_{IF} is the corresponding noise at IF.

Obtaining observables

After having down-converted and digitized a GNSS signal we can obtain, from the baseband processing block, observables, that are code pseudo-ranges and carrier phase measurements, and navigation data.

The digital processing of a GNSS signal in a channel starts with the acquisition, which is the detection that a signal is present. During this time frame coarse estimates of the code delay and Doppler of the signal are determined in feed-forward manner, and then the channel switches to code and carrier tracking to refine the estimates in a feedback structure.

Correlator method In order to detect and track the GNSS signals, the receiver employs the auto-correlation principle. It generates a transmitted GNSS signal copy of a single satellite inside the receiver and correlates this replica signal with the received signal. If the signal parameters in terms of code phase and Doppler shift match reasonably well, then the correlation value increases. The correlation is realized as an integration of the product of received and replica signal.

The replica signal can be modelled as

$$\hat{r}_{IF}(t) = \hat{r}_{IF}(k;\hat{\tau};\hat{\varphi};\hat{f}_D;\hat{A}) = 2C(kT_s - \hat{\tau})e^{j[2\pi(f_{IF}+\hat{f}_D)kT_s+\hat{\varphi}]} \tag{2.5}$$

and, by replacing $\Theta = 2\pi(f_{IF} + f_D)kT_s + \varphi$ and $\hat{\Theta} = 2\pi(f_{IF} + \hat{f}_D)kT_s + \hat{\varphi}$, we have

that the correlation function is

$$corr[r_{IF}(k), \hat{r}_{IF}(k)] = \sum_{k=1}^{M} r(k)\hat{r}(k) \tag{2.6}$$

where M is the number of samples within the integration time $T = MT_s$, which is usually shorter or equal to the navigation data bit/symbol period. From [6] we obtain that

$$\begin{aligned} corr[r_{IF}(k), \hat{r}_{IF}(k)] &= \bar{A}DR(\delta\tau)sinc(\delta f_D T)e^{j\delta\varphi} + \eta = \\ &= I + jQ \end{aligned} \tag{2.7}$$

where $\hat{A}$ is the amplitude of the baseband signal component assuming a normalized noise component, η is the noise after correlation operation, $R(\delta\tau)$ is the normalized correlation function of $C(kT_s)$, $\delta\tau$ is the code delay error (s), $\delta\varphi$ is the carrier-phase error (rad) and δf_D is the Doppler error (Hz). Finally, I and Q represent post-correlation values in in-phase and quadrature components respectively.

$$\begin{aligned} I &= \bar{A}DR(\delta\tau)sinc(\delta f_D T)\cos(\delta\varphi) + \eta_I \\ Q &= \bar{A}DR(\delta\tau)sinc(\delta f_D T)\sin(\delta\varphi) + \eta_Q \end{aligned}$$

Acquisition The purpose of acquisition is to determine visible satellites and coarse values of carrier frequency and code-phase of the satellite signals. These values will be then refined during the tracking. During search and acquisition stage a correlation function is computed and compared to a specific threshold, then, if the correlation value exceeds that level, the signal is declared to be present and the position of the peak are the coarse estimates (see Fig. 2.9).

Tracking After acquisition stage is completed, the GNSS receiver start the tracking stage, which is characterized by tracking loops that are designated to adjust the input of the local replica signal generators to match the received signals. There are three different tracking loops architectures: Delay Lock Loop (DLL), for code delay tracking; Phase Lock Loop (PLL), for carrier-phase tracking; finally the Frequency Locked Loop (FLL), for carrier Doppler frequency shift tracking.

During tracking the channel synchronizes to the broadcast navigation data message and de-

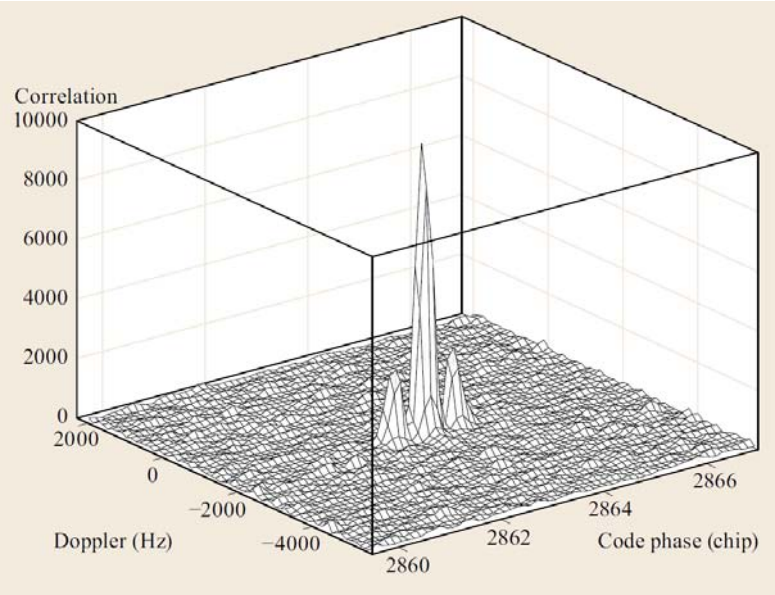


Figure 2.9: Correlation function for a Galileo satellite at low elevation. [6]

codes it. The decoded bit information contains the satellite's ephemeris and almanac, system time information, and meteorological parameters. The information from code and carrier tracking blocks together with time synchronization information is used to generate the primary measurements of GNSS. Using these, finally, the navigation unit computes the GNSS navigational equation to obtain the user position, velocity and timing (PVT) information.

3

GNSS threats

GNSS ARE INCREASINGLY BEING RELIED UPON for safety-related and commercially sensitive applications, such as autonomous vehicles and time-synchronization, so these systems have become an attractive target for illicit exploitation by different types of attackers for different reasons. Given also that the GNSS signals' power is very low when they reach Earth surface (about -160 dBW), even a low-power interference can easily jam or spoof GNSS receivers within a radius of several kilometres. This ease of attack, together with the technological advance, implies that the number of threats to the different systems is constantly increasing and they are becoming more sophisticated.

The range of threats and vulnerabilities that can impact a navigation satellite system is rather wide (see Fig. 3.1) and they can be mainly classified into intentional or unintentional. What we will focus on in this thesis are two intentional threats which are jamming, a Denial of Service (DoS) attack, and spoofing, which consists of sending forged GNSS signals to the receiver.

3.1 Jamming

Jamming is probably the easiest type of attack one can perform on GNSS signals, as it does not need previous knowledge about them. The classic jamming attack is a form of RFI generated by devices, called jammers (see Fig. 3.2), which deliberately transmit powerful signals at

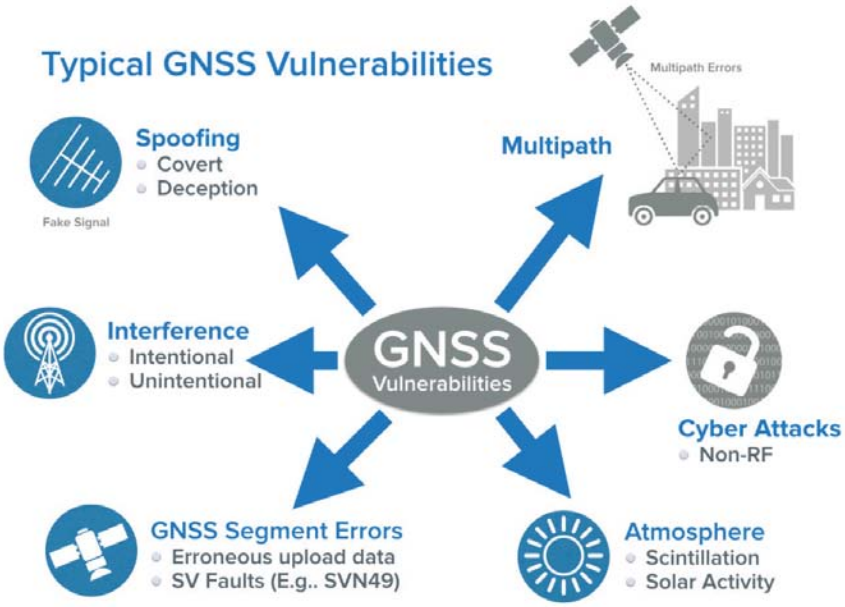


Figure 3.1: Typical GNSS vulnerabilities. [25]

the GNSS frequencies. The interference signals can be, for example, continuous wave, wide-band or narrow-band radio frequency signals, or chirp signals, and the higher power has the jamming signal, the more damage will be caused and the further it will reach.

- *Continuous wave*: is a signal with constant amplitude A and frequency f_{CW}, typically a sine. So a continuous wave jamming signal $q(t)$ can be modeled as

$$q(t) = A\sin(2\pi f_{CW} t).$$

- *Broad or narrow band AWGN*: AWGN is generated by a series of Gaussian independent and identically distributed variables X_i, with uniform power σ^2 across the whole frequency band, and zero mean. So each variable can be modeled as

$$X_i \sim \mathcal{N}(0, \sigma^2),\ X_i \perp X_j \quad \forall i \neq j.$$

- *Chirp signal*: chirp signal sweeps the frequency from low to high frequency linearly. It can be modeled as a sinusoidal wave that increases in frequency linearly over time

$$q(t) = A\cos(2\pi(f_0 + \alpha t)t),$$

where f_0 is the starting frequency, and α is the frequency variation rate.

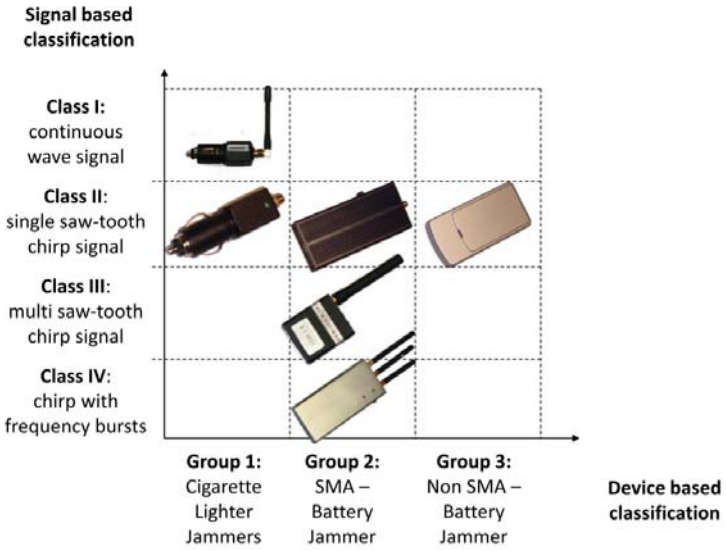


Figure 3.2: Composite jammer classification accounting for both signal and device characteristics. [26]

With this type of attack, the recovery time for a receiver may be of a few seconds, or several minutes (based also on the receiver quality), after the interference is eliminated. Depending on the receiver part that is affected by the jamming threat, usually there could be three different consequences:

- *Front-end*: in the presence of strong jamming signals several elements of the front-end (filters, amplifiers) may be led to work outside their nominal regions, generating, for example, clipping phenomena (signal amplitude exceeding the hardware capability to treat them). In Fig. 3.3 we can see the impact of jamming on AGC count, which is significantly reduced by the threat.
- *Acquisition*: as said in 2.3.3, the main operation performed by the acquisition block is to correlate input signal with local replicas of the signal code and carrier. In this respect, the cross-ambiguity function (CAF) is evaluated, in which, when the GNSS signal is present and in the absence of interference, a single dominant peak should appear. The peak reveals the signal presence and it is located at the approximate signal code delay and Doppler shift. As we can see in Fig. 3.4, in the presence of a jamming attack the peak-to-noise-floor separation decreases as the interfering power increases.
- *Tracking*: since this stage is in charge of generating GNSS measurements such as pseudoranges, Doppler, carrier phase and the amplitude of the received signals, what a jamming attack causes is a quality deterioration of these measurements. In Fig. 3.5 we can see the shifted results, caused by a jammer on a u-blox receiver, with respect to the true coordinates.

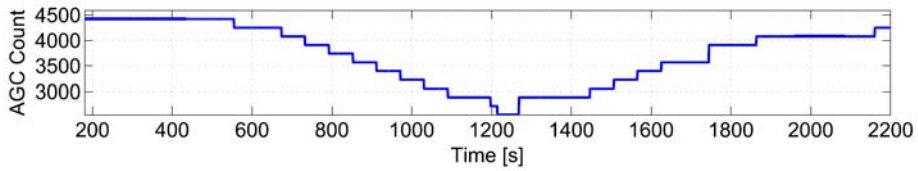


Figure 3.3: Impact of jamming on a GNSS receiver on AGC count. [26]

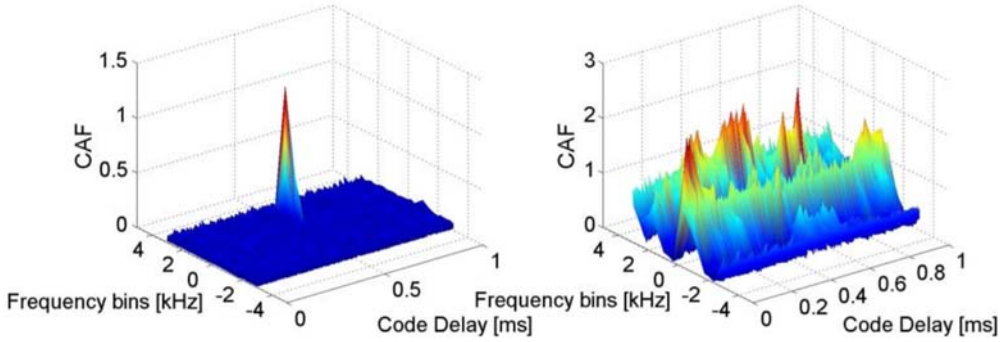


Figure 3.4: Comparison of the CAF for a GPS L1 C/A acquisition search space in an interference-free environment (left) and in the presence of an in-band CW signal at -130 dBW (right). [26]

In the following sections, and in the next chapter, I will use many times the carrier-to-noise density power ratio C/N_0, that is the ratio of the signal power P and noise PSD N_0. The C/N_0 is continuously estimated by the receiver and it is usually provided in logarithmic units, dB-Hz. It is used to characterize the relation between signal and jamming powers.

3.1.1 Jamming attacks

The classification of jamming attacks to GNSS takes into account several different parameters, so, as we can see in Fig. 3.6, we can describe a jamming signal in the frequency and time domain, with antenna directionality and also the specific jammer's waveform modulation.

Given this parameters it is possible to define any possible jamming attack as we can see from Table 3.1, where some examples of threats are listed taken from [28] and [29]:

- *Spot jamming*: occurs when a jammer focuses all of its power on a single frequency.
- *Sweep jamming*: the jammer attacks multiple frequencies one at a time in quick succession.
- *Barrage jamming*: also this attack threatens multiple frequencies, but, unlike sweep jamming, does it simultaneously.

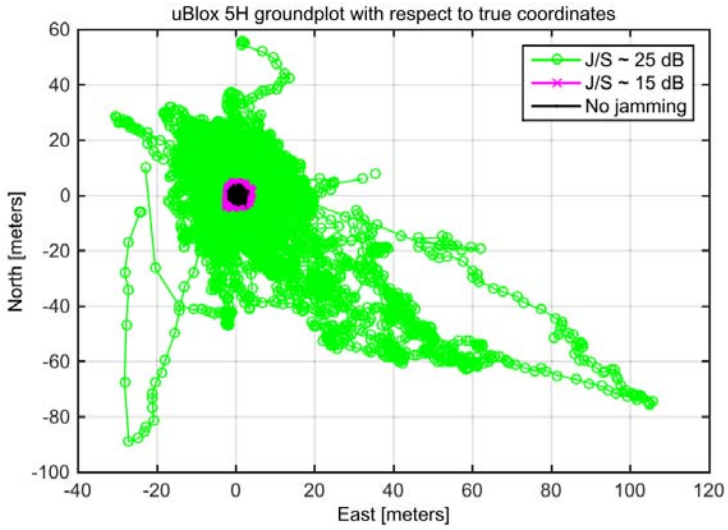


Figure 3.5: Positioning results around the true coordinates of U-Blox 5H receiver in a single-frequency jamming test. [26]

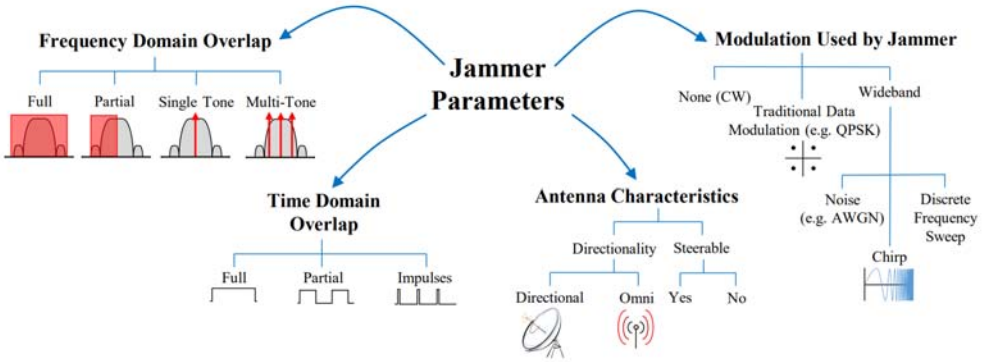


Figure 3.6: Jammer parameters organized into trees. [27]

		Spot jamming	Sweep jamming	Barrage jamming	Systematic jamming
Frequency domain	Full band		×	×	
	Partial band				
	Single-tone	×			
	Multi-tone				×
Time domain	Full time	×	×	×	
	Partial time				
	Impulses				×
Modulation used by the jammer	CW	×			×
	Traditional data modulation				
	AWGN			×	
	Chirp		×		×
	Discrete frequency sweep				

Table 3.1: Classification of specific jamming attacks.

- *Systematic jamming*: jamming attack synchronized with GNSS signals, with the intention of causing maximum disruption with the minimum power expenditure.

3.1.2 Jamming detection

Clearly, given what I have described in the previous paragraph, what a GNSS user needs is a means to detect the jamming attack, at least to give him/her a notification about the threat. And, in the end, it all comes down to a binary hypothesis testing problem where it is necessary to decide between

- H_0: absence of interference

$$y[n] = s[n] + w[n] \qquad \text{for } n = 0, 1, ..., N-1, \tag{3.1}$$

- H_1: presence of interference

$$y[n] = s_{IF}[n] + vq[n] + w[n] \qquad \text{for } n = 0, 1, ..., N-1, \tag{3.2}$$

where $w[n]$ is a realization of a zero-mean white discrete-time Gaussian noise $W[n]$ with variance σ_w^2, v is an amplitude factor, and $q[n]$ is the IF digital version of the signal $q(t)$ generated by a jammer.

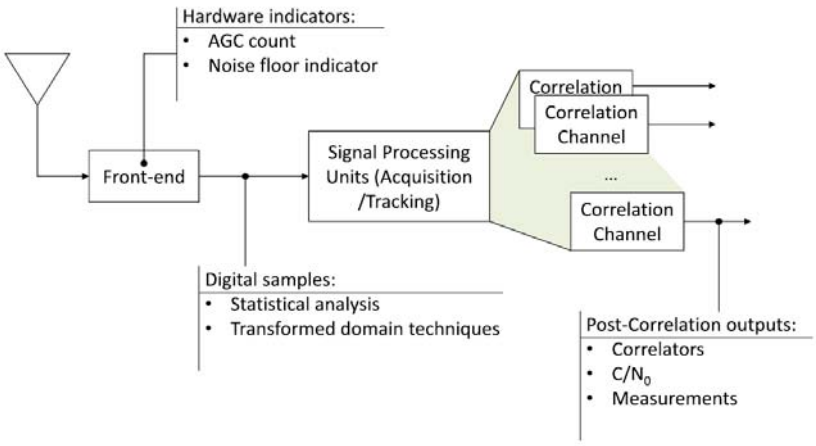


Figure 3.7: Different approaches for jamming detection which can be implemented using measurements from different receiver stages. [26]

In the hypothesis modelling here above, a decision is taken using N digital samples. A general approach is to use such samples and construct a decision statistic D, designed on the basis of, for one, a statistical model describing the behaviour of the digital samples in the absence and in the presence of jamming. A decision between H_0 and H_1 is then taken by comparing D with a decision threshold T_h, which should be chosen such that a constant false alarm rate is obtained. Since this model may be difficult to obtain, T_h is often set using criteria based on Monte Carlo simulations or on empirical results [26]. In Fig. 3.7 we can see what is used to detect a jamming attack in different receiver stages.

3.2 Spoofing

By spoofing attack to the GNSS signals we consider the broadcast of false signals with the intent that the victim receiver will misinterpret them as authentic signals. This may lead to false position fixes, false clock offsets, or both, with the possible outcome that may be, for example, that a hovering drone is sent into an unplanned dive by an attacker.

This type of attack, as one can expect, is more complicated since the spoofer must replicate the RF carrier, PRN/spreading code and data-bits of each open-service GNSS signal that it intends to spoof. Anyway, given the fact that the structure of most civilian GNSS signals is known to the public and also since there has been advances over the years in software defined radio (SDR) technologies, spoofing has become more feasible and less costly.

Spoofing signals can be generated with different techniques that can be more or less com-

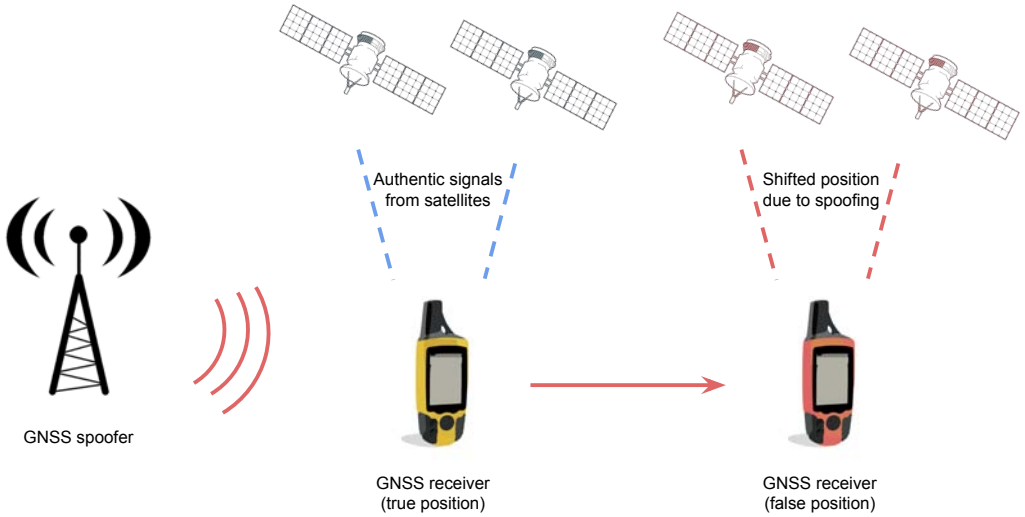


Figure 3.8: GNSS spoofing attack.

plex based on the result the attacker wants to achieve. A simple solution could be the use of a GNSS signal simulator together with a RF transmitter which can send a forged signal, that most likely won't be synchronized with a legit one, to a GNSS receiver which will see the new signal as noise. This, anyway, could be enough to negatively affect the acquisition, or tracking, phase and degrade the receiver measurements. An example of a more complex case is a receiver-based spoofer, which synchronizes itself with the current GNSS signals and extracts the GNSS measurements. After this initial stage, the spoofer generates the spoofing signal and sends it to the target's receiver's antenna.

3.2.1 Spoofing attacks

Based on the target, the spoofing attacks can be divided into signal processing and data level attacks.

Signal level attack

As already said before, the structure of civilian GNSS signals, including the modulation type, PRN signals, transmit frequency, signal bandwidth, Doppler range, signal strength and many other features are publicly known. In this way a spoofer can generate forged signals similar to the one in Eq. (2.3) except for some spoofed parameters so as to effectively

	Lift-off delay and aligned	Meaconing	Selective delay	Jam and Spoof	Nonline of sight spoofing	Trajectory spoofing
Amplitude	×	×	×	×		×
Delay	×		×			×
Doppler phase	×				×	

Table 3.2: Classification of specific spoofing attacks.

mislead its target receiver [30]

$$r_s(t) = a_s\sqrt{2P_s}D(t-t_{p,s})C(t-\tau_s)\cos[2\pi(f_{RF}+f_{D,s})(t-t_{p,s})+\varphi_{0,s}]+n_s(t). \quad (3.3)$$

In Table 3.2 we can see some possible signal processing level attacks from [31] and the description of what they modify.

- *Lift-off delay*: spoofer approaches the authentic signal with a relative delay $\Delta\tau_I(t)$ (and possibly Doppler), adjusting the spoofing signal's power. It's goal is to minimize the delay and at the same time to increase its power so to move the tracking point farther away from the true signal parameters.
- *Lift-off aligned*: as the lift-off delay, but it start with a $\Delta\tau_I(t)$ near zero.
- *Meaconing*: it's a fixed delay ($\Delta\tau_I(t)$ = constant) replica spoofing signal, that can adjust its power levels.
- *Selective Delay*: these attacks are formed by estimating the code chip, replaying them in delay to a user, and thus can be selective in terms of the satellites to be spoofed. In case its power is smaller than the power of the real signal, it can be called *multipath attack* as the spoofing signal looks like a nearby reflected signal.
- *Jam and spoof* : the spoofer forces the receivers into the acquisition mode using a jamming attack that causes loss-of-lock on the authentic GNSS signals. Then the jammer is switched off with the intention that the receiver acquires the spoofing signals.
- *Nonline of sight spoofing*: exploiting the fact that in suburban and urban environments a receiver will, in general, neither be able to track all satellites above the recommended mask angle, nor will it be aware of the surrounding obstructions, the spoofer can transmit signals only for potentially blocked satellites.
- *Trajectory spoofing*: a spoofer with the use of a software-defined radio or a GNSS signal simulator attempts to capture the tracking points of all channels of a receiver along its intended trajectory, forcing the user to follow the spoofed trajectory.

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

Table 3.3: Highest Risk Navigation Data Parameters. [31]

Data level attack

Also the framing structure (*e.g.* almanacs and ephemeris) of a GNSS signal is publicly known and, moreover, the information contained in it does not change in a short time (see Fig. 2.2 and Fig. 2.4). This allows the spoofer to take advantage of this period of time in order to tamper the valid frame and have a different impact on the navigation message based on the modified element (see Table 3.3). In 4.1.2 there will be the description of the software that was created to modify a SDR simulator log file, which contains the single units of a navigation message and is needed in order to create a navigation scenario.

It is clearly possible that both of the previous methods are implemented for a specific attack, since the two types of attacks have different outcomes, and also jamming could be used along with a spoofer to achieve better results.

3.2.2 Spoofing detection

To deal with the spoofing threat there exist several methods, but they can be divided into two categories, *predespreading* and *postdespreading* [32]. In Tab. 3.4 we can see a summary of the methods described in the following paragraphs.

Predespreading detection

The techniques that belongs to this detection method rely on the assumption that interfering signals are more powerful than the authentic ones. Predespreading methods evaluate the overall power content of the received signal set without separately analyzing different PRN signals. This category of detection looks for any abnormal variation in the received signal power prior to the despreading process in the receiver. Some examples of this type of spoofing detection metrics are

- *Baseband variance analysis*: it monitors the variance of baseband signals in order to detect additional power injected by interfering signals. This method does not take advantage of any spoofing signal features and simply assumes that the spoofing signals' power content elevates the ambient noise floor.
- *Structural power content analysis*: it is a low complexity predespreading spoofing detection approach that takes advantage of the cyclo-stationarity* of GNSS signals in order to detect excessive amount of structured signal power in the received sample set.

Postdespreading detection

After the despreading process in the receiver, the used spoofing detection techniques rely on the signal strength and its quality to identify the threat. A couple of examples of this detection method are

- *Effective C/N_0 analysis*: since the C/N_0 monitoring is available in most commercial receivers, this technique is a common signal strength monitoring metric. The cross-correlation term caused by high power spoofing signals can become the dominant term, so an abnormally high C/No value can be an indication of a spoofing attack.
- *Signal quality monitoring, (SQM)* the interaction between authentic and spoofing signals causes distortion on the shape of the correlation function. SQM becomes an excellent spoofing detection tool in the matched power spoofing scenario where all PRNs are affected by spoofing.

*Signals that have statistical properties that vary cyclically with time.

Anti-spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
Baseband variance analysis	Higher power	Low	Medium	AGC monitoring	Medium
Structural power content analysis	Higher power	Low	Medium	Specific pre-despreading processing unit	High
Effective C/N_0 analysis	Higher C/N_0	Low	Medium	C/N_0 monitoring	Medium
Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low

Table 3.4: Summary of spoofing detection techniques. [33]

4

GNSS threat analysis

In this chapter there is the description of the studies, the work and the testing that were done during the internship carried out between August 2019 and February 2020.

4.1 Testbed for Attacks and Mitigations

In August 2019 I've started an internship to work on the *Testbed for Attacks and Mitigations (TAM)* project, of which the Department of Information Engineering (DEI) is a subcontractor.

The goal of this project is to develop a tool to store, search and distribute services for vulnerability, and threat and mitigation identification for GNSS. The TAM will include both technology and application specific threats, as well as real time location-based threats observed in the territory for context awareness and emergency warning.

TAM is composed of the following key elements:

- *IT infrastructure*: a central physical infrastructure storing in a database all the vulnerabilities and mitigations. It comprises all the information technology security needed for the protection of information.
- *Laboratories and control room and equipment*: a number of laboratories and a control room, connected to the infrastructure, which populate vulnerabilities and solutions.

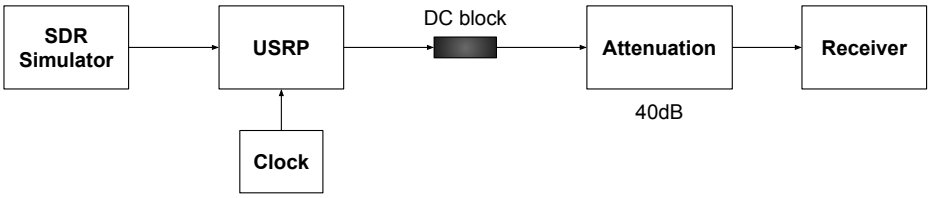


Figure 4.1: Equipment setup for the tests performed during the internship.

In addition, the TAM application will be used together with a specific GNSS simulator to independently test the navigation/threat scenarios. For this reason, the ability to simulate every possible threat to GNSS will be needed from this SDR simulator. So, besides the tests needed to populate the database, also a software to emulate a data level spoofing attack, and that had to be used together with this program, was proved necessary.

4.1.1 Equipment setup for the tests

To perform the various tests needed to fill the TAM database, we had to prepare the equipment as can be seen in Fig. 4.1.

SDR Simulator The SDR simulator used for the tests is a real time GNSS multi-constellation simulator, with advanced capabilities in terms of interference simulation. It is fully configurable for flexible generation of GNSS signals, interferences and authentication schemes up to RF level. It runs in a laptop and, being fully software, enables a fast assessment of existing and new emerging scenarios. It was used to create the navigation and threat scenarios to be imported in the TAM database.

USRP Along with the simulator, the USRP was used to convert signals, to be sent to the receiver, from digital to analog.

Clock The presence of an external reference oscillator improves the RF signal quality if the internal clock is not stable enough.

DC block The DC blocks are passive coaxial components that prevent (block) the flow of direct current (DC) frequencies to RF signals.

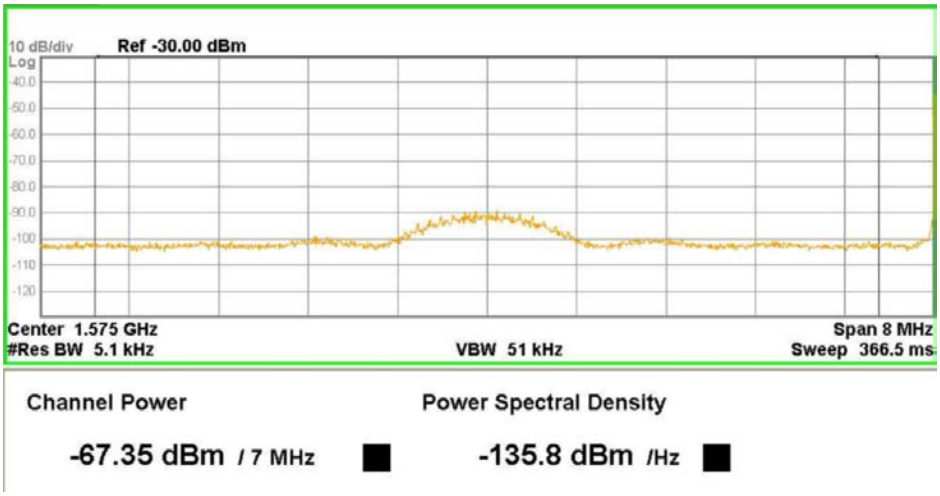


Figure 4.2: Power computed by the signal analyzer for a GPS signal from one satellite generated by the USRP.

Attenuation This component was needed to avoid receiver failure. To verify the attenuation needed by the commercial receiver, we used a signal analyzer to compute the USRP output power (see Fig. 4.2). So, given that the used commercial receiver expected a gain of $20dB$ from the antenna, and since $-67.35dBm$ are equal to $-97.35dBW$, the attenuation a needed was

$$a_{(dBW)} = -97.35 - (-158.5) - 20 \simeq 40dBW,$$

where is $-158.5dBW$ is the power of a GPS signal that reaches the Earth surface.

Receiver A commercial high precision multi-band GNSS receiver, that provides tracking and measurements of all available GNSS signals (GPS, Galileo, GLONASS and BeiDou), has been provided to carry out the tests.

4.1.2 Data level spoofing software

Given the lack of support for data level spoofing attacks in the SDR simulator, we had to develop a software, to be used for the TAM project, to modify a log file of the simulator * to emulate this type of attack. In this thesis, since the data structure for Galileo message is more complex, but also mainly because the logic behind the classes needed to model the navigation

*A csv file which contains all the smaller units of a navigation message, in hexadecimal digits.

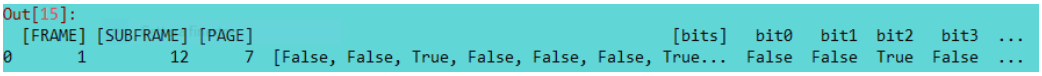


Figure 4.3: Columns added to the imported csv by EditDF class (random values in the fields).

messages[†] is similar, there will be described just the Python classes written for the E1b I/NAV message.

First of all, some Python classes were written to address each component of a frame/sub-frame/page in the Galileo navigation message. At first the csv is imported through the class *Csv2Message* in a *pandas* DataFrame, a tabular data structure with labeled axes where each of the functions to be used on the navigation message could be applied to groups of pages at once quickly and easily. Then the class *EditDF* identifies which sub-frame/frame the pages, that are ordered by TOW, belonged to, by simply using a counter and the modulo operation, knowing that each sub-frame is composed of 15 pages and each frame by 24 sub-frames. As last preliminary steps, some more columns are added to the original DataFrame table:

- `"[bits]"`: contains the conversion from hexadecimal to binary using the Python module *bitarray*.
- `"bit0"` ÷ `"bit239"`: contain each bit of a page from `"[bits]"` column by numbering them from 0 to 239.

In Fig. 4.3 we can see the added columns by class *EditDF* to the original DataFrame, obtained from the imported csv file, on a page composed of 60 hexadecimal random digits.

After this initial stage, there are several classes that deal with the modification of the different elements of a navigation message, and each one of them employs the *BaseEdit* class. When a modification function is called, each class has its own way to obtain the needed parameters and then it calls a method of the *BaseEdit* class based on the type of edit wanted by the user.

As regards the specific modification classes, after realizing that almanacs are elements that are repeated every frame, ephemeris and clock corrections every sub-frame, and so forth, the classes below were created with the following composition: a DataFrame containing the name of the parameters that could be changed and the coordinates of those parameters inside of specific frames/sub-frames/pages, some *getter* methods to print a specific parameter or a specific element (*e.g.* an entire almanac), and the different methods to edit the single parameters.

[†]The message composition was found in [34] for the GPS SPS, and in [20] for the Galileo I/NAV.

- *Almanac*: used to modify the Almanac of one, or more, satellite.
- *ArbitraryEdit*: used to edit arbitrary parts of a page (without considering the specific elements of each page).
- *Corrections*: used to manage time/ionospheric corrections and conversion parameters.
- *Ephemeris*: modifies the parameters of ephemeris.
- *GstGpsConversion*: for GST-GPS conversion parameters.
- *OtherParams*: for parameters that aren't part of bigger *entities* and that are updated in each subframe.
- *OtherParamsInTwos*: for parameters that aren't part of bigger *entities* and that are updated every two subframes.
- *PageUpdate*: is called every time the CRC has to be changed and is used to modify the parameters of a single page.

Finally, a common element in each created class is the need for a method to update the CRC field in the modified pages. So, the `change_crc` function was added at the end of each edit method to allow the user to choose to update the CRC as it should be with the new values, with one of the 3 *BaseEdit* methods, or by leaving unaffected that field.

Since each class of this software was designed almost with the same structure, except clearly for the fact that different elements are updated with different rates, here below there is the description of just the *Almanac* class as an example of all the classes that were written for this task.

Almanac class

As regards Galileo I/NAV message, the almanacs are located into words 7, 8, 9 and 10, so, for each subframe, they are located in the 4^{th} and in the 5^{th} pages. To receive the almanacs of every satellite, an entire frame is needed, so every 2 subframes we have the transmission of 3 different almanacs. [20]

To describe this fact, a dictionary `SV_ALMANACS` was created by linking the parameter name with its position in the navigation message. Then, to ensure ease of use, `SV_ALMANACS` values were passed to a DataFrame.

The first two methods of this class are two *getters*: one to get a single almanac parameter, and the other for the entire almanac of a specific Space Vehicle (SV) in a specific frame. Thanks to the DataFrame, only a couple of filters are needed to implement both *get*s.

The next step was to create a method, `edit_support`, to obtain a tuple of coordinates to be used with edit methods. This function takes as input the common parameters of the three edit methods, and returns a list containing the tuples with the coordinates for the edit. This specific part of code is used for three similar functions that, for the sake of clarity, has the same name of the three *BaseEdit* methods. All of them are written equally, except for the *BaseEdit* method used by each one of them, so we have the computation of the coordinates of the pages to edit followed by the editing, and, before the last row, the CRC update.

No editing method that was written has a return statement. This is due to the fact that when a DataFrame is referenced, even if just a fragment of it, it is the same object we are modifying and not a copy of it.

4.2 Threat modeling

In this section we describe how a threat is parameterized for insertion into the TAM database. In particular, in order to describe jamming and spoofing signals, we created a model that takes into consideration both the parameters needed by the SDR simulator software, and also the parameters needed to model an attack as generic as possible. In the case of multiple jamming, multiple spoofing, or jamming and spoofing together in the same scenario, each single attack is modeled and then they are linked together in the simulation scenario.

Unlike the specific parameters that describe the configuration of an attack, those that describe the navigation scenario are the same for all attacks (see Table 4.1).

Simulation start time and duration Time and date (which are then converted respectively in TOW and WN) of the simulation and how long it lasts.

Visible GNSS Which GNSS was/were used during the simulation.

Satellites used Which satellites were used for each GNSS which was selected.

Receiver Information about the model of the receiver, and the different receiver configuration settings used for the test.

Motion type If the vehicle where the receiver is installed is stationary or, otherwise, which type of motion it should expect (*e.g.* terrestrial or airborne).

Parameter	Value
Time and date	`February 04, 2020, 12:00:00`
Duration	`00:03:00`
Visible GNSS	`GPS`
Satellites used	`1 ÷ 32`
Receiver model	`receiver_a`
PVT mode	`kalman`
Multipath mitigation	`none`
Motion type	`static`

Table 4.1: Example of the key-value pairs needed to model a navigation scenario.

4.2.1 Jamming modeling

With regards to the jamming threat, the parameters described in the following paragraphs were considered to effectively represent it (see Table 4.2).

Time of activation/deactivation Relative to the start of the test and indicates after how many seconds the jammer starts/stops.

Jamming power The power of the jamming signal when the jammer is activated.

Jamming type The type of signal transmitted by the employed jammer (*e.g.* continuous wave, Gaussian noise or chirp).

Jamming signal bandwidth The bandwidth of the jamming signal. If needed, it can be also modeled a jamming attack that sweeps a certain frequency span with a given rate.

Impact description A brief explanation of the results from the test.

Parameter	Value
Time of activation [s]	`90`
Jamming power [dBW]	`-122`
Jamming type	`chirp (sawtooth)`
Impact description	`Small` C/N_0 `loss`

Table 4.2: Example of the key-value pairs needed to model a jamming attack.

4.2.2 Spoofing modeling

As regards the spoofing threat instead, the parameters needed to represent this type of attack to the GNSS receivers were:

Time of activation/deactivation Relative to the start of the test and indicates after how many seconds the spoofer starts/stops.

Gain offset The spoofing signal gain offset relative to the legit signal power.

Spoofing type The type of the implemented spoofing attack (*e.g.* fixed position or trajectory spoofing).

Spoofed coordinates Single position, for the fixed position attack, or, otherwise, a set of coordinates.

Impact description A brief explanation of the results from the test.

In Table 4.3 you can see an example of key-value pairs for the parameters needed to model the spoofing attack.

Parameter	Value
Time of activation [s]	`80`
Gain offset [dB]	`20`
Spoofing type	`fixed position`
Spoofed coordinates	`latitude and longitude values`
Impact description	`Gradual shift towards the spoofed position`

Table 4.3: Example of the key-value pairs needed to model a spoofing attack.

4.3 Tests and results

During the internship period, several tests were performed with the equipment setup described in 4.1.1 to verify the reactions of the commercial receiver Open Service to different types of threats. In the following sections there will be a list of parameters used for the tests and a description of the outcomes for each of them.

4.3.1 Jamming tests

The goal for these tests was to verify, for each combination of GNSS used (GPS, Galileo or GPS and Galileo):

- if some specific type of jamming was more dangerous than others for the receiver;
- the power interval $[\min, \max]$ associated to a loss of accuracy of the attacked GNSS signal. Below this interval no effect occurs, while, above this interval, the receiver loses the track (*i.e.* the attack lead to a denial of service).

For the jamming tests, we set a test duration of 3 minutes and the attack is activated after 80 seconds. We have tried different jamming power, starting from the same power as the GNSS signal and up to -105dBW, increasing from time to time by 20dBW, or until we experienced a loss of accuracy. As jamming type, we tested

Continuous Wave Jamming The attack did not result in any problem for the receiver, except for the maximum jamming power case where there was just a C/N_0 loss (see Table 4.4). We have assumed that these results were caused by some kind of implementation of a Notch filter to mitigate this type of threat. In Table 4.5 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A		Galileo E1-B	
	min	max	min	max
Jamming power needed to have loss of accuracy [dBW]	-	-	-	-

Table 4.4: Results from the CW jamming attacks.

Parameter	Value
Time and date	`February 04, 2020, 12:00:00`
Duration	`00:03:00`
Visible GNSS	`GPS`
Satellites used	`1 ÷ 32`
Model	`receiver_a`
PVT mode	`auto`
Multipath mitigation	`none`
Motion type	`static`
Time of activation [s]	`80`
Jamming power [dBW]	`-105`
Jamming type	`continuous wave`
Impact description	C/N_0 `loss on jamming activation`

Table 4.5: Example of the key-value pairs needed to model a CW jamming attack.

Broad Band AWGN Jamming In this case we found out that at maximum jamming power we have a denial of service, regardless of the GNSS. By decreasing the power (-111dBW for the GPS or -112dBW for the Galileo) we could keep tracking but with a loss of accuracy, a substantial C/N_0 loss and a discontinuity in availability (see Table 4.6). In Table 4.7 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A		Galileo E1-B	
	min	max	min	max
Jamming power needed to have loss of accuracy [dBW]	-117	-111	-118	-112

Table 4.6: Results from the broad band AWGN jamming attacks.

Parameter	Value
Time and date	`February 04, 2020, 12:00:00`
Duration	`00:03:00`
Visible GNSS	`Galileo`
Satellites used	`1 ÷ 36`
Model	`receiver_a`
PVT mode	`auto`
Multipath mitigation	`none`
Motion type	`static`
Time of activation [s]	`80`
Jamming power [dBW]	`-112`
Jamming type	`AWGN`
Impact description	`Availability discontinuity, loss of accuracy and substantial` C/N_0 `loss`

Table 4.7: Example of the key-value pairs needed to model a broad band AWGN jamming attack.

Narrow Band AWGN Jamming This attack was more successful than the broad band one, since a smaller power was needed to cause a loss of accuracy and a denial of service. With -122dBW of jamming power against a GPS signal we have a loss of accuracy, while, under -119dBW, we had a definitive loss of lock with Galileo (see Table 4.8). Since there is a fast shift between tracking the GNSS signals and having a denial of service, there was no substantial C/N_0 loss in these tests. As regards the parameterization, you can see the broad band AWGN case since it is the same attack with a different jamming signal bandwidth.

Given that from the results of the CW jamming tests we hypothesized that the receiver implements a Notch filter, we've also tested the AWGN jamming with increasingly narrow band to see what is its upper bound. In the end we found out that the maximum bandwidth where the noise is canceled is 500Hz.

	GPS L1 C/A		Galileo E1-B
	min	max	
Jamming power needed to have loss of accuracy [dBW]	-122	-111	Straight transition from tracking to DoS

Table 4.8: Results from the narrow band AWGN jamming attacks.

Chirp (Sawtooth) Jamming As before, a smaller jamming power was needed to lose tracking of Galileo signals (under -114dBW), while GPS still tracked, even if with a loss of accuracy, with a jamming power of -110dBW (see Table 4.9). Under these values there was a denial of service. In Table 4.10 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A		Galileo E1-B	
	min	max	min	max
Jamming power needed to have loss of accuracy [dBW]	-121	-110	-117	-115

Table 4.9: Results from the chirp jamming attacks.

Parameter	Value
Time and date	`February 04, 2020, 12:00:00`
Duration	`00:03:00`
Visible GNSS	`GPS`
Satellites used	`1 ÷ 32`
Model	`receiver_a`
PVT mode	`auto`
Multipath mitigation	`none`
Motion type	`static`
Time of activation [s]	`80`
Jamming power [dBW]	`-122`
Jamming type	`chirp (sawtooth)`
Impact description	`Small` C/N_0 `loss`

Table 4.10: Example of the key-value pairs needed to model a chirp jamming attack.

Frequency Hopping Jamming As last jamming attack, we also tested frequency hopping[‡]. As for the CW jamming, for GPS we did not have denial of service, no matter the jamming power. Anyway, we still had loss of accuracy on GNSS measurements up to -116dBW. With regard to Galileo instead, we had loss of accuracy below -116dBW and loss of lock under -111dBW (see Table 4.11). Above these values there was a denial of service. In Table 4.12 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A		Galileo E1-B	
	min	max	min	max
Jamming power needed to have loss of accuracy [dBW]	-116	-105	-116	-112

Table 4.11: Results from the frequency hopping jamming attacks.

Parameter	Value
Time and date	`February 04, 2020, 12:00:00`
Duration	`00:03:00`
Visible GNSS	`GPS`
Satellites used	`1 ÷ 32`
Model	`receiver_a`
PVT mode	`auto`
Multipath mitigation	`none`
Motion type	`static`
Time of activation [s]	`80`
Jamming power [dBW]	`-118.5`
Jamming type	`frequency hopping`
Impact description	`No effect`

Table 4.12: Example of the key-value pairs needed to model a frequency hopping jamming attack.

4.3.2 Spoofing tests

Concerning these tests, they were made to see what would happen if we activate a fixed spoofing attack without trying to cause a loss of lock with the legit GNSS signal. We tried with

[‡]Method of transmitting radio signals by rapidly changing the carrier frequency among many distinct frequencies occupying a large spectral band.

a gain offset of the spoofing signal, compared to the GNSS signal, from 0dB to 40dB in 3 different scenarios: a spoofed position at about 100m from the real position, then 1km and, in the last one, 100km. As for the jamming tests, we set a test duration of 3 minutes and the spoofing attack is activated after 80 seconds.

Fixed spoofed position at about 100m No matter the power difference with the spoofing signal, there was no problem with the reception of the legit GPS signal. As regards Galileo instead, even a 3dB gain offset was enough to gradually shift the position of the receiver toward the spoofed position (see Table 4.13). In Table 4.14 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	-	3dB

Table 4.13: Results from the fixed spoofing at about 100m attacks.

Parameter	Value
Time and date	February 04, 2020, 12:00:00
Duration	00:03:00
Visible GNSS	GPS
Satellites used	1 ÷ 32
Model	receiver_a
PVT mode	auto
Multipath mitigation	none
Motion type	static
Time of activation [s]	80
Gain offset [dB]	20
Spoofing type	fixed position
Spoofed coordinates	position at about 100m from the receiver
Impact description	No effect

Table 4.14: Example of the key-value pairs needed to model a fixed spoofing at about 100m attack.

Fixed spoofed position at about 1km In this test, the spoofed position is configured 1km away from the actual receiver position. Concerning the other parameters, the same con-

figuration considered for the previous test is exploited (see Table 4.14).

By increasing the spoofed distance we observed a loss in the C/N_0 values for the GPS signals from a 10dB gain offset. A 30dB gain offset was needed to effectively spoof the receiver position. As regard the Galileo signal, the increased distance resulted in an higher gain offset needed to spoof the legit position (see Table 4.15).

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	30dB	10dB

Table 4.15: Results from the fixed spoofing at about 1km attacks.

Fixed spoofed position at about 100km In this test, the spoofed position is configured 100km away from the actual receiver position. Concerning the other parameters, the same configuration considered for the 100m case is exploited (see Table 4.14).

In this case we had the same results of the 1km case for the GPS system, while, for Galileo, there was again an increment to 30dB of the gain offset needed to spoof the legit position (see Table 4.16). Probably this was caused by the fact that the receiver did not believe that it moved so far. In the end, anyway, the gain offset was so overwhelming to cause a loss of lock of the Galileo signal and to start the tracking on the spoofing signal.

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	30dB	30dB

Table 4.16: Results from the fixed spoofing at about 100km attacks.

4.3.3 Jam and Spoof tests

After the previous tests, we thought we would try a smarter attack, the jam and spoof (see 3.2.1). The attack was composed by:

- *chirp (sawtooth) jamming*: we verified with previous tests that this attack could provoke a denial of service for both GPS and Galileo with a power of -105dBW;
- *spoofing*: we tried the same fixed position spoofing attacks that we tested before.

In particular, we increased the simulation time to 4 minutes and we organized that time like this

Time	Description
00:00	Simulation start with GNSS signal transmission
01:30	Jamming attack
02:30	Spoofing attack
02:50	Jamming stop
04:00	Simulation stop

Table 4.17: Jam and spoof tests time organization.

From these tests we verified that if the spoofing attack succeeded with a specific gain offset, then it would succeed also with higher gain offsets for sure.

Jam and spoof at about 100m As we expected, after 90 seconds, there was a denial of service caused by the chirp jamming. After additional 60 seconds then, also the spoofer was activated and, starting from a 0dB gain offset for the GPS, and from 3dB for Galileo, the receiver started the tracking on the forged position (see Table 4.18). In Table 4.21 you can see an example of parameterization of this attack for a TAM database entry.

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	0dB	3dB

Table 4.18: Results from the jam and spoof at about 100m attacks.

Jam and spoof at about 1km In this test, the spoofed position is configured 1km away from the actual receiver position. Concerning the other parameters, the same configuration considered for the 100m case is exploited (see Table 4.21).

We obtained that both GPS and Galileo just needed 3dB as spoofing signal gain offset from the GNSS signal to start tracking on the spoofed position (see Table 4.20).

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	3dB	3dB

Table 4.19: Results from the jam and spoof at about 1km attacks.

Jam and spoof at about 100km This case needed an higher gain offset of the spoofing signal power, compared to the legit one, to succeed. To spoof the real position for the GPS, a

10dB gain offset was enough. As regards the Galileo system, an higher gain offset was needed, so we verified that with 30dB we could deceive the receiver (see Table 4.20). You can see the parameterization for this attack in the 100m case (see Table 4.20).

	GPS L1 C/A	Galileo E1-B
Minimum gain offset needed for successful spoofing	10dB	30dB

Table 4.20: Results from the jam and spoof at about 100km attacks.

Parameter	Value
Time and date	February 04, 2020, 12:00:00
Duration	00:04:00
Visible GNSS	GPS
Satellites used	1 ÷ 32
Model	receiver_a
PVT mode	auto
Multipath mitigation	none
Motion type	static
Jamming time of activation [s]	90
Jamming time of deactivation [s]	170
Jamming power [dBW]	-105
Jamming type	chirp (sawtooth)
Spoofing time of activation [s]	150
Gain offset [dB]	10
Spoofing type	fixed position
Spoofed coordinates	position at about 100m from the receiver
Impact description	Spoofed position after the loss of lock caused by the jamming attack

Table 4.21: Example of the key-value pairs needed to model a jam and spoof at about 100m attack.

4.3.4 Jam and Spoof tests (shorter Jamming duration)

Since it is possible that a receiver may react differently, in a jam and spoof scenario, based on the jamming attack duration, we deemed it appropriate to repeat the previous tests using a different time of deactivation of the jammer.

What we expected was that the receiver could possibly understand that it was not possible for it to reach a certain distance in a shorter time. So, by decreasing the jamming attack duration, we should observe that a larger spoofing signal power gain offset is needed in order to obtain a successful attack.

What we observed, from the tests we performed, confirmed our assumption. In particular, we can see from Table 4.22 that, while on smaller distances (100m or 1km) the gain offset needed was of 0dB or 3dB, on larger distances (100km) we need a much larger gain offset to obtain the same results. This result may be caused by the fact that the receiver may not believe that such distance may be covered in such a short time.

Jamming duration in the jam and spoof attacks

	60s		30s		10s	
	GPS	Gal	GPS	Gal	GPS	Gal
100m	0dB	3dB	3dB	3dB	3dB	3dB
1km	3dB	3dB	3dB	3dB	3dB	3dB
100km	10dB	30dB	20dB	40dB	20dB	40dB

Table 4.22: Results for the jam and spoof tests, on GPS L1 C/A and Galileo E1-B, with different jamming duration.

5 Conclusion

In this thesis we showed the work that we did during the internship, in the context of the TAM project. To better explain the topics we have dealt with during the internship, we also presented a description of Global Navigation Satellite Systems, with a more focused look at their signals and the threats that may harm them.

During the time spent at the company, we developed a software to simulate a data-level spoofing attack. This software is able to address different civilian GNSS signals, specifically the GPS SPS and the Galileo I/NAV. It can address every single parameter of a navigation message and change it as required by the user. After the editing, it can then save the new navigation message in a format convenient for spoofing simulations with the SDR simulator software.

After that, some tests were performed to fill the TAM database with realistic threat scenarios. A parameterization of the navigation and threat scenarios was needed and we have described the main parameters used to model specific attacks to the GNSS. Other parameters, different from the ones in this work, are now present in the TAM database that are needed to characterize a generic threat to the GNSS that may arise in the future. Anyway, they were not shown because they were not required to effectively describe the tests that were performed.

From the tests results, we showed that the used commercial receiver was strong against continuous wave jamming attacks, possibly for the presence of a Notch filter capable of filtering an interfering signal with a bandwidth up to 500Hz. As regards other tested jamming

attacks, it turned out that narrow band jamming signals were more effective in disrupting the tracking of the GNSS signals.

For spoofing attacks instead, the used receiver began to have problems even when we transmitted the spoofing signal without a prior jamming phase. As expected then, since we already had seen that the receiver was weak against this type of attacks, a smarter spoofing attack (*jam and spoof*) gave us the spoofed position as soon as the spoofer was activated.

For what concerns future work, it may be interesting to test the developed software to change the navigation message fields with realistic scenarios and verify its impact on a receiver. Besides that, clearly, more tests will have to be performed, with other types of attacks and with different receivers, in order to make the database as exhaustive as possible. Moreover, it may be interesting to find out which is the maximum distance, between the real and the forged position, where the receiver may be deceived by our attacks, no matter the jamming attack duration, using a small gain offset (0dB or 3dB).

A

Error sources

GNSS MEASUREMENTS are affected by different types of errors that may be generated by various sources: satellites, receivers and even from the signal propagation. [35]

A.1 Errors from satellites

EPHEMERIS ERRORS The control segment predicts the position of satellites as a function of time. Anyway, given that satellites can be affected by the asymmetry of the Earth's gravitational field, or the attractive force of celestial bodies, just to name a couple, these variations may lead to differences of the position of the satellites with respect to the projected orbit. This results in an information that is transmitted to the ground segment, that can generate an error in the measurement of the satellite-receiver distance. Thanks to subsequent readings done by the control segment, these errors can be reduced by using precise ephemeris.

SATELLITE CLOCKS ERRORS To provide frequency and time control requirements for GNSS signals, atomic clocks are employed. Since these clock are not perfect, even if they are highly precise, they produce errors in the order of meters, that, if we consider that a receiver's clock is much less accurate, turns into an error in the order of hundreds of meters. By acquiring the navigation signal from, at least, 4 satellites, the receiver may greatly reduce this error.

A.2 Errors from receivers

Multipath errors Multipath is the main source of errors for phase and pseudorange measurements, and it is due by receiving a signal reflected by, for example, a building. Since the reflection causes a slight delay with respect to a signal that is received directly, the receiver will compute an incorrect position. This error may be greatly reduced by placing the receiver antenna far from the reflective source. Anyway, current technology is able to provide a stronger defense against this problem.

Receiver noise errors Receiver noise refers to the position error caused by the GNSS receiver hardware and software. High-end GNSS receivers tend to have less receiver noise than lower cost GNSS receivers.

A.3 Errors from signal propagation

Ionospheric delay The ionosphere contains electrically charged particles called ions that delay the satellite signals and can cause a significant amount of satellite position error. Ionospheric delay also varies based on the radio frequency of the signal passing through the ionosphere, so GNSS receivers that can receive more than one GNSS signal (*e.g.* L1 and L2) can use this to their advantage. By comparing the measurements for L1 to the measurements for L2, the receiver can determine the amount of ionospheric delay and remove this error from the calculated position.

Tropospheric delay Variations in tropospheric delay are caused by the changing humidity, temperature and atmospheric pressure in the troposphere. Since tropospheric conditions are very similar within a local area, the base station and rover receivers experience very similar tropospheric delay. This allows Differential GNSS and RTK systems* to compensate for tropospheric delay.

*Differential GNSS is a kind of GNSS Augmentation system, while Real-Time Kinematic systems use a single base-station receiver and a number of mobile units to enhance the precision of the position data derived from GNSS.

References

[1] *GSA GNSS Market Report*, 2nd ed., European Global Navigation Satellite System Agency, 2019.

[2] "Space Race," https://en.wikipedia.org/wiki/Space_Race, accessed: 2019-11-22.

[3] K. Borre, D. Akos, N. Bertelsen, P. Rinder, and S. Jensen, *A Software-Defined GPS and Galileo Receiver*, 1st ed., ser. Applied and Numerical Harmonic Analysis. Birkhäuser Basel, 2017.

[4] J. Subirana, M. Hernandez-Pajares, and J. Zornoza, *GNSS Data Processing, Vol. I: Fundamentals and Algorithms*, ser. ESA TM. ESA Communications, 2013.

[5] H. Kuusniemi, "User-Level Reliability and Quality Monitoring in Satellite-Based Personal Navigation," Ph.D. dissertation, Tampere University of Technology, 06 2005.

[6] P. Teunissen and O. Montenbruck, *Springer Handbook of Global Navigation Satellite Systems*, 1st ed., ser. Springer Handbooks. Springer International Publishing, 2017.

[7] "GSA Galileo," https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system, accessed: 2019-11-22.

[8] "Galileo Space Segment," https://gssc.esa.int/navipedia/index.php/Galileo_Space_Segment, accessed: 2019-11-22.

[9] "GPS Constellation status," https://www.navcen.uscg.gov/?Do=constellationStatus, accessed: 2019-11-22.

[10] E. Berger, "The last single-stick Delta rocket launched Thursday, and it put on a show," *Ars Technica*, 08 2019.

[11] "GPS Accuracy," https://www.gps.gov/systems/gps/performance/accuracy/, accessed: 2019-11-22.

[12] S. Moore, "Superaccurate GPS Chips Coming to Smartphones in 2018," *IEEE Spectrum*, 09 2017.

[13] I. Srivastava, "How Kargil spurred India to design own GPS," *The Times of India*, 04 2014.

[14] "Galileo Constellation status," https://www.gsc-europa.eu/system-service-status/constellation-information, accessed: 2019-11-22.

[15] "BeiDou Constellation status," http://www.csno-tarc.cn/system/constellation&ce=english, accessed: 2019-11-22.

[16] G. Hein, "GNSS Interoperability: Achieving a Global System of Systems or "Does Everything have to be the same?"," *InsideGNSS*, pp. 57–60, 02 2006.

[17] "Agreement on the Promotion, Provision and use of Galileo and GPS Satellite-based Navigation Systems and related Applications," 06 2004.

[18] "GPS International Cooperation," https://www.gps.gov/policy/cooperation/, accessed: 2019-11-22.

[19] A. De Martino, *Introduction to Modern EW Systems*, 2nd ed. Artech House, 2018.

[20] *European GNSS (Galileo) Open Service Signal-in-Space Interface Control Document*, 1st ed., European Union, 12 2016.

[21] "An Introduction to GNSS," https://www.novatel.com/an-introduction-to-gnss/chapter-1-gnss-overview/section-1/, accessed: 2019-11-22.

[22] "GPS satellite trilateration," https://giscommons.org/chapter-2-input/, accessed: 2019-11-22.

[23] "GPS Control Segment," https://www.gps.gov/systems/gps/control/, accessed: 2019-11-22.

[24] L. Boccia, G. Amendola, S. Gao, and C.-C. Chen, "Quantitative evaluation of multipath rejection capabilities of gnss antennas," *GPS Solutions*, vol. 18, 04 2014.

[25] S. Communications, "Spirent - Test Scenario Pack for GNSS Vulnerabilities and Threats," https://www.spirent.com/-/media/datasheets/positioning/test-pack-gnss-vulnerabilities-and-threats.pdf?la=en&hash=6B8125AF0B0E09B3778409CC35743DFED08FF889, 2018.

[26] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1233–1245, June 2016.

[27] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security Privacy*, vol. 14, no. 1, pp. 47–54, Jan 2016.

[28] A. Graham, *Communications, Radar and Electronic Warfare*. Wiley, 2011.

[29] J. T. Curran, M. Bavaro, P. Closas, and M. Navarro, "On the threat of Systematic Jamming of gnss," in *Proc. ION GNSS*, 2016.

[30] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, June 2016.

[31] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174–1194, June 2016.

[32] A. Broumandan, R. Siddakatte, and G. Lachapelle, "An approach to detect gnss spoofing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64–75, Aug 2017.

[33] L. Chiarello, "Security Evaluation of GNSS Signal Quality Monitoring Techniques against Optimal Spoofing Attacks," Master's thesis, Università degli Studi di Padova, 2018.

[34] *Global Positioning System Standard Positioning Service Signal Specification*, 2nd ed., United States Government, 6 1995.

[35] "GNSS error sources," https://www.novatel.com/an-introduction-to-gnss/chapter-4-gnss-error-sources/error-sources/, accessed: 2019-11-22.

Acknowledgments

I would like to thank prof. Nicola Laurenti, my supervisor for both my bachelor and master studies, who got me into information security and inspired me with his vast knowledge about this immense topic.

A special thank you goes to my closest friends Matteo and Martina. We shared the laughter and the tears and I will forever be in your debt.

I am also grateful to all my friends that helped me relieve my stress during these years: the ones with whom I roll dice every week, my colleagues from university, the ones that I have known ever since I was little and the ones that I have met just a few years ago.

My deepest gratitude goes to my parents, Alessandro and Seila, and to my girlfriend, Domiziana. You kept me going on and this work would not have been possible without you.