POLITECNICO DI TORINO

Master's Degree in ICT4SS

Master's Thesis

Experimental Analysis of Intentional Radio-Frequency Attacks on GNSS-based Time Synchronization for Communications Networks

Supervisors

Prof. Fabio DOVIS

Dr. Alex MINETTO

Candidate

Brendan David POLIDORI

December 2021

Abstract

Accurate and reliable time synchronization in telecommunication networks is fundamental to ensure the superior performance of upcoming and next-generation paradigms of mobile communications, such as 5G New Radio (NR).

In a modern network infrastructure, sub-microsecond synchronization requires a large number of reliable clocks such as Rubidium (Rb) and Cesium (Cs) atomic oscillators, technologies that are too expensive to be deployed throughout multiple network nodes.

To overcome the cost problem, atomic clocks are being replaced by less-expensive GNSS receivers that provide a specific synchronization signal, the Pulse Per Second (1-PPS), that can be exploited to distribute time synchronization across the network at more sustainable costs.

However, GNSS receivers expose the network to the growing risk of radio-frequency attacks, thus introducing a significant security flaw.

This thesis research sought to determine the effects of intentional radio frequency interference on GNSS State-of-the-Art timing receivers, with the aim of assessing the reliability of the generated 1-PPS. Jamming, meaconing and spoofing attacks were investigated singly or in combination of two or more as options against the GNSS receivers under test.

Specific test procedures were designed to intentionally disrupt the activities of the receiver and to observe the effect on the 1-PPS generation. Generally, they focused on four periods, the first with no interference applied, the second with mild interference, the third with high levels of interference to cause maximum damage, and the fourth post-interference period during which the return to normal operation was assessed.

High-power jamming signals completely disrupted the normal operation of the receiver, while in the case of low-power jamming levels, the receiver's interference mitigation algorithm was able to effectively detect and compensate for them. Meaconing proved to be the most effective method to introduce a delay in the 1-PPS generation, since the receiver erroneously interprets the delayed signals as caused by the multipath effect. Finally, simplistic spoofing signals are completely blocked by the receiver, and when their power level exceeds a certain threshold the receiver classifies them as interference, and completely stops its operation. Throughout the tests, the target receiver proved to be an excellent time keeping source, able to satisfy stringent synchronization requirements. It also performed with excellent interference mitigation capabilities, but ultimately was defeated by meaconing and its own algorithms.

Summary

Time is the invisible utility, and it is fundamental for critical infrastructures. The time standard used by the world is Coordinated Universal Time (UTC), derived from a composite of different clocks from many laboratories around the globe. Global Navigation Satellite Systems (GNSS) are all related to the UTC time scale. Therefore GNSS constellations are seen as a freely available synchronized clock. The work of this thesis has been to explore the reliability against radio frequency interference of multi-frequency, multi-constellation, Open Service Navigation Message Authentication (OSNMA) capable GNSS receivers, built with anti-jamming and anti spoofing interference mitigation capabilities. Today's telecom networks are synchronized through the use of atomic clocks which are highly expensive. The introduction of GNSS receivers as elements to aid in time synchronization of telecom networks, affords the benefits of high accuracy timing, it also opens the system to vulnerabilities, including Radio Frequency Interference (RFI). A GNSS receiver works by calculating four variables, three being the position and one being the difference in time between the constellation system time and the receiver time, known as the receiver clock bias. The local clock is not synchronized to the system time by design. The receiver finds these values by calculating its distance from each of the satellites used, since the position of the satellites is known. GNSS satellites transmit a signal that is generated by using a carrier frequency, a pseudo random noise (PRN) code and a data stream carrying data needed for the position, velocity and time (PVT) estimation, namely satellites ephemeris and Time-of-Week (TOW). Once the receiver calculates its PVT, it starts outputting the signal of interest for this research: the 1-Pulse Per second (1-PPS). This is an electrical signal characterized by low jitter and long term stability. The exact methods through which this signal is generated are well kept secrets, but some architectures make use of the receiver PRN generators, by design set to an all ones state every ms, along with a pulse generator, a phase comparator and a microcontroller that disciplines the local oscillator (LO). Clock steering is used to guide the LO in order to compensate for the receiver clock bias. If the LO and steering process are disturbed by RFI attacks, then also the 1-PPS will suffer the consequences.

Intentional radio frequency interference can be classified into three main categories:

- Jamming is the simplest and most common, given the availability of jammers. These types of attacks are meant to completely stop any receiver from operating correctly by introducing noise in the GNSS frequency bands.
- Meaconing, more complex than jamming, is an insidious attack and it consists in the re-transmission of the legitimate GNSS signals with an added delay and with higher power. This fools the receiver to lock on to these delayed signals and consequently steer its LO to be synchronized with them.
- In spoofing, counterfeit GNSS signals are transmitted in order to fool the receiver into calculating an incorrect PVT. These are the hardest attacks to protect from because the signals transmitted have exactly the same appearance as the legitimate ones.

For this thesis, an experimental testbed and different test procedures were designed to analyze the vulnerabilities of the receiver. We can see the testbed in Figure 1, where the timing receivers are numbered 3 and 4. At point 7, we see the input point to the system for the RFI signals, together with the variable attenuator used to control the power of these signals with precision. Both receivers obtain an external frequency reference through a rubidium atomic clock, indicated as 1 in Figure 1. The test procedures are designed with the 1-PPS in mind. The main objective was to see how the signal reacts under different levels of interference. Jamming was performed using a desktop jammer, with 100 mW of power at the output for each frequency band. The jamming signal was attenuated by a fixed 30 dB attenuator and then was modulated using the variable attenuator during the test procedure to subject the receiver to different levels of interference power. Meaconing was introduced by branching the legitimate GNSS signals, from point 2 in 1, and passing them through a 25 dB amplifier and then an RF cable that delayed them by a fixed amount. If the attack is successful, this delay should be reflected in the 1-PPS. Simplistic spoofing attacks were created using the combination of a software defined radio (SDR) and GnuRadio, a graphical user interface that allows to control the SDR. The spoofing attacks were record and replay, meaning the SDR was first used to record the legitimate GNSS signals, and then used to reproduce them at a later time. The different attack procedures resulted in different receiver behaviours:

- Jamming at low and intermediate intensities was detected and mitigated by the receiver which allowed for continued output of the 1-PPS signal without any notable disturbances. Instead, high intensity multi frequency jamming resulted in the complete loss of acquisition and tracking of the receiver, which stopped

the 1-PPS generation after the pre-defined time set during configuration. If such an attack would take place it could force the network node to rely on backup synchronization protocols.

- Meaconing was highly effective because it was interpreted by the receiver as multipath and not as an interference source. Multipath in normal conditions is a natural source of RFI that derives from signals being reflected and then reaching the receiver, delaying the travel time. When the meaconing signals were introduced to the system, with a power of 2 dB/Hz more than the legitimate GNSS signals, the receiver locked on to them and a shift in the generation of the 1-PPS of 200 ± 30 ns could be seen using an oscilloscope. This amount of delay violated the requirements set by the reference project. This threat poses serious risks to the synchronization of the network because it affects the system undetected.

- Spoofing, on the other hand, was not successful, which can be attributed to the anti-spoofing capabilities of the receiver, as it was immediately detected either as interference or as actual spoofing signals. Such a highly skilled attack is mostly not likely given the easier possibility of meaconing and the success of it.

In conclusion GNSS receivers, even if equipped with anti jamming and anti spoofing mitigation systems, are vulnerable to radio frequency attacks. If used as tools to aid with network synchronization more needs to be done to protect these assets.

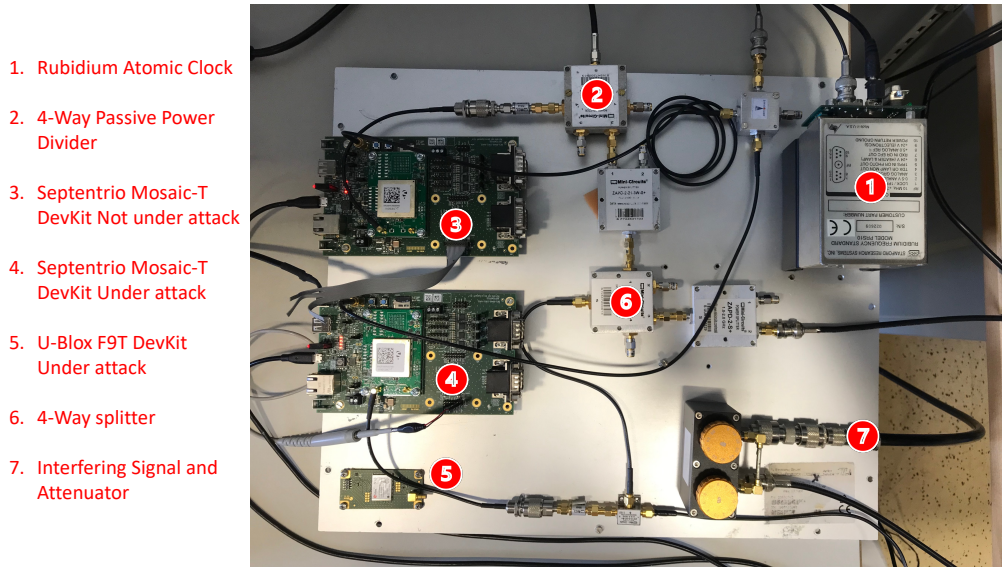


Figure 1: Lab implementation for the experiments

Acknowledgements

"To my parents, friends, professors and those close"
Brendan

Table of Contents

List of Tables

List of Figures

Acronyms

GNSS
Global Navigation Satellite System

MIMO
Multiple Input Multiple Output

FDD
Frequency Division Duplex

TDD
Time Division Duplex

OSNMA
Open Service Navigation Message Authentication

MPLS
Multi Protocol Label Switching

C-GMC
Centralized Grandmaster Clock

D-GMC
Distributed Grandmaster Clock

WRN
White Rabbit Network

WRS
White Rabbit System

ePTRC

Enhanced Primary Time Reference Clocks

OCXO

Oven Controlled Crystal Oscillator

PNT

Positioning, Navigation and Timing

GPS

Global Positioning System

BPSK

Binary Phase-Shift Keying

DSSS

Direct Sequence Spread Spectrum

PRN

Pseudo Random Noise

CDMA

Code Division Multiple Access

MEO

Medium Earth orbit

TDOP

Time Dilution of Precision

UNSO

United States Naval Observatory

UTC

Coordinated Universal Time

BIPM

Bureau International des Poids et Mesures

1-PPS
: Pulse Per Second

FLL
: Frequency Lock Loop

PLL
: Phase Lock Loop

RFI
: Radio Frequency Interference

ITU
: International Telecommunication Union

RR
: Radio Regulations

DGPS
: Differential GPS

CAF
: Cross Ambiguity Function

BPF
: Band Pass Filter

AGC
: Automatic Gain Control

BER
: Bit Error Rate

ADC
: Analog to Digital Converter

C/N_0
: Carrier to Noise Ratio

FDAF

Frequency domain Adaptive Filtering

FFT

Fast Fourier Transform

CWI

Continuous Wave Interference

IIR

Infinite Impulse Response

SMA

SubMiniature version A

DAC

Digital to Analog

Chapter 1

Introduction - Time Synchronization in Communication Networks

1.1 Smart Cities and Time Critical Applications

Given the rise of smart city projects around the world, these are going to require a new type of infrastructure. The framework necessary for the transition of current day architectures requires a leap in the information and communication sectors. The European union defines a Smart City as a place where digitization is used to enhance the already existing infrastructure, and provide more efficient resources to its inhabitants [1]. The Cybersecurity and Infrastructure Security Agency (CISA) emphasises the critical role of timing reliability and resilience, and that without it critical infrastructures could become unreliable or unavailable [2]. Communications, Transportation, Power Grid, Finance, Security and IT are all sectors and industries that are dependent on time. This work focuses on the next generation of telecommunication networks, and being critical infrastructures, the attacks that can be perpetrated against them. Current day networks are reliant on costly atomic clocks, but future requirements in terms of phase synchronization are pushing the envelope on the need for higher standards. To this end GNSS is being proposed as a time keeping standard, this introduces new advantages and new threats. The main benefits of using GNSS receivers for time synchronization are reduced cost and availability, with an accurate time scale. This change also brings new vulnerabilities that can be exploited, such as radio frequency interference and cyberattacks. In order to assure good quality service and deter possible intrusions we perform an analysis on the efficacy of these systems.

1.2 Modern Day Synchronization Requirements in Telecommunication Networks

The continuous advancement of technology in telecommunication networks has also brought the need for new requirements of synchronization capabilities, along with the support for older technologies. Architectures such as 5G and LTE-TDD introduce new phase synchronization requirements [3]. The reasons why such phase synchronization requirements are necessary, involve the use of advanced strategies, such as enhanced inter-cell interference cancellation or the adoption of massive Multiple Input Multiple Output (MIMO) [3]. Given the complex timing synchronization required by future 5G networks, this results in the need for rigorous synchronization through different levels of a hierarchical network [3]. 5G can be implemented by using either Frequency Division Duplex (FDD) or Time Division Duplex (TDD), but the latter provides a more flexible solution. The basic way TDD works can be seen in Figure 1.1, where only one dedicated duplex frequency band is used, but upload and download are completed in different time slots. This time division calls for a "Guard Band" that separates upload and download frames, to avoid collisions. With different arrangements of these frames, different network performance is possible, each unique to the required scenario [4].

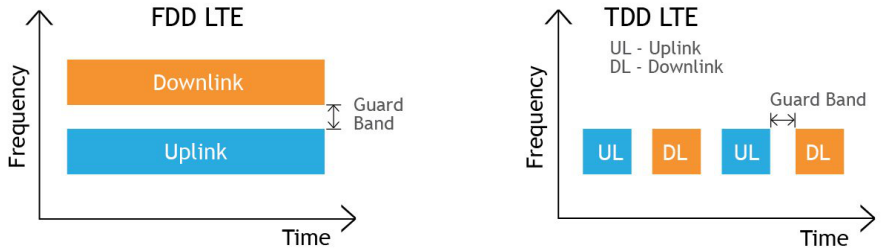


Figure 1.1: FDD vs TDD Operation, [5]

Overlapping TDD cell sites, that function at the same frequency, require strict synchronization among each other in order to avoid interference either between base stations or user devices [6]. In [7], the authors provide the estimate of ±65 ns to ±130 ns as the end-to-end accuracy requirement needs for the 5G inter-site Carrier Aggregation and Joint Transmission technologies. This is in line with the requirements also proposed in the ROOT project [3].

1.3 The ROOT Project and Reference Network Architecture

The core of the ROOT project is the creation of a hardware solution that utilises an interference resistant and Open Service Navigation Message Authentication (OSNMA) capable GNSS receiver to authenticate Galileo's navigation message and limit spoofing attacks. Previously, telecommunication operators have utilized specifically targeted networks for different services. With the continuous evolution of equipment this meant redundant upgrades that are costly, and the ever increasing complexity of the network. To sustain future paradigms and provide scalability, the ROOT project aims at the deployment of an all-IP network. This architecture utilizes end to end Multi Protocol Label Switching (MPLS) technology and is structured in hierarchical levels. In the specific case of the ROOT project, five different levels are envisioned, each with different roles [3]. As stated previously the aim is phase alignment, ranging from 65 ns to 130 ns for 5G front-haul applications [3]. In order to provide such accuracy to a network a Centralized Grandmaster Clock (C-GMC) node is tasked with the generation of a time reference by combining different time sources (i.e., multi-constellation, multi-frequency GNSS receivers, multiple co-located atomic clocks). The way though which the Centralized Grandmaster Clock obtains the time reference is a GNSS receiver that provides both a 1 Pulse Per Second (1-PPS) and a 10 MHz timing signal. The synchronization information is then spread across the network though the use of specific protocols (White Rabbit PTP) [3]. Figure 1.2 shows a possible high level definition of the reference network, where we can see the different elements providing synchronization information to the network, such as the Centralized Grandmaster Clock and Distributed Grandmaster Clock (D-GMC).

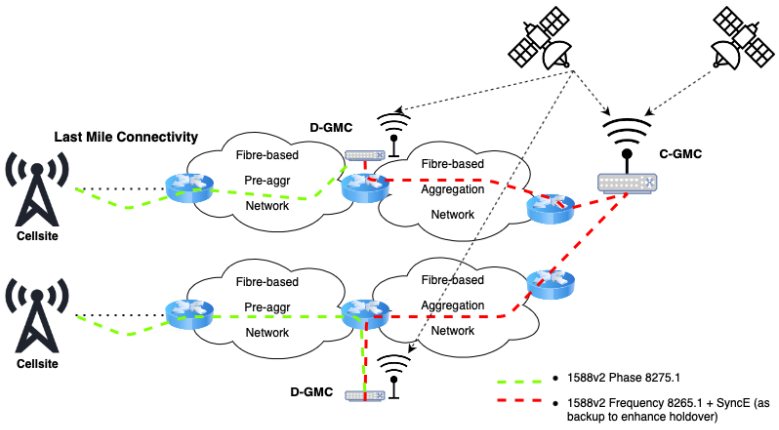


Figure 1.2: Possible Network Topology, [3]

We can see an example of how the synchronization is distributed in the network, though a White Rabbit Network (WRN) in Figure 1.3, where each White Rabbit switch is capable of housing a GNSS receiver, and also being synchronized by means of a distributed 1-PPS. A WRN consists of White Rabbit Nodes (nodes) and White Rabbit Switches (switches) interconnected by fiber or copper links [8]. A node is considered the source and destination of information sent over the WRN. A switch is defined as the key component of the White Rabbit System (WRS) that provides precision timing and high accuracy synchronization in an Ethernet-based network. The WRS distributes the clock of a WRS master (or its internal clock) to all the nodes in the network using a hierarchical architecture [9]. In Figure 1.3 we see the WR master in the top row on the left, that is aided by the integration of a GNSS receiver and/or Cesium atomic clock, that aims at providing long term stability to the clock. The information distributed over a WRN includes both timing and data, the former as frequency and International Atomic Time, and the latter as the ethernet traffic between nodes [8]. These can be seen as two different networks operating in the same system. To bring high accuracy and synchronization to the network the aim is to utilize multi-frequency GNSS receivers, integrated inside the Centralized Grandmaster Clocks (C-GMC) and Distributed Grandmaster Clocks (D-GMC), to provide a tool for drift control over long time periods and utilize the White Rabbit PTP (IEEE 1588 2019) protocol for the distribution of such signal [3]. The previous statement relies on the fact that the 1 Pulse Per Second signal is considered long term stable, while the stability of atomic clocks (Cesium and Rubidium) is questionable if left "free running" over long periods of time, such as various days or months. The distributed timing nodes are seen as the D-GMC in Figure 1.2 and are meant to provide resilient timing information to the system in case of outages, given their low cost. Each hierarchical level of the network has different clock implementations: the higher levels have GNSS aided receivers using a cesium atomic clock making them ePTRC (Enhanced Primary Time Reference Clocks), while lower levels house the GNSS receiver accompanied by Rubidium atomic clocks or OCXO (Oven Controlled Crystal Oscillator). Finally the simplest nodes only implement the GNSS receiver as time keeping source, obtaining the synchronization information through the timing distribution. This redundancy aims to make the network more reliable and resilient to possible loss of synchronization.

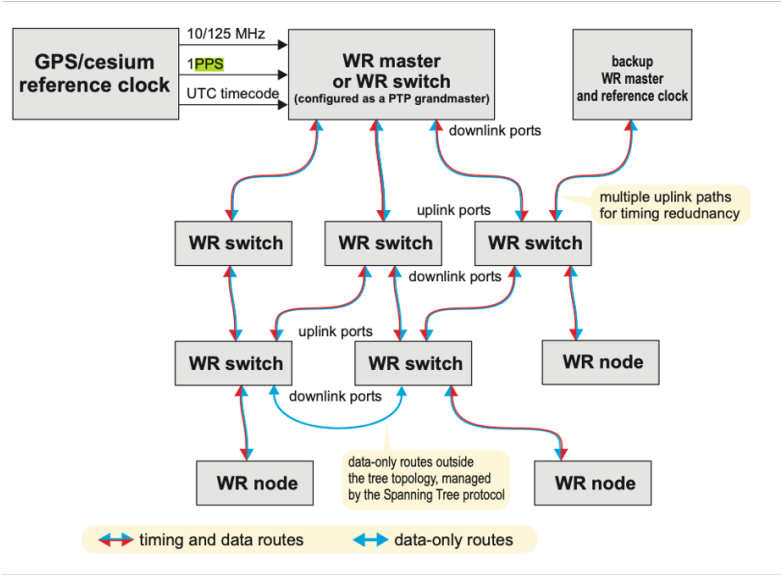


Figure 1.3: 1-PPS distribution through a White Rabbit network, [8]

Chapter 2

Time estimation and provisioning in GNSS receivers

2.1 Introduction to GNSS

GNSS systems today are used for three main purposes: positioning, navigation and timing (PNT). The USA's GPS constellation consists of 32 satellites, 24 of which are active at any time. The Russian GLONASS similarly has 26 total and 24 fully operational ensuring global coverage. Galileo, the European Union's constellation, also is made up of 24 operational satellites. As for GPS, the satellites are arranged into six equally spaced orbital planes, and each plane contains four slots each occupied by satellites. This arrangement makes it possible to almost always have line of sight with at least 4 satellites from any point on earth [10]. Galileo utilizes 3 orbital planes, 56.0° inclination, ascending nodes separated by 120.0° longitude (8 operational satellites and 2 active spares per orbital plane) [11]. Also GLONASS makes use of 3 orbital planes [12]. The GPS satellites transmit at different frequencies, L1, L2 and L5, respectively centered at 1575.42MHz, 1227.6 MHz and 1176.45 MHz. GPS signals are modulated using binary phase-shift keying (BPSK) that is a two phase modulation scheme where a RF carrier is either transmitted "as is" or with a 180 degree phase shift over successive intervals in time depending on whether a digital 0 or 1 is being conveyed [13]. The data signal takes the values of +1 or -1, as do the others. The main components that create the GPS signal are the navigation message, the C/A codes and the carrier frequency. The way in which these are combined make up the specific characteristics of the final signal. Direct sequence spread spectrum (DSSS) is an extension of BPSK

used by GPS and others. DSSS makes use of a third component, with respect to simple BPSK, referred to as spreading or Pseudo Random Noise (PRN) waveform, which is similar to the data waveform but at a much higher symbol rate. This PRN waveform is known to the intended receivers and often periodic [13]. DSSS is used for three main reasons. First, the phase inversions make precise ranging by the receiver possible. Second, the use of different PRN codes by each satellite enables the simultaneous transmission on the same frequencies. Third, DSSS provides significant rejection of narrowband interference, because for each bit that is transmitted there is a redundant bit pattern [14]. The use of multiple DSSS signals with different PRN codes on the same carrier frequency is referred to as code division multiple access (CDMA) [13]. We can see an example (not to scale) of how this process works for GPS in Figure 2.1, the navigation message is BPSK modulated with the spreading code and then with the carrier frequency. In the last row of Figure 2.1 we can see the final product of the modulation and as such the signal that is transmitted through space.

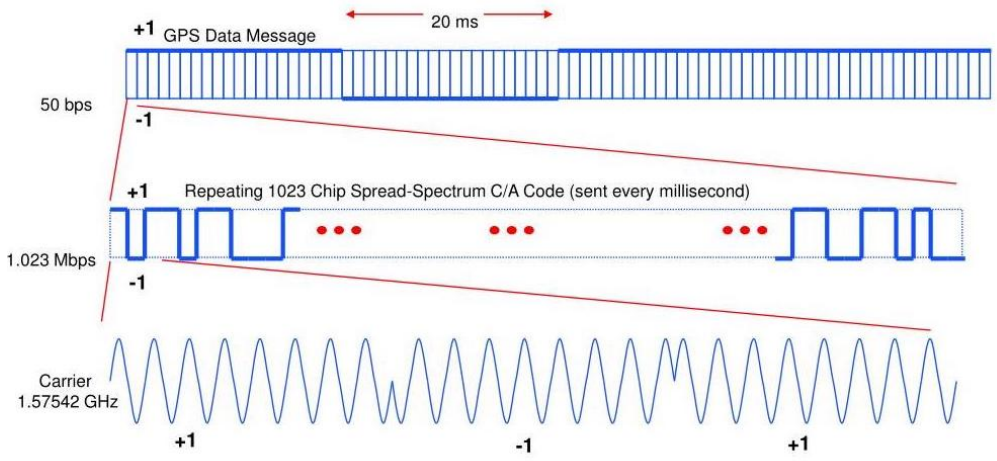


Figure 2.1: From top to bottom: Navigation message, C/A code and Carrier Frequency L1, [15]

GLONASS transmits at the center frequencies of G1 1602 MHz and G2 1246 MHz, using on the Frequency Division Multiple Access (FDMA) technique in contrast to CDMA employed by all the other GNSS systems. In Figure 2.2 we can see an illustration of how the different signals from the various constellations occupy the spectrum. In Figure 2.3 we can see how the different techniques of signal transmission, namely CDMA and FDMA, differ with respect to each other. The notable difference is between how GPS and Galileo transmit their signals vs how GLONASS uses a different frequency for each satellite.

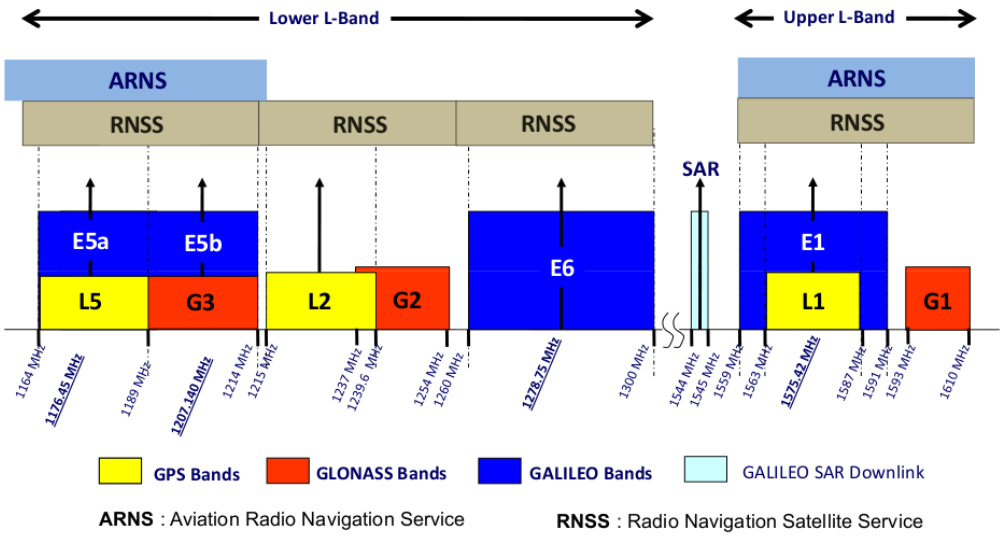


Figure 2.2: GNSS navigational frequency bands, [16]

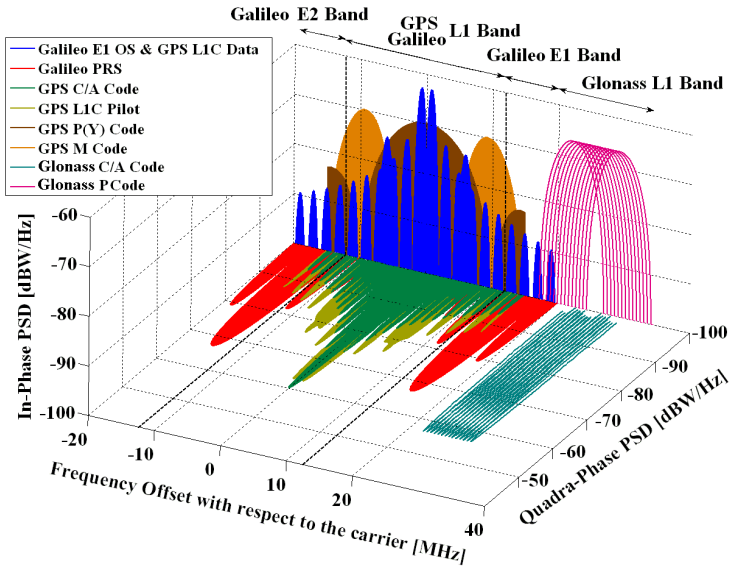


Figure 2.3: GNSS navigational frequency bands spectrum, [17]

The statements above explain the basic information about GPS, Galileo and Glonass satellites and how they cover almost any point on earth with their signals. For a user to obtain its position it is necessary to find the distance between them and multiple satellites. The distances are calculated as velocity·time, where the latter is the propagation time of the signal from the satellite to the user. The fact

that the signal transmitted by each satellite travels at the speed of light, means that even the smallest error in time synchronization creates large scale errors. This highlights the importance of accurate time keeping for the constellation. The way through which position and time are calculated by GNSS systems is called trilateration [13]. This procedure involves finding the intersecting point between at least 4 spheres.

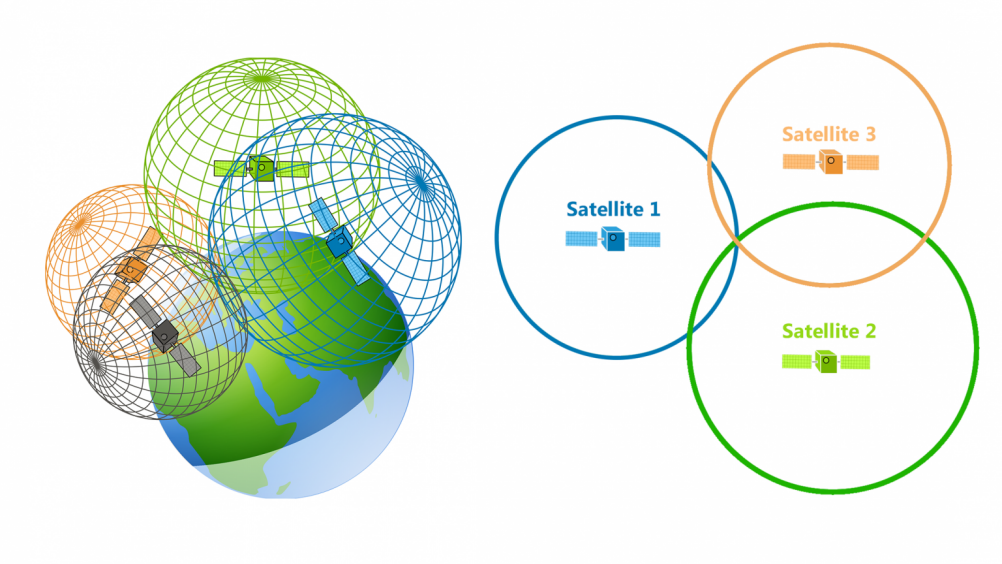


Figure 2.4: Trilateration in 3D and 2D, [18]

Each satellite is equipped with multiple atomic clocks, this is for redundancy only, that are used for time synchronization with the constellation. We cannot assume that the satellite clock and the receiver clock are synchronized, as this would introduce extreme costs for the user clock, because even the simplest chip scale atomic clock costs around 1500$ [19]. Each satellite's clock has a small deviation from the real GNSS time, called δt^S, but for simplicity we consider it zero as it is a known value and it is controlled by ground stations and included in the ephemeris data, in order to be compensated for. In order to calculate the distance between a satellite and the receiver we calculate the pseudorange as:

$$\rho = c \cdot \tau + c \cdot \delta_{tu} \tag{2.1}$$

where τ is the transmission time, in the sense of how long it takes for the signal to reach the receiver, and δ_{tu} is not an error but a design choice that indicates the clock error of the user receiver with respect to the GNSS system time. We can see that the pseudorange is not an Euclidean distance, because it involves the misalignment of time between the two systems. But if we write the pseudorange

equation as

$$\rho_1 - b_{ut} = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} \tag{2.2}$$

we see that on the right we have the equation that represents a sphere, centered in x_1, y_1, z_1.

The satellite and receiver clocks are not aligned and this introduces a new unknown, time. We then need to have at least four satellites in order to solve for the unknown variables of position (x,y,z) and deviation from the satellite system time, which we call the user clock bias b_{ut}. The user needs to measure four different pseudoranges in order to solve for the three position coordinates and the user clock bias. It is not possible to solve only one equation.

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} + b_{ut} \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} + b_{ut} \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} + b_{ut} \\ \rho_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} + b_{ut} \end{cases} \tag{2.3}$$

The satellite's position and signal transmission time are known, and transmitted by the satellite to the user. An important detail is that all satellites in view, need to be in line of sight, since we are measuring the propagation time of the signal. If the signal is reflected this leads to what is called the multi-path error [20]. We can perform two types of measurements on the satellite signals. The first one is called code phase measurement. The satellite sends a binary code, and the receiver generates the same code locally. The two codes are then compared and the difference in time between the codes is measured. The definition of pseudorange to a satellite is:

$$\rho(n) = c[T_R(n) - T_T(n)] \tag{2.4}$$

where c is the speed of light, $T_R(n)$ is the receive time corresponding to epoch n of the GPS receiver's clock (seconds) and $T_T(n)$ is the transmit time based on the Satellite vehicle clock (seconds) [13]. From (2.4), we can say that if the receiver can extract the transmit time from the code, then it can provide a pseudorange measurement [13]. Inside the time difference both τ and δt_u are present. We rely on the comparison of the two codes in order to obtain the pseudorange. The operation performed between the two signals is correlation, that provides the maximum correlation value where the signals are the same.

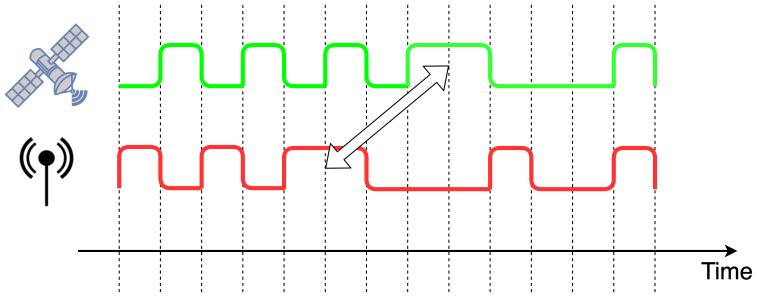


Figure 2.5: Codes generated by each satellite and receiver that are correlated

The second type of measurement is carrier phase, it is based on the fact that the code is modulated. Since there is modulation around the carrier frequency we can measure the distance in terms of how many cycles of the carrier are present between the user and the satellite. We measure an integer number of wavelengths and a fractional part. A local carrier is compared to the signal received from the satellite. Solving this problem introduces a new unknown, which is the number of integer cycles. It requires a more complex processing and is used in professional receivers. The (2.3) equations are then approximated using the Taylor expansion around a point that is assumed known. This is done because when the first satellites were developed, the computational capability available for receivers was not enough to solve these equations without linearization. Since the satellites are located in medium Earth orbit (MEO) at an altitude of 20,200 km [21], linearizing the spheres at the user's position does not create any major errors. We apply a Taylor expansion on the pseudorange. We assume that we know a point close enough to our position and known user clock bias value. This initial approximated position can be chosen with different methods, such as last known position. The Taylor expansion of the first order is:

$$\Delta\rho_j = \hat{\rho}_j - \rho_j \tag{2.5}$$

with $\hat{\rho}_j$ being the approximated pseudorange. Since $\Delta\rho_j$ is composed of different variables we write it as:

$$\Delta\rho_j = a_{xj}\Delta x_u + a_{yj}\Delta y_u + a_{zj}\Delta z_u - \Delta b_{ut} \tag{2.6}$$

with the a coefficients being the partial derivative of the function in the known location. By doing the derivative we find the coefficients to be:

$$a_{xj} = \frac{x_j - \hat{x_u}}{\hat{r_j}}, a_{yj} = \frac{y_j - \hat{y_u}}{\hat{r_j}}, a_{zj} = \frac{z_j - \hat{z_u}}{\hat{r_j}} \tag{2.7}$$

where $\hat{r_j} = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2}$ is the Euclidean distance between the linearization point and the satellite. The coefficient for each unknown is a

unitary vector centered in the approximated position of the user and pointed towards the satellite, and changes depending where the satellite is with respect to the user. The coefficients track the geometry of the problem.

$$\begin{cases} \Delta\rho_1 = a_{x1}\Delta x_u + a_{y1}\Delta y_u + a_{z1}\Delta z_u - \Delta b_{ut} \\ \Delta\rho_2 = a_{x2}\Delta x_u + a_{y2}\Delta y_u + a_{z2}\Delta z_u - \Delta b_{ut} \\ \Delta\rho_3 = a_{x3}\Delta x_u + a_{y3}\Delta y_u + a_{z3}\Delta z_u - \Delta b_{ut} \\ \Delta\rho_4 = a_{x4}\Delta x_u + a_{y4}\Delta y_u + a_{z3}\Delta z_u - \Delta b_{ut} \end{cases} \tag{2.8}$$

We can then state the problem in matrix notation:

$$\Delta\rho = H\Delta x \tag{2.9}$$

$$\Delta\rho = \begin{bmatrix} \Delta\rho_1 \\ \Delta\rho_2 \\ \Delta\rho_3 \\ \Delta\rho_4 \end{bmatrix} H = \begin{bmatrix} a_{x1} & a_{y1} & a_{z1} & 1 \\ a_{x2} & a_{y2} & a_{z2} & 1 \\ a_{x3} & a_{y3} & a_{z3} & 1 \\ a_{x4} & a_{y4} & a_{z4} & 1 \end{bmatrix} \Delta x = \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ -\Delta b_{ut} \end{bmatrix} \tag{2.10}$$

Where H is the geometric matrix of approximation coefficients. In the case of four satellites we can obtain the solution as:

$$\Delta x = H^{-1}\Delta\rho \tag{2.11}$$

This requires that H is invertible, so the matrix needs to be full rank. If two rows are linearly dependent the matrix is not full rank, meaning that the two vectors are parallel. The geometry of the problem has a high impact on the quality of the solution. If we use more than four satellites, the H matrix has a number of rows equal to the number of satellites used. The solution can be found using the least squares method. The solution is found by the Δx that minimized the square of the residual:

$$R_{SE}(\Delta x) = (H\Delta x - \Delta\rho)^2 \tag{2.12}$$

The solution is found by differentiating with respect to Δx and then setting the gradient of the transpose to zero, that gives:

$$\Delta x = (H^T H)^{-1} H^T \Delta\rho \tag{2.13}$$

2.2 Position, Velocity and Time estimation and errors

The pseudorange measurement unfortunately comes with errors, that affect the final solution of the problem.

$$\rho_j = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2} + b_{ut} + \epsilon \tag{2.14}$$

The introduction of errors to the equation changes the problem to be solved, that becomes:

$$\Delta\rho + \delta\rho = H(\Delta x + \delta x) \tag{2.15}$$

Since Δx represents the four unknowns, δx contains the errors relative to position and time. The solution is valid if the H matrix is full rank, and is:

$$\delta x = [(H^T H)^{-1} H^T]\delta\rho \tag{2.16}$$

The first part of the equation only depends on the geometry of the problem. The modelling of the error is statistical, and is described as a Gaussian variable with zero mean and variance σ_{UERE}. Each pseudorange measurement is independent from the other, but all the errors are described with the same statistical distribution. We are interested in the estimation of the error on the position given the error in pseudorange measurement. If we consider the covariance of the error δx, the result is the variance of the error in each dimension on the diagonal, and the cross correlation between the variables.

$$cov\ (\delta x) = \begin{bmatrix} \sigma^2_{xu} & . & . & . \\ . & \sigma^2_{yu} & . & . \\ . & . & \sigma^2_{zu} & . \\ . & . & . & \sigma^2_{b_{ut}} \end{bmatrix} \tag{2.17}$$

The trace of the error covariance matrix provides the variance of the error in position for each dimension. By definition the covariance matrix is calculated as:

$$cov(\delta x) = E\{(H^T H)^{-1} H^T \delta\rho\delta\rho^T H(H^T H)^{-1}\} \tag{2.18}$$

The expectation only acts on the $\delta\rho\delta\rho^T$ since it is the only random element of the equation, and this is like applying the definition of covariance matrix to the pseudorange error factor.

$$cov(\delta x) = (H^T H)^{-1} H^T cov(\delta\rho) H(H^T H)^{-1} \tag{2.19}$$

where only the elements on the diagonal have value because each satellite is independent from the other in terms of pseudorange. As said before, the $\delta\rho$ is characterized statistically as a Gaussian random variable with zero mean and variance σ^2_{UERE}.

$$cov\ (\delta\rho) = \begin{bmatrix} \sigma^2_{sat_1} & 0 & 0 & 0 \\ 0 & \sigma^2_{sat_2} & 0 & 0 \\ 0 & 0 & \sigma^2_{sat_3} & 0 \\ 0 & 0 & 0 & \sigma^2_{sat_4} \end{bmatrix} = I_{nxn}\ \sigma^2_{UERE} \tag{2.20}$$

We can then define

$$\begin{aligned} cov\ (\delta x) &= (H^T H)^{-1}\sigma^2_{UERE} \\ G &= [H^T H]^{-1} = [g_{ij}] \end{aligned} \tag{2.21}$$

$$cov\ (\delta x) = \begin{bmatrix} \sigma^2_{xu} & . & . & . \\ . & \sigma^2_{yu} & . & . \\ . & . & \sigma^2_{zu} & . \\ . & . & . & \sigma^2_{b_{ut}} \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & g_{13} & g_{14} \\ g_{21} & g_{22} & g_{23} & g_{24} \\ g_{31} & g_{32} & g_{33} & g_{34} \\ g_{41} & g_{42} & g_{43} & g_{44} \end{bmatrix} \sigma^2_{UERE} \tag{2.22}$$

Through these steps it is possible to analyze the error for each dimension.

$$\sigma^2_{xu} = g_{11}\sigma^2_{UERE},\ \sigma^2_{yu} = g_{22}\sigma^2_{UERE},\ \sigma^2_{zu} = g_{33}\sigma^2_{UERE},\ \sigma^2_{b_{ut}} = g_{44}\sigma^2_{UERE}, \tag{2.23}$$

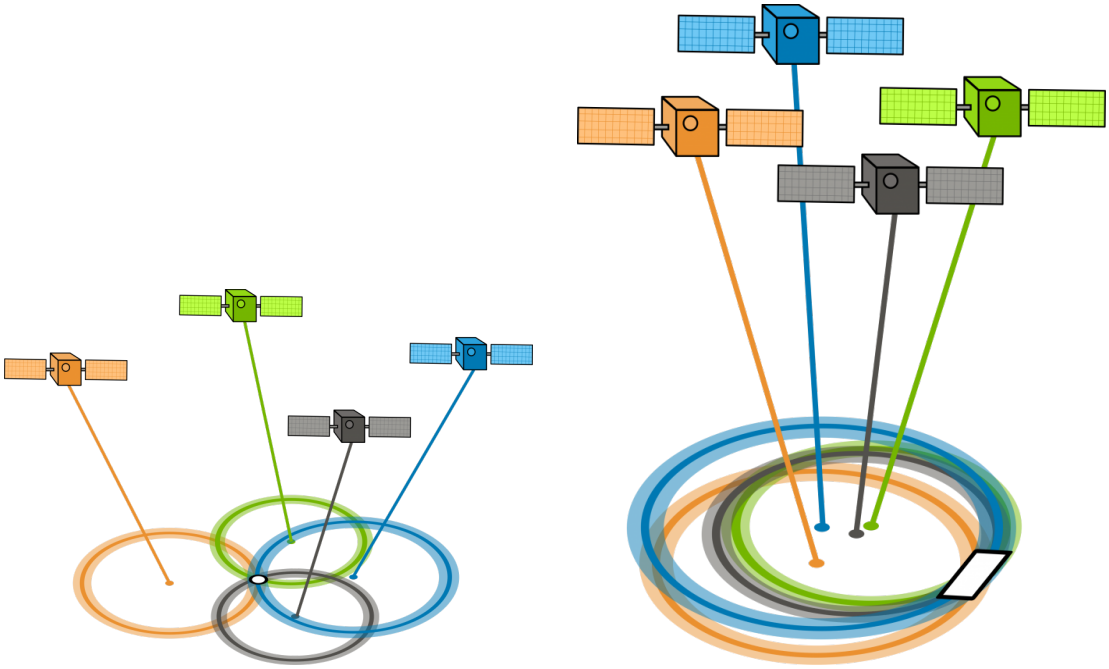
Through these definitions we can find the standard deviation of the positioning error σ_x as:

$$\sigma_x = \sqrt{\sigma^2_{xu} + \sigma^2_{yu} + \sigma^2_{zu} + \sigma^2_{b_{ut}}} = GDOP\ \sigma_{UERE} \tag{2.24}$$

with

$$GDOP = \sqrt{g_{11} + g_{22} + g_{33} + g_{44}} = \sqrt{tr\{(H^T H)^{-1}\}} \tag{2.25}$$

What is the meaning of the GDOP? Going back to the trilateration problem we assumed circles with no error boundary, but in real measurements there are errors and uncertainty as we described above. In Figure 2.6 we can see how the geometry of the problem influences the precision of the solution. The uncertainty around the spheres in 3D and the circles in 2D is described by zero mean and variance σ_{UERE}. The error definition is always the same but in 2.6b the uncertainty region is larger and depends only on the geometry of the problem.



(a) Good geometry problem (b) Bad geometry problem

Figure 2.6: Difference in good vs bad GDOP, [22]

In timing applications of GPS, the Time Dilution of Precision (TDOP) is the important value to observe for the precision of time generation.

2.3 Receiver time keeping and provisioning

GNSS systems were created as a navigation solution, but as a design requirement they also needed to be synchronized to extremely accurate levels. All satellites are equipped with multiple atomic clocks, known for their precision, accuracy and stability, but they are the most efficient when adjustments are kept to a minimum. For this reason the on board clocks are not exactly synchronized with the constellation but each one presents its own differences [23]. Since each satellite is not completely aligned with GPS time, the United States Naval Observatory (UNSO) tracks and monitors these drifts and uploads the information to each satellite in order for it to be transmitted in its navigation message. The main difference between GPS time and UTC is that unlike the latter, there are no leap seconds in GPS time, meaning it is a continuous time scale. GPS time starts at midnight between the 5th and 6th of January 1980. An example of how a satellite, receiver and actual GPS time might be aligned can be seen in Figure 2.7.

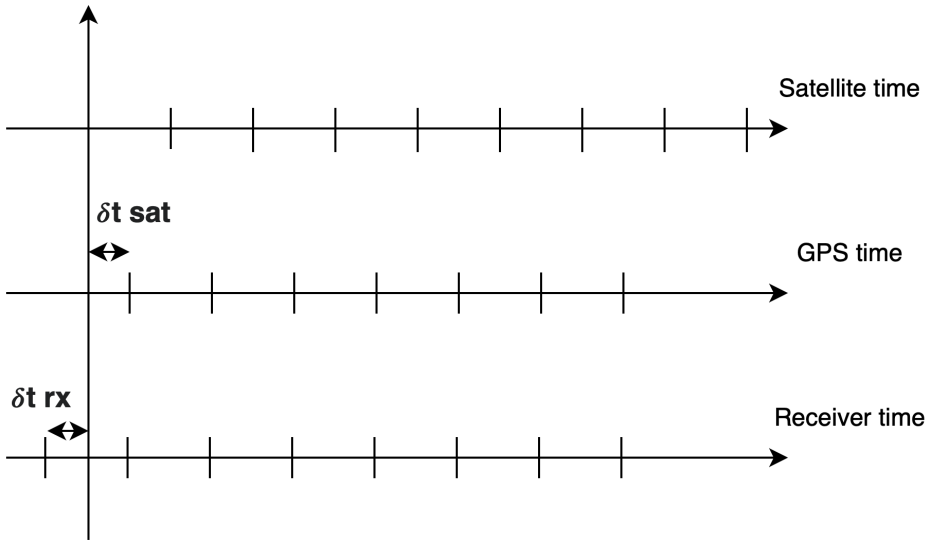


Figure 2.7: Timing offsets between GPS time, satellite time and receiver time

Many other factors need to be taken into account such as Einstein's Special Theory of Relativity. It states that a clock moving with a constant speed with respect to another clock appears to run more slowly. This phenomena is present in satellites since they are moving in almost circular orbits around earth. Einstein wrote in his General Theory of relativity that clocks that are under the influence of different gravitational potentials are subject to different properties. In the case of satellites, they are subject to a smaller gravitational potential than clocks on earth, so they appear to run faster. The combination of these effects creates a 38.4 microsecond gain for the clocks on board the satellite. In order to remove the effect of this gain, the satellite clock frequency is adjusted to 10.22999999545 MHz. Since GPS orbits are not perfectly circular, but tend to an elliptical orbit, the gravitational potential of each satellite also changes with time. This introduces an offset that varies with time that needs to be compensated. Fortunately all these drifts are tracked and compensated by the United States Naval Observatory. The same is done for all other constellations by each governing authority.

2.4 Relationship between GPS time and UTC

GPS Time now derives from a composite or "paper" clock consisting of all operational monitor station and satellite clocks. "Coordinated Universal Time (UTC), is obtained from the average of about 450 atomic clocks maintained in about 80 national laboratories worldwide" [24], and is maintained by the Bureau International

des Poids et Mesures (BIPM). GPS Time is steered over the long run to keep it within about 1 microsecond of UTC [23].

2.5 GNSS receiver time keeping capabilities

Considering all these factors GPS time is regarded as an excellent time keeping source. When using GNSS systems for timing applications, we are interested in the so called 1-PPS (Pulse Per Second) signal, generated by the receiver, used to synchronize and discipline consumer devices to the system time. The devices connected to the GNSS receiver use the PPS pulse as an indication of when to synchronize their clock to the incoming signal [25].

2.5.1 What is the 1-PPS

As the name implies it is a 1 pulse per second electrical signal generated by the receiver. The 1PPS is characterized in the literature as a low jitter signal [26]. Jitter can be defined as "Short-term variations of the significant instants of a digital signal from their ideal positions in time" (ITU).

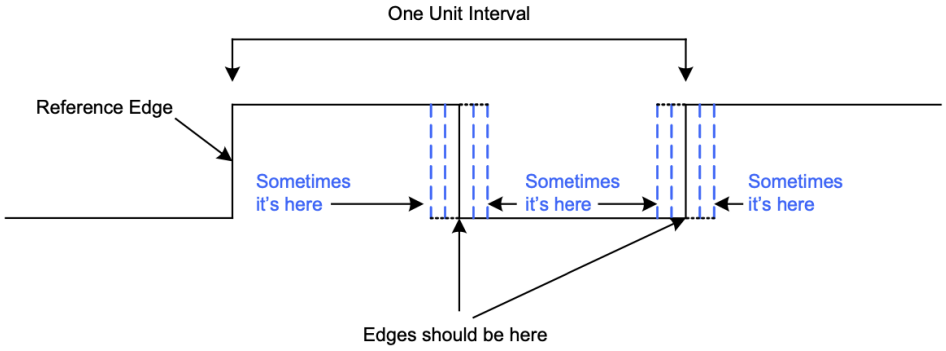


Figure 2.8: Digital waveform with jittered edges, [27]

The worst case short term fluctuations of the signal are around tens of ns, that translates to frequency variations as small as 10^{-7} Hz [26]. The receiver under test presents a 1-PPS jitter uniform distribution, as seen in Figure 2.9.

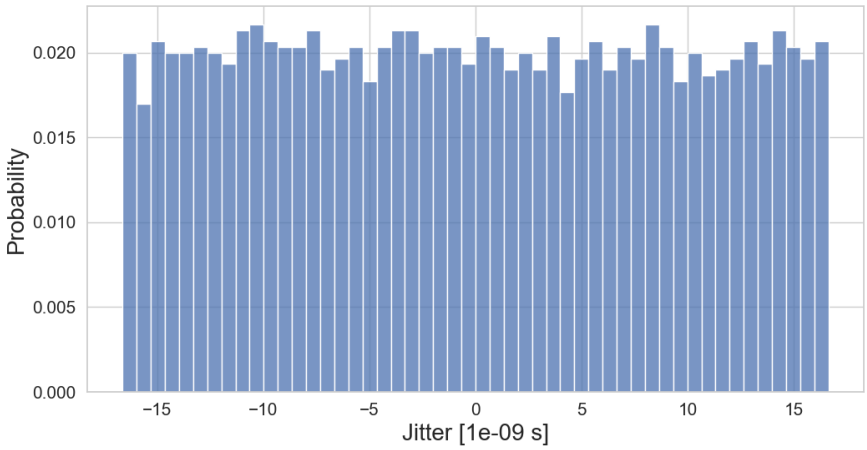
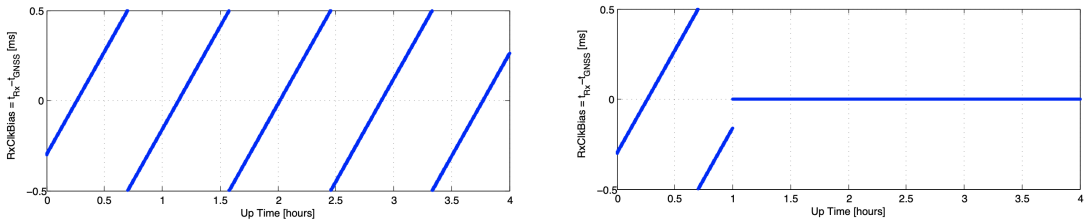


Figure 2.9: 1-PPS Jitter Probability Distribution

Satellite and receiver clocks are not synchronized by design, so when the receiver is activated it generates a random phase 1-PPS based on the local receiver time. This introduces an initial Δt between the real 1-PPS and the locally generated one [28]. The receiver then solves the first PVT and determines the receiver clock bias, and it obtains a new Δt_1 offset [28]. It applies this offset as a correction to the local time. After this adjustment the clock offset error is reduced from micro seconds to nanoseconds. The internal receiver clock is not perfect and is subject to drift with time, therefore some manufacturers provide the receiver with the "clock steering" capability. This method continuously tracks the local oscillator's drifts and compensates them [28]. For the receiver under test, the manufacturers explain the different clock modes in reference manual [29]. The receiver clock can be utilized in two different modes: Free Running or Steered. In free-running mode, the receiver time drifts with respect to GNSS time but it continuously monitors the offset: that is the clock bias term computed in the PVT solution. A clock jump of an integer pre-defined number of milliseconds is introduced to reset the clock each time it exceeds a threshold. This typically results in a saw-tooth profile similar to that shown in Figure 2.10a. In this example, each time the clock bias becomes greater than 0.5ms, a jump of 1ms is applied. In steered mode, the receiver time is continuously steered to GNSS time to within a couple of nanoseconds.



(a) Free Running Clock

(b) Steered Clock starting at 1 hour

Figure 2.10: Receiver clock bias behaviour Free Running vs Steered, [29]

Although the real position of the 1-PPS pulse is calculated correctly by the receiver, the expected edges in a digital data stream never occur exactly where desired. For this reason the actual pulse is generated at the first edge (rising or falling) of the local clock as shown in Figure 2.11. This leaves an offset (noted "D" in the Figure 2.11) between the true 1-PPS pulse and the one actually generated by the receiver. This offset can reach a few nanoseconds.

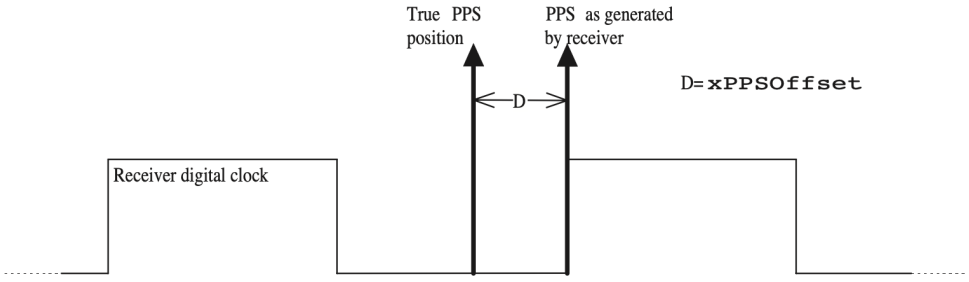


Figure 2.11: PPS offset, [29]

2.5.2 1-PPS Generation Techniques

How the 1-PPS signal is generated for a specific receiver is a tightly held industry secret. Thus we can only introduce the basic working principles. One possible technique used to generate the 1-PPS uses the combination of many elements inside the receiver, such as the internal clock, counters, registers, a latch and control unit. In Figure 2.12 we can see how the counter, registers and latch are used. The basic idea is to count "L" internal clock cycles that amount to the desired length of the impulse. We can see a first problem with the 1-PPS generation in Figure 2.13, since the impulse is generated synchronous to the local time base, if there is any misalignment between the internal clock and GPS 1-PPS then there is an error.

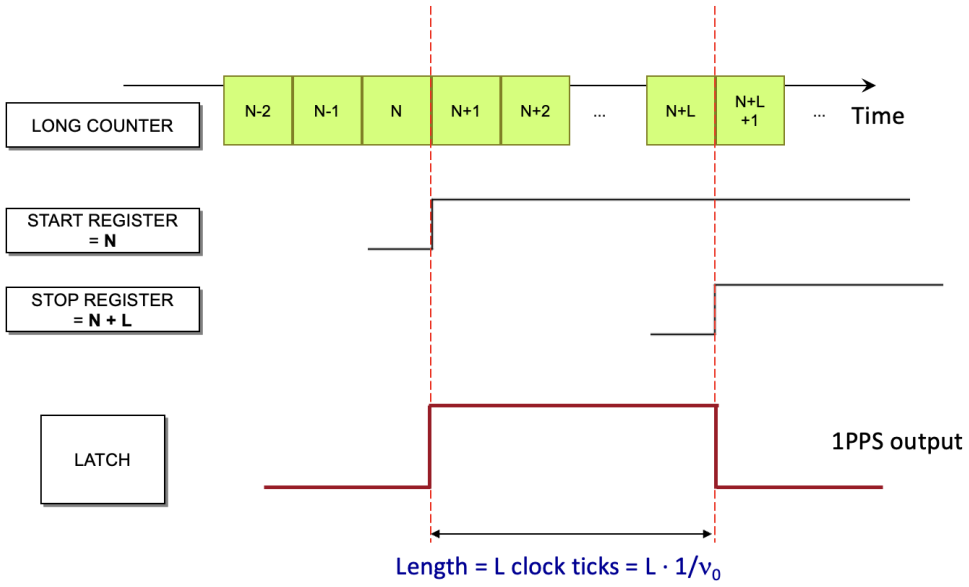


Figure 2.12: Electronic elements used to generate the 1-PPS, [30]

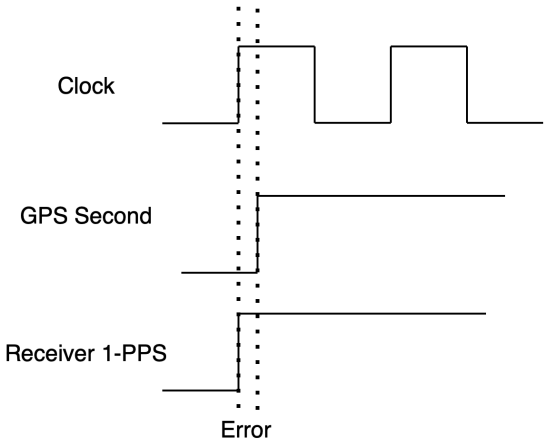


Figure 2.13: Error in 1-PPS generation due to non aligned GPS 1-PPS and internal clock

In order to generate the 1-PPS signal the control unit first calculates the PVT, extracting both the GPS 1-PPS and system time. The offset is calculated between the rising edge of the local clock and the computed GPS second. The first register used, named Start, is set to the closest edge (rising or falling) of the local clock with respect to the rising edge of the GPS second. Then the counter is used to track N cycles of the local clock that sum up to the desired impulse length. The

Stop register is then set to the closest edge to that of the GPS second falling edge. The two registers, Start and Stop, are the inputs to the latch which generates the electrical pulse. In Figure 2.14 we can see the relevant time instants. An important detail is the fact that the 1-PPS generated is not one second long, the receiver under test generates by default a 5ms pulse.

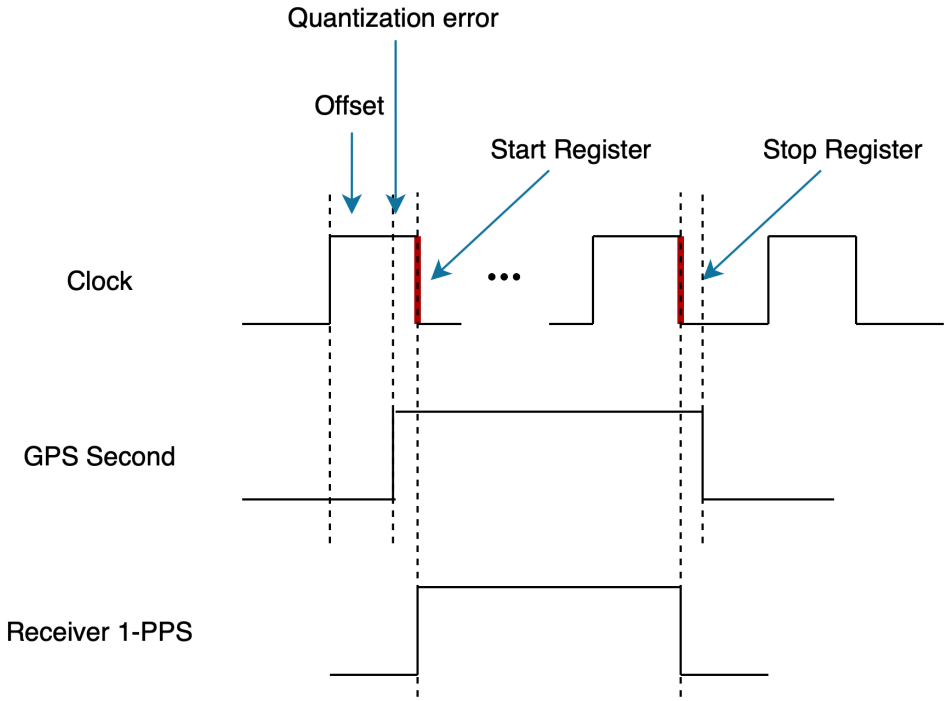


Figure 2.14: 1-PPS generation steps

A second method of generating the 1-PPS is by using the receiver's PRN code generator. Since by definition all bits of the codes are reset to ones every millisecond, though the use of decade dividers and a pulse generator, a 1-PPS signal can be created. Such an implementation is shown in Figure 2.15, where we can also see the clock steering mechanism.

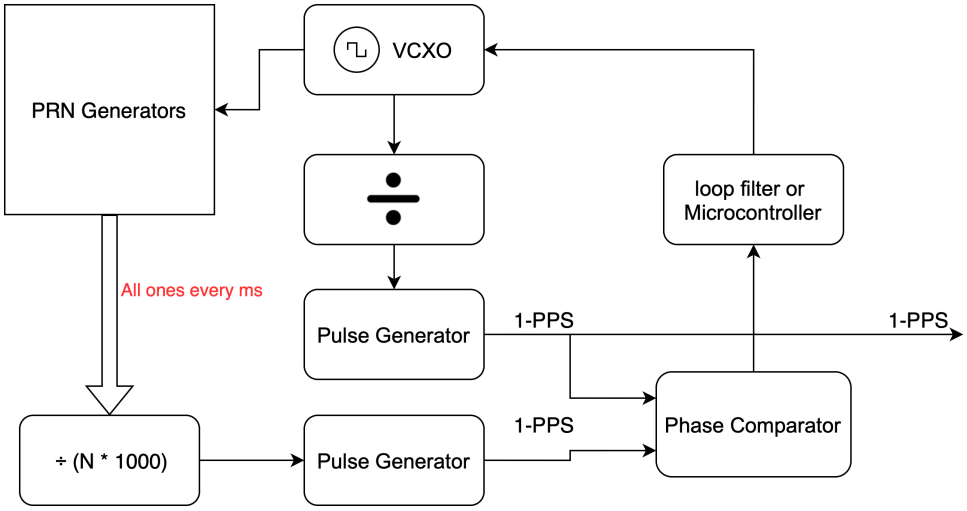


Figure 2.15: 1-PPS generation with steering

This system relies on the PRN generators being reset to the all ones state every millisecond. Making the assumption that GNSS receivers only use one internal clock to discipline all systems, if the clock is compromised by an attack, then also the PRN generators suffer from delays. In Figure 2.15 we can also observe a simple implementation of clock steering. The basic principle is to continuously adjust the internal clock to best follow the GPS system time. The system works by using a phase comparator on the signals generated by the PRN branch and the local clock branch, that outputs the phase difference between the two. This difference is fed to a loop filter or microcontroller which in turn sends the appropriate signals to the VCXO.

2.6 GNSS Receiver Front End, Acquisition and Tracking Stages

Before introducing the main types of attacks used in the next chapter, we briefly overview a GNSS receiver. In Figure 2.16 we can see a simplified block diagram.

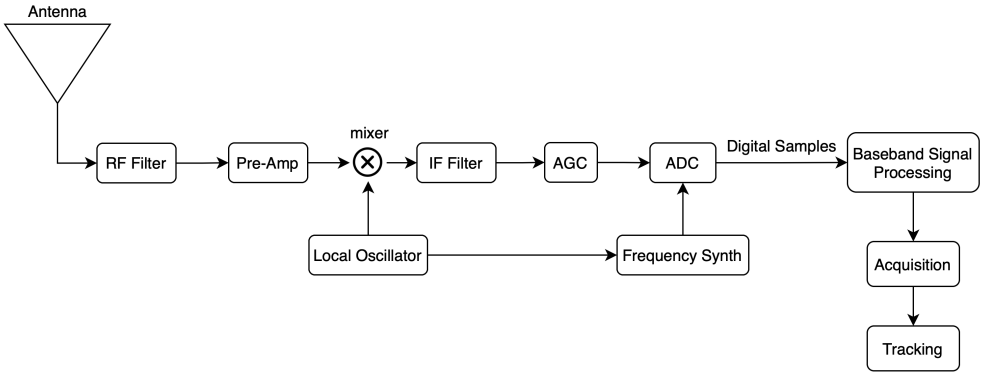


Figure 2.16: Simplified receiver functional blocks

The signal transmitted by the satellite can be written as:

$$s_{sat}(t) = Ac(t)d(t)cos(2\pi f_{L1}t) \tag{2.26}$$

where A is the amplitude of the signal, c is the PRN code of the particular satellite, d is the data and f_{L1} is the carrier frequency. The receiver obtains at its input $y_{RF,l}$, that is the sum of the signals from all the satellites in view along with noise and possible interference. We can see the incoming signal definition in equation 2.27.

$$y_{RF}(t) = \sum_{l=0}^{N_s-1} s_{RF,l}(t) + i(t) + n(t) \tag{2.27}$$

Only the $s_{RF,l}$ is the legitimate signal from satellite l, and can be written as:

$$s_{RF}(t) = \sqrt{2P_R}c(t-\tau)d(t-\tau)cos(2\pi(f_{L1}+f_d)t+\Phi) \tag{2.28}$$

where P_R is the power of the sinusoidal signal, τ is the time of flight of the signal, f_d is the Doppler shift and Φ is the change is phase.

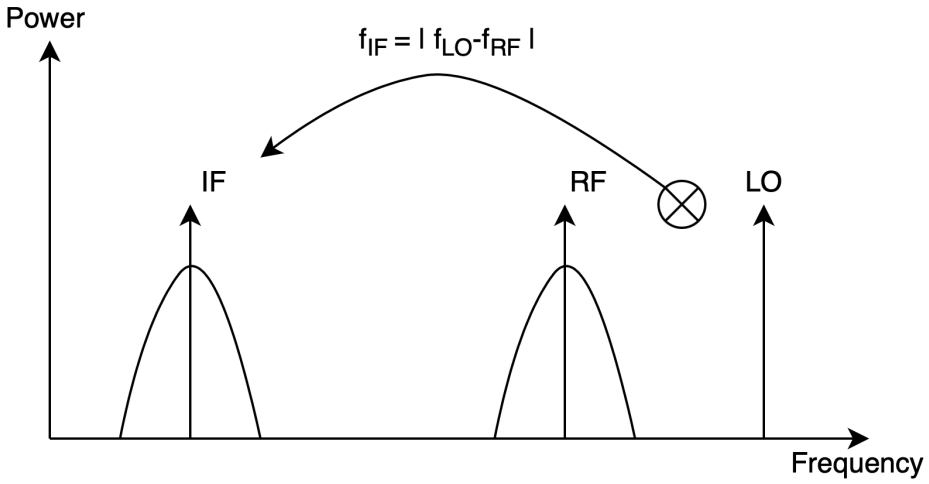


Figure 2.17: Mixer output of down sampled signal, with $F_{IF} \neq 0$

The initial operations performed by the front end of the receiver are filtering and down sampling of the incoming signal. The carrier frequency of the L1 signal is 1575.42 MHz, which would require a sampling frequency, as dictated by the Nyquist theorem, of at least twice the value. This would prove technically difficult. First the signal is passed through a band pass filter centered at the carrier frequency, then it is down sampled using a mixer. The mixer property is $cos(a) * cos(b) = 1/2[cos(a+b) + cos(a-b)]$, and we can see the effect in Figure 2.17. The signal we generate locally that is used to bring the received signal to intermediate frequency is:

$$l(t) = \sqrt{2} cos(2\pi(f_L + f_{IF})t + \Phi_{IF}) \tag{2.29}$$

The signal that is outputted by the combination of mixer and low noise amplifier (LNA) is:

$$\begin{aligned} y_{IF-FULL}(t) = \sqrt{C} c(t-\tau) d(t-\tau) \\ \Big[cos(2\pi(f_d + f_{IF})t + \Phi - \Phi_{IF}) \\ + cos(2\pi(2f_L + f_d + f_{IF})t + \Phi + \Phi_{IF}) \Big] \end{aligned} \tag{2.30}$$

The signal is then passed through a band pass filter (BPF) that removes the high frequency and keeps the signal centered ad f_{IF}. The output of the band pass

filter is :

$$y_{IF}(t) = \sqrt{C}c(t-\tau)d(t-\tau)cos(2\pi(f_d + f_{IF})t + \Phi - \Phi_{IF}) \tag{2.31}$$

This procedure is applied to enable the conversion from analog to digital with a feasible sampling frequency of f_s. The signal is then passed through both the automatic gain control (AGC) and the analog to digital converter (ADC), where the digital samples are generated. The digitized signal can be written as:

$$y_{IF}[n] = y_{IF}(nT_s) = Q_k^u \left[\sum_{l=0}^{L-1} s_{IF,l}(nT_s) + i_{IF}(nT_s) + n(nT_s) \right] \tag{2.32}$$

where Q_k^u is the quantization over k bits and n is the discrete time index.

We can expand equation 2.33 for a single satellite signal to:

$$y_{IF}[n] = Q_k^u \left[\sqrt{2P_R}d[nT_s - \tau]c[nT_s - \tau]cos(2\pi(f_{IF} + f_d)nT_s + \Phi) + i_{IF}[n] + \eta[n] \right] \tag{2.33}$$

where P_R is the received power, $i_{IF}(nT_s)$ is the interference, $n(nT_S)$ is the noise, τ is the delay, f_d the Doppler shift, d is the navigation data and c is the pseudo-random noise sequence. The receiver needs to estimate the τ, f_d and Φ parameters.

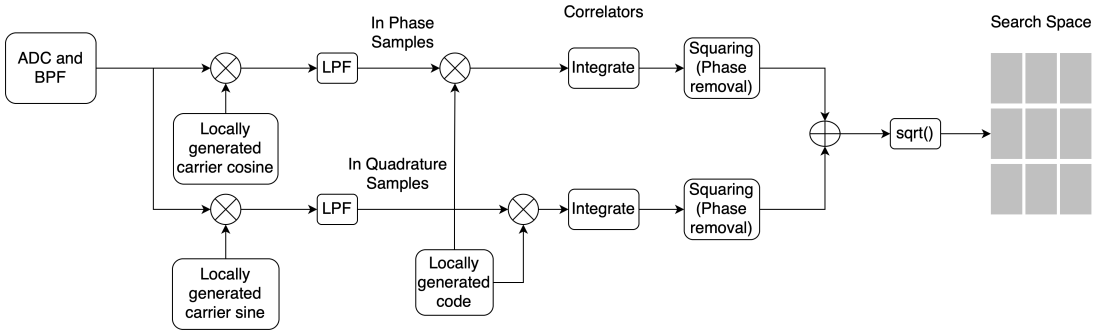


Figure 2.18: Acquisition block with coherent integration

In Figure 2.18 we can see the scheme of the acquisition stage, where the locally generated carrier cosine and sine are:

$$2cos(2\pi(f_{IF} + \hat{f}_d)[nT_s] + \hat{\Phi}) \tag{2.34}$$

$$-2sin(2\pi(f_{IF} + \hat{f}_d)[nT_s] + \hat{\Phi}) \tag{2.35}$$

Once these locally generated carriers are mixed with the incoming signal we obtain the in phase and quadrature samples S_I and S_Q, that are then combined with a locally generated code replica, that is:

$$c(nT_s - \tau) \tag{2.36}$$

The next step is the integration of the signals, that gives the final in phase and in quadrature components. The integration time is called coherent integration time. These are then squared and summed to remove the dependence from phase. This yields the bidimensional function $S^2_{y,r}(\hat{\tau}, \hat{f}_d)$, that is then evaluated over the search space. In the acquisition stage the main objectives are the detection of visible satellites and the rough estimation of delay and Doppler shift. An easy way to visualize this process is to imagine the tuning of a manually operated radio in a car. We know what a radio station should sound like, so we move the frequency in order to find a station, moving through the noise until we find a station. The search acquisition stage follows a similar procedure, where the radio channels are the search space, and our brain is the correlation function that finds the peak. The operation performed by the receiver in the acquisition stage is correlation, between the incoming signal and the locally generated counterpart. It is actually a two dimensional correlation operation, performed both for the code and carrier. Both a local code and carrier are generated, the latter being either a complex exponential $cos + j * sin$ that has both in phase and in quadrature components of the signal, or two different branches of a locally generated carrier that are shifted with respect to each other. The receiver estimates τ and f_d by considering the squared modulus of the correlation function, that we call the cross ambiguity function or CAF:

$$R_{y,r}(\hat{\tau}, \hat{f}_d) = \left[\sum_{n=0}^{L-1} y_{IF}[n] c[nT_s - \hat{\tau}] e^{j(2\pi(f_{IF} + \hat{f}_d) n T_s + \Phi)} \right] \tag{2.37}$$

We also set Φ to zero as an initial estimation.

$$S^2_{y,r}(\hat{\tau}, \hat{f}_d) = \left| R_{y,r}(\hat{\tau}, \hat{f}_d) \right|^2 \tag{2.38}$$

The cross ambiguity function is evaluated over a search space S, that is a grid of points that span the time and frequency domains. The receiver takes two approaches to using the search space, cold start and warm start. The former is used when no information is available, while the latter is used in cases where previous information is available or external tools provide such information. The main difference between the two techniques is the number of bins of the search space explored, using a warm start the receiver can find a fix in less time. Once the acquisition stage has fulfilled its purpose and found an initial estimate of τ and f_d, the tracking stage takes over. At the input of the tracking stage we have a signal that is as a code multiplied by a carrier. If we are able to remove the code

we can perform a fine frequency estimation, and similarly if we can remove the carrier we can obtain a code that we can use for a more precise delay estimation. The carrier wipe off is done by multiplying the incoming signal $y_{IF}[n]$ by the local replica of the carrier, generated thanks to the acquisition's initial estimate of the Doppler frequency and the feedback loop coming from the code wipe off branch. The signal resulting from the multiplication is then passed through a low pass filter, which outputs the code, that is then passed through a delay lock loop to continuously estimate the delay which is sent to the local code generator. The code wipe off is done in the other branch. The incoming signal is multiplied with the locally generated code, that if in phase with the incoming one should produce a unitary signal. Then we are left with a clean carrier, that is passed through a frequency lock loop (FLL) or phase lock loop (PLL), depending on the receiver architecture, for a fine frequency estimation. This value is then used as feedback and is sent to the local carrier generator. At the output of the tracking phase both a synchronized code and sinusoidal carrier are available.

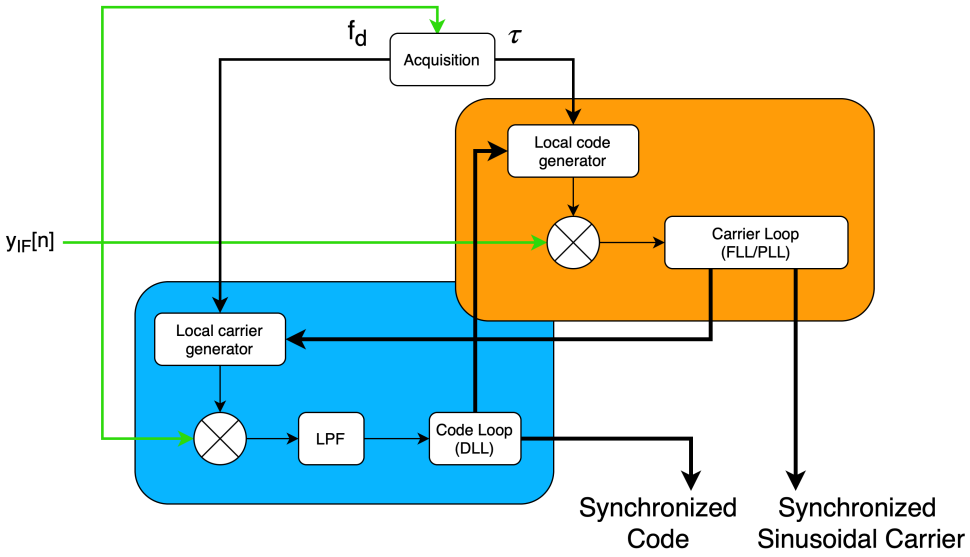


Figure 2.19: Tracking Loop

When both branches are locked to the incoming code, this is despread and converted to baseband, where all the processing is done. The navigation data bits can be decoded and the receiver knows when a new code period starts and can understand where the navigation message boundaries are. From here the receiver keeps track of all satellites in view and is able to calculate the needed pseudoranges to find both position and time.

Chapter 3

Threats to GNSS-based Time Synchronization

3.1 Radio-Frequency Interference

Radio frequency interference (RFI), is defined by No. 1.166 of the International Telecommunication Union (ITU) Radio Regulations (RR) as "the effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation or loss of information which could be extracted in the absence of such unwanted energy" [31]. By this definition we understand that any signal source that utilizes the same frequency as another can cause interference and consequently modify the original signal. As seen in the previous chapter, the pseudorange estimation is based on the measurement of the propagation time. Any signal that interacts with the GNSS signals causes interference, since it disturbs the original state [32].

3.1.1 RFI Examples and Current Day Events

Examples of radio frequency interference are not hard to find. Jamming devices are easy to buy though the internet and are used as personal protection devices by users trying to hide from tracking elements that make use of GNSS signals. These incidents have been reported starting at least 8 years ago, as seen in [33], many of them concerning lorry drivers trying to avoid being tracked, or avoidance of pay as you go systems. A more sophisticated example concerns the Russian Khmeimim Air Base in Syria. It is speculated that RFI is used to protect against possible threats, since months before there had been a coordinated drone attack on the base. As consequence the signals have reached Tel Aviv's Ben Gurion International Airport

[34], [35]. An extensive report on Russian interference was compiled by C4ADS, they describe themselves as "a non profit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide". Along with the help of Todd Humphreys and powered by Palantir. They claim to have detected 9,883 suspected instances across 10 locations that affected 1,311 civilian vessel navigation systems since February 2016 of GNSS spoofing events perpetrated possibly by Russia [36]. A commonly reported incident is discussed in [37], where a possible spoofing attack is detected by multiple ships in the black sea, which reported all being located in the same location. Another more recent example of using RFI as countermeasures is reported in [38], where during the most recent Nagorno-Karabakh conflict, the Russian Polye-21 system was utilized to negate the Azerbaijani drones [39]. Militaries are not the only ones that are adopting this technology, in [40] the author reports how Cartels have started using spoofing and jamming against border control drones. We can see how radio interference is a real problem in today's world, and can appreciate the importance of detection and mitigation of these events.

3.2 Classification of Interference

Interference sources can be either intentional or unintentional, as shown in the next sections. In order to classify an interference source two main aspects are analyzed: carrier frequency f_{cInt} and bandwidth B_{int}. Using these two main points we can make a first distinction between interference sources:

- Out of Band Interference, that refers to signals whose carrier frequency is close to GNSS bandwidth ($f_{cInt} < f_{GNSS} - B_{GNSS}/2$ and $f_{cInt} > f_{GNSS} + B_{GNSS}/2$)
- In band Interference is such that the carrier frequency falls within the bandwidth of the GNSS signals ($f_{GNSS} - B_{GNSS}/2 < f_{cInt} < f_{GNSS} + B_{GNSS}/2$)

When comparing the bandwidth values of legitimate signals with respect to interference signals a further classification is possible:

- Narrowband Interference, when $B_{int} \ll B_{GNSS}$
- Wideband Interference, when the bandwidths are similar, $B_{int} \approx B_{GNSS}$
- Continuous wave interference, is a special case of narrow band, when the bandwidth of the interference tends to zero

These first classifications rely only on carrier frequency and bandwidth but do not describe either time or frequency properties. Some interference sources are characterized by having frequency variation in time, such as chirp signals, that

appear in the frequency domain as wide band interference [32]. Others such as pulsed interference are characterized by a repeating on-off status and they are mostly found in aviation scenarios [32].

3.3 Naturally Occurring Interference

3.3.1 Multipath

The basic idea of multipath, is signal reflection. As explained in the previous chapters, GPS works by measuring the distance in terms of time between the satellites and the receiver. This means that if a reflected signal reaches the receiver, it has traveled a distance which is grater than the real one, making the receiver calculate a bad PVT. Usually most errors that affect the measurements can be removed using DGPS (Differential GPS), but not multipath, since there is no correlation of multipath error between two different receivers. All satellites move in time, making multipath also variable in time. The effect that multipath has on the receiver is a distorted cross ambiguity function, along side the displacement of the correlation peak. Methods to reduce multipath can be either in space or in time. The former involves the use of special antennas. GPS signals are right handed circular polarized, so when reflected they become left hand polarized, meaning that a special antenna with high gain for right handed polarized signals can be used. Time domain corrections involve the early and late codes used for the correlation function, usually receivers adopt a 1 chip difference, but using 1/2 chip can be beneficial, along with a wider bandwidth. In Figure 3.1 we can see the difference in travel distance between legitimate signals and reflected ones.

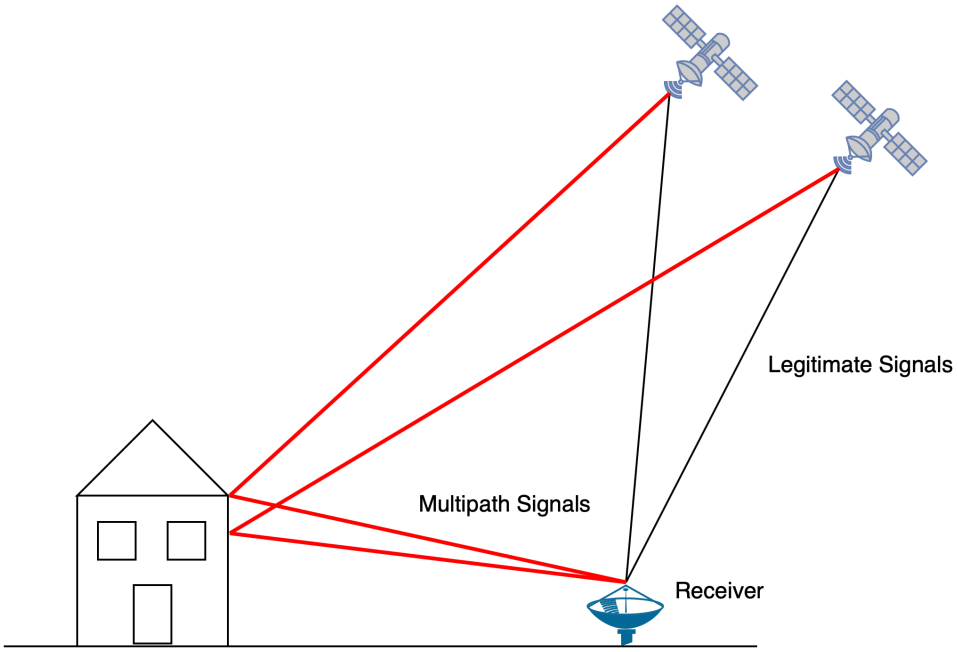


Figure 3.1: Legitimate Signals vs Multipath Signals

3.3.2 Atmospheric Effects

The ionosphere has to be taken into account when analyzing the propagation of a signal in the atmosphere. Due to the electron concentration, GNSS signals are affected by delays. These errors can either be corrected in part using purpose built models, or completely if dual frequency measurements are used [32]. Scintillations can introduce variations in amplitude and in phase, these depend on solar flares, location, season and magnetic effects [32].

3.4 Artificial Interference

3.4.1 Unintended

Intrasystem and Intersystem

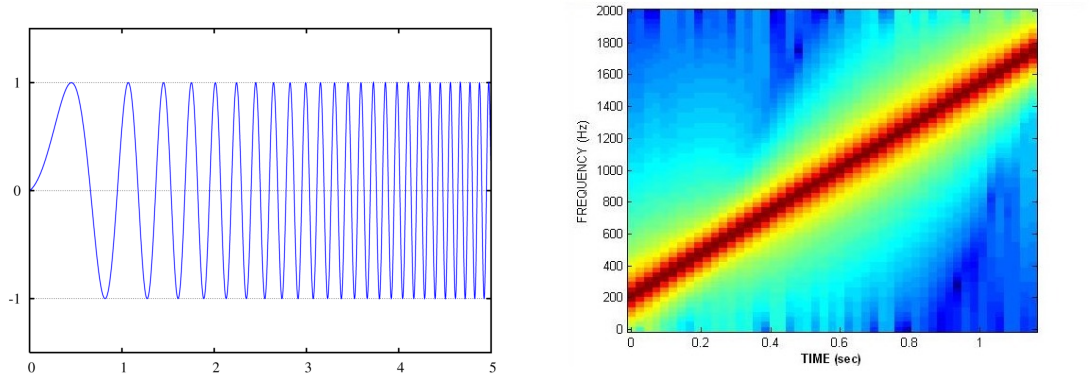
Intrasystem and intersystem interference analyzes the effect that signals from the same and other constellations have what arrives to a receiver [32]. Intrasystem interference belongs to signals from the same constellation, that are designed to be orthogonal, but this feature is not perfect so power leaks are always present. Intersystem interference is seen between constellations that use the same carrier.

For example both GPS and Galileo use similar frequencies, and power from the signals of one can disrupt the other. The effective carrier power to noise density theory is used in the design phase in order that a maximum level of interference is not exceeded [32]. These errors are mostly addressed in the design phase, and from a user's point of view only the use of directional antennas can mitigate such problems [32].

3.5 Intentional Radio-Frequency Attacks

3.5.1 Jamming attacks

Jamming, consist of specifically designed RF transmission overlapping GNSS signals bandwidths using amplitude-modulated, continuous wave, or chirp signals [3]. The objective of these attacks is masking certain portions of the spectrum with noise [32]. In the specific case of GNSS signals, a jammer is able to block a receiver from operating correctly [32]. They are the most frequent attacks since jammers are easy to acquire, and simple to use. For chirp signals bandwidth and sweep time are two main characteristics to keep track of. We can see an example of a chirp waveform in the time domain in Figure 3.2.



(a) Time domain

(b) Frequency domain

Figure 3.2: Linear chirp signal in time and frequency domains

Expected Effects on the Receiver

In this section we will analyze the effect of jammers on the different stages of a receiver. We can see the effects of jamming on the front end, the acquisition stage, tracking stage and estimated signal to noise ratio.

The front end filters the incoming signal, moves it to the intermediate frequency and then it sends it to the analog to digital converter. Before the signal reaches the ADC, it is passed through an automatic gain control element, which has the purpose of adjusting the power of the incoming signal. When no interference is present, the AGC mostly operates based on the thermal noise levels. When there is interference on the other hand, the AGC tries to reduce the signal in order to match the receiver input dynamics. This can be seen as a saturation, since the interference levels are so high, the AGC needs to lower the gain in order to function, thus loosing the original GNSS signal. If the interference is not saturating the receiver AGC and ADC process, then acquisition is still possible. The objective of the acquisition stage is to provide an initial estimation of the Doppler shift and code phase. The effect of interference on the acquisition stage is mostly concerned with the search space where both Doppler frequency and delay are being evaluated. The presence of interference makes it harder for the CAF to find a peak, even if thresholds are used. It is like looking for a peak among many peaks that are similar. Another way to look at it is imagining the noise floor as elevated. The impact of interference on the tracking stage has a direct correlation with the quality of the pseudorange [32]. The presence of jamming leads to an increase of the variance of the code and phase discriminator [41]. The navigation data decoding is highly affected by jamming and its power, events such as increased bit error rate (BER) and in the worst scenario it is not possible for the receiver to decode the navigation message [41].

3.5.2 Meaconing attacks

Meaconing attacks involve the reception and re-transmission of authentic GNSS signals, with the introduction of an additional delay. Such an attack can be modeled at the input of the receiver as:

$$y_{RF}[t] = \sum_{l=0}^{N_s-1} s_{RF,l}(t) + a_{RF}(t) + n(t) \tag{3.1}$$

where $s_{RF,l}(t)$ are the legitimate signals, $a_{RF}(t)$ are the retransmitted ones and $n(t)$ is the noise. The number of counterfeit signals are equal to the authentic ones, the only differences are the introduced delay and amplitude. The attack introduces additional noise to the system, due to the hardware components used to receive and re-transmit the original signal. Since for meaconing the interfering signals $a_{RF}(t)$ and the legitimate ones $s_{RF,l}(t)$ are the same, Equation (3.1) can be re-written as:

$$y_{RF}[t] = \sum_{l=0}^{N_s-1} A_m s_{RF,l}(t - \tau_m) + n_m(t) \tag{3.2}$$

An example of meaconing attacks is studied in [42], where the authors implement a detection strategy based on the receiver's clock bias. Their idea is to monitor the value of the receiver clock bias and mark any large increase and decrease with respect to the previous value as a possible start or end of an attack. Meaconing, when carried out correctly, is able to induce the receiver to display an incorrect a time which lags behind the correct system time. When a GNSS receiver is used as a synchronization element, such an attack can present a security flaw.

3.5.3 Spoofing attacks

Spoofing attacks are the most elaborate out of all. Their main feature is their aim of providing a incorrect position and time to a receiver without being detected, through the use of counterfeit GNSS signals. These attacks are usually classified into three main categories: simplistic, intermediate and sophisticated. A key attribute is the possible synchronization with the legitimate signals, which provides an additional layer of complexity. Simplistic attacks employ a GNSS simulator together with a front end in order to reproduce authentic signals, other methods involve the recording of authentic signals to be replayed at a later date, which draws similarities with meaconing. Intermediate attacks use devices that receive the authentic signals and through software generate authentic-looking counterfeit signals. Requirements for such attacks are stricter both in terms of accuracy and synchronization with original signals, along with knowledge of the intended target position and movement. The spoofer analyses key features of the authentic signal, such as the satellite information, in order to generate credible signals. The counterfeit signals are code phase aligned with the authentic ones, meaning the PRN codes that are a fundamental characteristic, are synchronized with the legitimate ones. In Equation (3.3) we can see the description of a single counterfeit signal, where $\hat{s}_{RF,l}$ can be either a delayed replica of the original signal or a newly generated one by the spoofer. Intermediate spoofing, attacks each tracking channel of the target receiver by acting on the delay lock loop (DLL).

$$s'_{RF,l}(t) = A_l \hat{s}_{RF,l}(t - \tau_l(t)) cos(2\pi \Delta f_l t + \Delta\theta_l) \tag{3.3}$$

The advantage spoofing presents over other types of attacks is the difficulty of detection. A detailed overview of how spoofers can be used to attack civilian GPS receivers is discussed in [43]. As their research shows even an intermediate spoofing attack is able to defeat many commercially available receivers. Finally the most intricate attacks are classified as sophisticated spoofing, where multiple portable receiver spoofers are used. This type of attack is able to bypass the angle of arrival mitigation technique since multiple transmitters are used. The complexity of such attacks makes them even more rare, with only experienced users able to deploy them. The majority of interference that receivers used as telecommunications

network timing sources encounter are mostly non intentional, jamming and at most meaconing. Since deploying a spoofing attack on a stationary target would not have as main objective the position, but time.

Spoofing: Generation, Receiver Vulnerabilities and Countermeasures

So far we have presented only a classification of different spoofing attacks but no actual knowledge on how they would be carried out and possible mitigation techniques to counter them. As for classification, also generation can be divided into categories. The main ones are done using a GPS Signal Simulator, Receiver-Based Spoofers or Sophisticated Receiver-Based Spoofers [44]. By using a GPS signal simulator the receiver sees the incoming signals as unstructured interference because the counterfeit signals are not synchronized to the GNSS system time [44]. The second type, receiver based spoofing, is more advanced since it uses a GNSS receiver to accurately retrieve position, time and satellite ephemeris. After this first step it then is able to generate legitimate looking spoofing signals [44]. This method is also harder to detect with mitigation strategies in view of the fact that the spoofing signals are hardly distinguished from the legitimate ones. A parameter that the spoofer needs to set correctly is the transmission power, in the interest of avoiding detection by transmitting too much power with respect to nominal values. Sophisticated Receiver-Based Spoofers are the most complex system to operate because they require high level of accuracy in antenna position and synchronization [44]. The effects that spoofing has on a receiver can be observed at different levels [44]:

- Signal Processing Level: Receivers are equipped with AGC elements that, if subject to high power spoofing signals, can increase vulnerability because they automatically adjust the input gain to compensate the high power, thus loosing the legitimate GNSS signals.
- Data Bit Level: The navigation data is acquired in less than one minute, but the ephermeris information remains the same for 12.5 minutes. By taking advantage of this factor, spoofers can regenerate the data frame.
- Navigation and position solution Level: The spoofer can introduce erroneous pseudorange measurements, forcing the receiver to calculate a wrong PVT solution.

Anti-Spoofing techniques are divided into detection and mitigation, as for many other types of interference. Some of today's spoofing detection methods are:

- C/N_0 Monitoring: Since Spoofers need to estimate the correct power to transmit, this can sometimes lead to an excessive amount of transmission

power. This factor can be used to detect a spoofing attack because the receiver should experience an sudden change in C/N_0 levels. A receiver can also store past information on power levels to compare as baseline values that should be correct [44].

- Absolute Power Monitoring: also this technique operates similarly to C/N_0 level monitoring, but it focuses on the noise floor. If there was to be a spoofing attack, this would lead to the noise floor increasing [44]. This can be seen as an indicator of an attack.

- Received Power Variations versus Receiver Movement: only available in dynamic situations and not for static receivers. If a spoofing attack is carried out using a fixed antenna, when the receiver moves it should see a considerable drop in power, with respect to a normal situation where the receiver movement should not highly influence the power received. On the other hand if the spoofer moves with the receiver, this is not a viable option.

- L1/L2 Power Level Comparison: There is a defined power level difference between the two frequencies L1 and L2, that should be monitored by the receiver. If this ratio is not respected, it could be an indication of a spoofing attack. Using such an approach entails having a multifrequency receiver able to monitor multiple frequencies at the same time [44].

- Spoofing Discrimination Using Spatial Processing: Techniques such as Multi-antenna Spoofing Discrimination are used where the phase difference between two different antennas is used as an indicator.

- Distribution Analysis of the Correlator Output: Under the condition of line of sight operation, the correlator output power should have a χ^2 distribution. The introduction of spoofing signals leads to disturbances in the correlator output amplitude, that no longer has a χ^2 distribution [44].

- Cryptographic Authentication: such as Galileo's new Open Service Navigation Message Authentication (OSNMA) that allows receivers to authenticate the origin of the incoming signals.

Mitigation on the other hand has as its main objective removing the spoofing signals and restore the normal operation of the receiver. Different algorithms and approaches have been proposed and gathered by [44]:

- Multi-antenna Beam Forming and Null Steering: A receiver using multiple antennas can detect and localize the direction of origin of spoofing attacks and consequently adjust the direction of gain of the antennas and possibly introduce nulls to cancel the spoofing signals.

- Receiver Autonomous Integrity Monitoring (RAIM): performs consistency checks on the values of the pseudoranges and eliminates outliers. This method is only viable when few spoofing measurements are seen by the receiver.

3.6 Interference Detection and Mitigation Strategies

When operating in an environment where GNSS receivers are subject to interference, both detection and mitigation become of fundamental importance.

The different modes that interference attacks the normal operation of a GNSS receiver are [32]:

- Saturation of the front end
- Mixing effects that come from the inability of the receiver of generating a pure tone for the down conversion
- Intermodulation products
- Misidentification of out of band signals that remain after filtering
- Reception of in band interference due to signal generation properties and imperfections

Radio interference attacks to the signal in space, such as spoofing and meaconing are not detectable by generic anti interference techniques that are meant to deal with "unstructured" signals [32]. In cases where the interference in unstructured, the objective is to recognize and detect such signals that make the receiver deviate from normal operating conditions, and alert the system to the presence of interference. The techniques use different variables found in different stages of the receiver.

3.6.1 Detection Models

The interference detection methods can be classified as [32]:

- AGC Monitoring
- Time domain statistical analysis
- Spectral monitoring
- Post correlation statistical analysis
- Carrier to noise power ratio monitoring

- Pseudorange monitoring

The first three approaches are applied to the DSSS signal received before any de-spreading is done [32]. This means that the output of these systems can alert the receiver procedures of interference. The last four items require an initial normal operation period in order to be successful at detection, since they hinge on monitoring normal values and checking for anything out of range. There is not a "one fits all" strategy for detecting interference, but some approaches can be tailored to specific problems [32].

3.6.2 AGC Monitoring

The Automatic gain control element of a receiver acts as a variable gain amplifier, and its job is to minimize the quantization losses by adjusting the input power of the signal to the ADC. Since power levels of legitimate GNSS signals are below the thermal noise floor, so the AGC is driven by the noise floor itself and not the GNSS signals. The way in which the AGC is adjusted means that if interference is present, the AGC increases the dynamic range by reducing its gain and limiting signal saturation [32]. The exact way that the AGC element reacts varies by implementation and build, but it usually follows a piece wise constant function [32]. Monitoring the AGC values has been found to be a good detection strategy for interference [45]. Under normal conditions the value of the gain should change slowly and be within known thresholds. Instead under interference conditions sudden changes would be visible, and marked as possible problems.

3.6.3 Time Domain Statistical Analysis

Statistical analysis can be used to detect time varying sources of interference. It is based on the observation of the ADC samples in time [32]. The concept relies on the fact that samples should follow a random process whose statistical peculiarities are influenced by interference. Since the type and attributes of the possible interference are not known before hand, a non parametric goodness-of-fit (GoF) detection model can be used [32]. In order to detect interference the intermediate frequency samples that are the output of the ADC are used to build a test statistic. A decision is then made based on the behaviour of the histogram [32]. The histogram that is an output of the ADC, is the distribution of samples that are converted, thus if there is noise the histogram has a larger spread with respect to the one that a normal signal would provide. To detect possible interference, the measurement is based on a finite number of samples. This is a particular application of hypothesis testing,

where a binary hypothesis is proposed as:

$$\begin{aligned} H_0\ (RFI\ absent) &: p_X(x) = p_Y(x), \\ H_1\ (RFI\ present) &: p_X(x) \neq p_Y(x), \end{aligned} \tag{3.4}$$

where $p_X(x)$ and $p_Y(x)$ are probability density functions (PDFs) of a stationary random process in the time interval of observation [32]. The detection method works by first having a process distribution where no interference is present, then building the observation histogram and evaluating the test statistic used to discriminate between the two hypothesis. A threshold value is chosen in order to make a decision, known as the level of significance [32]. Based on the value of the comparison and threshold, a decision is made on the whether interference is present or not.

3.6.4 Spectral Monitoring

The legitimate signal that arrives to a receiver has a power level that is smaller than that of the noise floor. A spectral estimation of the received signal is possible and it should be characterized by the equivalent transfer function of the front end of the receiver and multiplied by the noise variance [32]. After proper calibration the interference free expected spectral estimate is known. It is possible to detect an interfering signal by the power level exceeding the noise floor and comparing the estimated expected power spectral density with the nominal one [32]. This technique is resource heavy because it makes use of either fast Fourier Transforms (FFT) or periodogram methods. They need relatively long observation windows and periodograms are also subject to spectral leakages [32].

3.6.5 Post-correlation Statistical analysis

Interference that makes it past the correlators is one of the most insidious, because it degrades the measurement and thus damaging the PVT solution [32]. The unwanted interference can be detected by applying detection systems to the output of the correlators. Techniques based on the parametric spectral analysis built on harmonic analysis of random processes are used to detect narrow band interference. The idea relies on the vector of samples taken at the output of the correlators, that are subject to harmonic analysis. The largest eigenvalues of the covariance matrix of samples are signals of harmonic components and thus used to detect interference.

3.6.6 Carrier to Noise Power Ratio Monitoring

This approach is not a detection method as a stand-alone product, but it is a good resource for impact evaluation of possible interference [32]. The carrier to noise (C/N_0) levels are computed by the receiver for each satellite in view, based on

postcorrelation observations. Many factors can cause the reduction of C/N_0 levels, and because of this only generic information on the health of the signal is obtained. For example a slowly decreasing C/N_0 value of one satellite could indicate that it is on the path to the horizon. If all satellites in view suffer from a sharp C/N_0 variation, depending on the situation at hand, could indicate the possible presence of interference.

3.6.7 Pseudorange Monitoring

The levels of C/N_0 and their quality are determined by the correlators. The synchronization of the local replica code and carrier is of fundamental importance [32]. A deterioration in signal tracking also affects the pseudorange estimates. This system is highly effective when using multi-frequency receivers, since consistency control of the pseudorange measurements obtained from a single satellite on two different frequencies can show the presence of interference [32].

3.6.8 Mitigation of Interference

Classification of mitigation methods is based on the domain to which they belong. They are usually classified as [32]:

- Frequency domain techniques, where the spectrum is utilized as the main tool
- Time domain techniques, that work either by preventing the interference from reaching further stages of the receiver or by acting on the incoming signal itself
- Time space domain techniques, mostly based on spatial filtering that introduces attenuation in the direction of interfering signals, through the use of beamforming or null steering techniques

Frequency Domain Techniques

Frequency domain techniques try to remove as much interference as possible while preserving the maximum amount of spectrum at the same time. These techniques are highly effective when countering either narrow band interference or continuous wave perturbations, since these affect a small portion of the GNSS spectrum. If the interference changes its frequency characteristics in time the mitigation module has to adapt in order to follow the perturbation. We can see this frequency variation in time utilized for low cost jammers, where chirp signals are used to disturb a wide portion of the GNSS spectrum [32]. Frequency domain mitigation techniques are not best suited for combating pulsed interference since spectral estimation needs

to observe segments of time where the frequency characteristics are averaged to obtain the results [32].

The two common techniques usually seen implemented are Frequency domain adaptive filtering (FDAF) and notch filtering.

Adaptive Filtering (FDAF)

FDAF is based on the observation of the spectral characteristics of the incoming signal and the knowledge of how a "correct" spectrum should be. The spectral estimation is done through the use of fast Fourier transform (FFT) over a predefined time window of N samples [32]. The real GNSS signal's power are below the thermal noise floor, and when the FFT is performed the output should be flat. The FFT converts a signal into individual spectral components and thereby provides frequency information about the signal . If after the FFT computation, there are points that exceed a threshold in power, these are carefully removed from the spectrum and set to zero [32]. The inverse FFT is then computed to obtain the signal in the time domain. The two main parameters used that need to be correctly chosen are the sampling frequency of the incoming signal f_s and the number of samples N that are divided into segments each of N_D samples [32].

Notch Filtering

This type of countermeasure is aimed at compensating continuous wave interference (CWI) such as pure sinusoids. CWI causes high degradation in both the acquisition and tracking stages because it impacts the correlation stages [32]. The most common implementation is seen as infinite impulse response (IIR) filters, that are pass bands with a very narrow rejection band.

Time Domain Techniques

Time domain techniques for interference mitigation are not always the best, because the incoming GNSS signals are mixed with the interference and it is not possible to work on only one or the other separately [32].

Pulse Blanking

Design specifically for pulsed interference, initially implemented through hardware, today through digital circuits, pulse blanking techniques operate by thresholding the samples that are outputted from the ADC. This system requires ADC with high number of bits, because some are dedicated only for the GNSS signal, while the higher value ones are reserved for interference detection. Otherwise if the ADC is not properly tuned it would suppress the incoming GNSS signals [32].

Chapter 4

Experiment set up and configuration

4.1 GNSS receivers as Timing Elements

The idea of using GNSS receivers as timing elements is born from the fact that each constellation can be seen as a synchronized system. The International Bureau of Weights and Measures (BIPM) has the role of generating UTC that is a post-processed time scale since it is the result of worldwide cooperation of 78 institutes [46]. Coordinate Universal Time (UTC) provides the time reference in all countries, with the correct time zone and offsets applied and all GNSS systems are based on UTC, each with its particular design decisions [46]. Knowing the offset of the GNSS system time with respect to UTC from the navigation message, the user can estimate the offset of its clock to UTC [47]. Each constellation steers its time towards UTC, except for the integer second offsets that result from different choices of origin and system time scales [46]. The GNSS receivers in question are those able to discipline their internal clock [46]. These are then able to generate both the 1-PPS signal and a 10MHz reference [48].

4.2 Experiment Setup

The analysis proposed in this thesis required the experimental set up to be designed from scratch. The only constraint was to have one receiver under attack along with another receiver used for comparison and not under attack. Along side the two state of the art receivers, an older module was also used for under attack comparison. The state of the art receiver under test is the mosaic-T by Septentrio. We can see the receiver in Figure 4.1, with all important inputs/outputs highlighted.

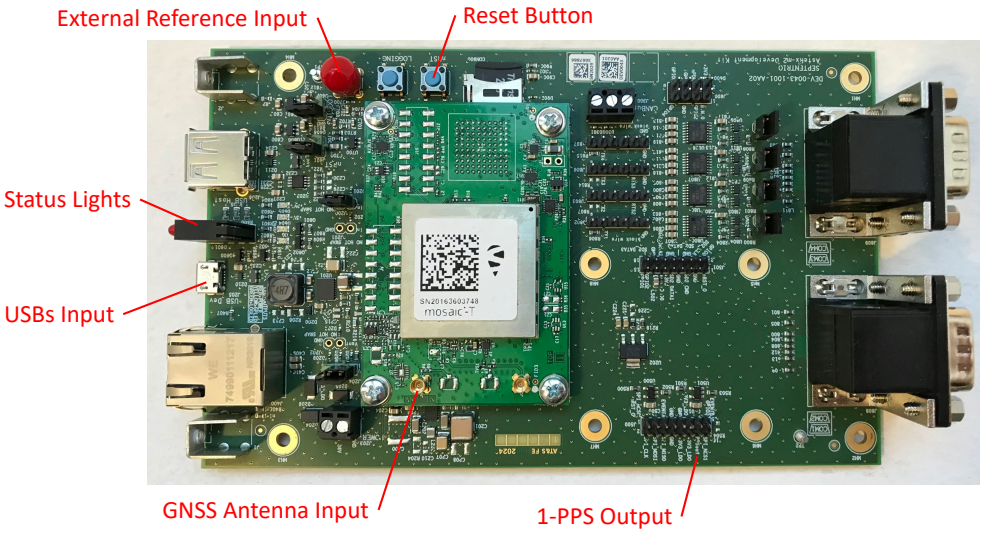


Figure 4.1: Septentrio mosaic-T state of the art timing receiver

We can see the jamming configuration set up in Figure 4.2, where the components are the following:

1. Is the Rubidium atomic clock, used as an external frequency reference of 10MHz for the state of the art receivers

2. The four way passive power divider, where the legitimate GNSS signals enter the system and are then split and sent to the receivers under test

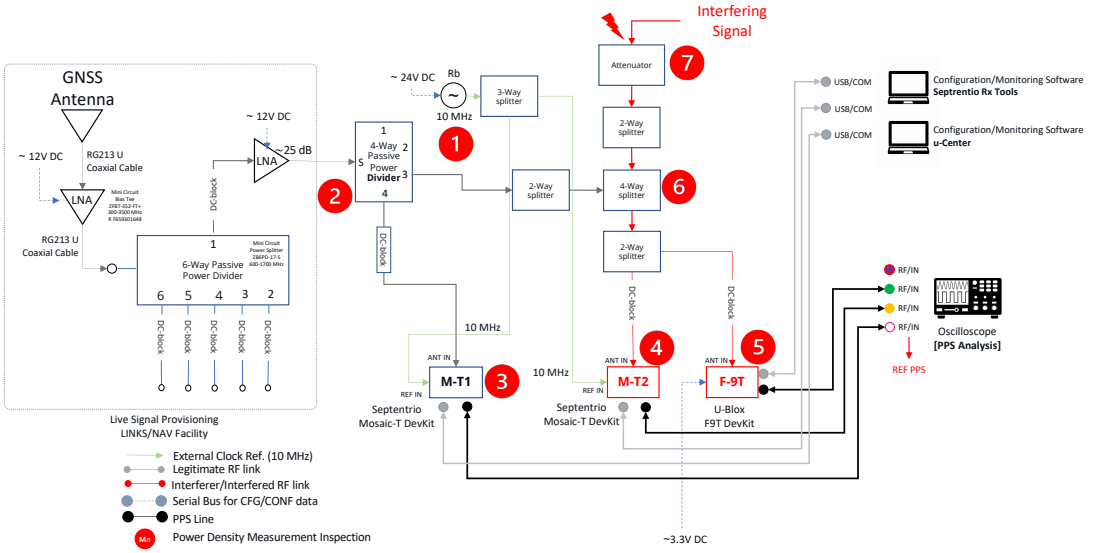
3. Septentrio mosaic-T development kit used for reference, not under attack, where the undisturbed 1-PPS is generated

4. Septentrio mosaic-T development kit under attack

5. Ublox FT-9 development kit under attack, used as a reference of non timing receiver without Septentrio's radio frequency mitigation

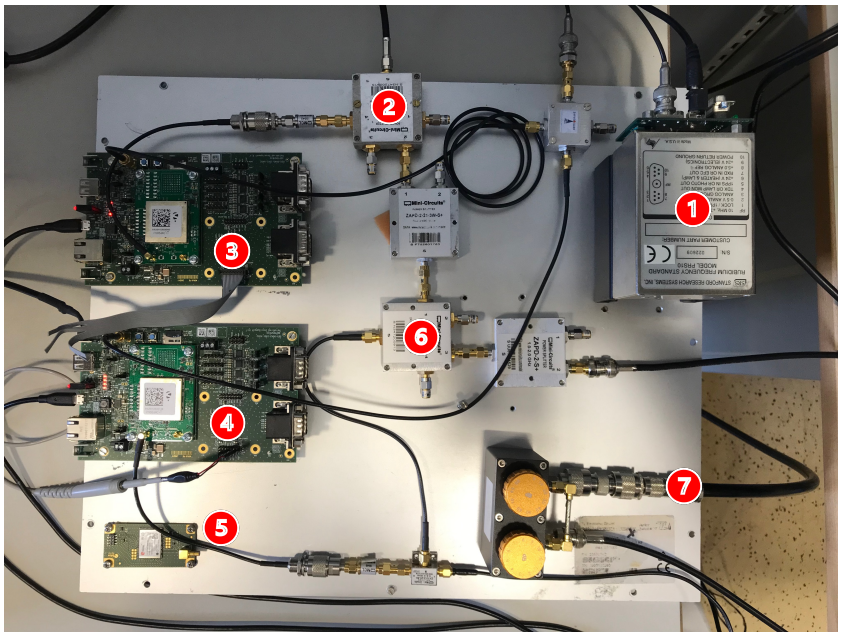
6. The 4 way combiner used to inject the interference signals into the system

7. Interference signal entering the variable attenuator



(a) Test bed schematics

1. Rubidium Atomic Clock
2. 4-Way Passive Power Divider
3. Septentrio Mosaic-T DevKit Not under attack
4. Septentrio Mosaic-T DevKit Under attack
5. U-Blox F9T DevKit Under attack
6. 4-Way splitter
7. Interfering Signal and Attenuator



(b) Laboratory set up

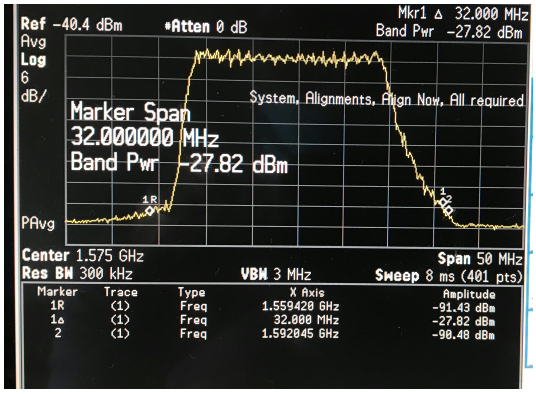
Figure 4.2: Schematics and Lab implementation for the experiments

4.3 Spectrum analyzer Power Measurement Procedure

An Agilent E4402B ESA-E Series spectrum analyzer was utilized to measure the signal power levels of both the legitimate signals, but primarily to characterize the jammer power, meaconing signal power and spoofer signal power. The procedure through which the power of the signal of interest was measured is as follows [49]:

- Hit the Preset button
- Use the average to display the signal
- Select center frequency, span, reference level and input attenuation
- Press Marker, span pair, and set center and span values desired
- Go to Marker, More, Function and choose Band Power as output

The output of this measurement method provides the power levels of the signal analyzed. We can see an example in Figure 4.3. A quite important detail of the measurements is the reference level chosen. Its main function is to allow the visualization of the signal's spectrum to the user, while also if tuned properly provides a higher accuracy in the output value [50].



(a) Spectrum analyzer power measurement of the jammer

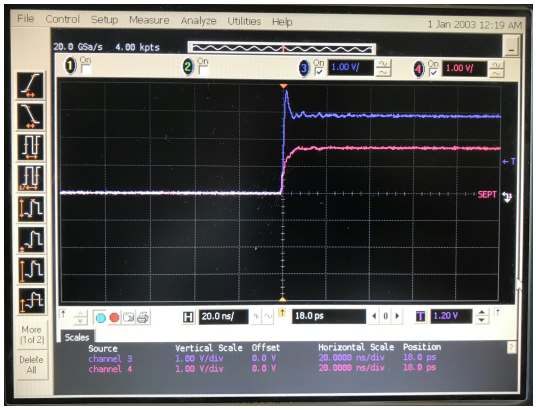
(b) Agilent E4402B ESA-E Series Spectrum Analyzer

Figure 4.3: Detail power measurement and Spectrum Analyzer

4.4 Oscilloscope 1-PPS visualization

The second instrument utilized is an Agilent Infinium 54853A DSO, as seen in Figure 4.4, an oscilloscope that allows us to visualize the 1-PPS output from the receivers. In Figure 4.4 we can see an example of the readings. The difference in

amplitude is given by the use of two different cables that connect the receivers to the oscilloscope.



(a) The two 1-PPS outputs from the state of the art receivers

(b) Agilent Infinium 54853A DS

Figure 4.4: Agilent Infinium 54853A DS and close up view of 1-PPS

4.5 Test Campaign Design

Different test campaigns were designed with the purpose of evaluating the receivers under study, each with a specific goal in mind.

4.5.1 Jamming

Jammer Characterization

In order to understand the levels of power needed to attack the receiver, a characterization of the power output of the jammer is carried out. The jammer used is a adjustable desktop jammer, seen in Figure 4.5, that is capable of jamming different frequencies at once. Each of its outputs refers to one frequency band, for example either L1 or L2 and L5. The jammer power is adjustable by a knob, but this does not allow for accurate power tuning. In order to have full control over the power delivered to the receiver, attenuation was used as a means of controlling the power. Thus at the jammer maximum power was always output while at the variable attenuator the real decision on the power levels was taken. A fixed attenuation of 30 dB was used as a starting point, as the jammer is quite powerful with 100 mW of power at the L1 output, since the intended use involves the transmission of the signal through antennas and not cables. In Figure 4.5 we can see the desktop jammer utilized, with the outputs for L1 and L2 connected via SubMiniature version A (SMA) connectors to a combiner that then feeds the signal to the testbed.

In Figures 4.6 and 4.7 we can see the bandwidth occupied by the jamming signal in red, in the different GNSS frequencies. As we can see in Figure 4.6 the jammer does not cover the GLONASS bandwidth, so during the attacks the receiver is still able to obtain measurements from those satellites. In Figure 4.7 we can see that the bandwidth of the jammer is much larger with respect to that of the L1 frequencies, and is able to cover both GPS' L2 and L5, along with Galileo's E5a and E5b.

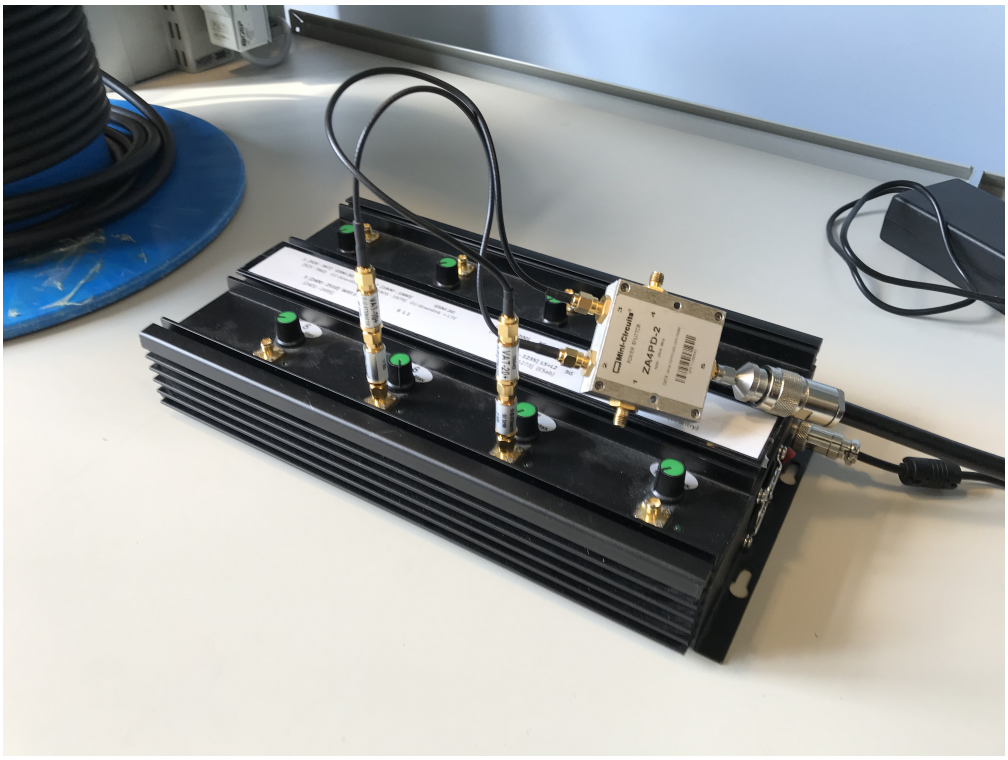


Figure 4.5: Desktop jammer utilized, with L1/E1 and L2/E5 outputs connected

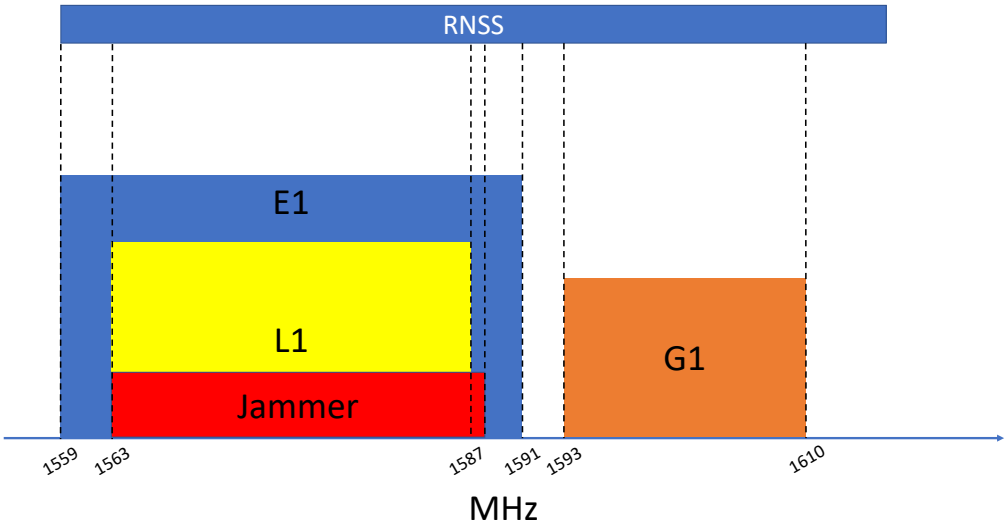


Figure 4.6: Jamming Bandwidth on L1/E1

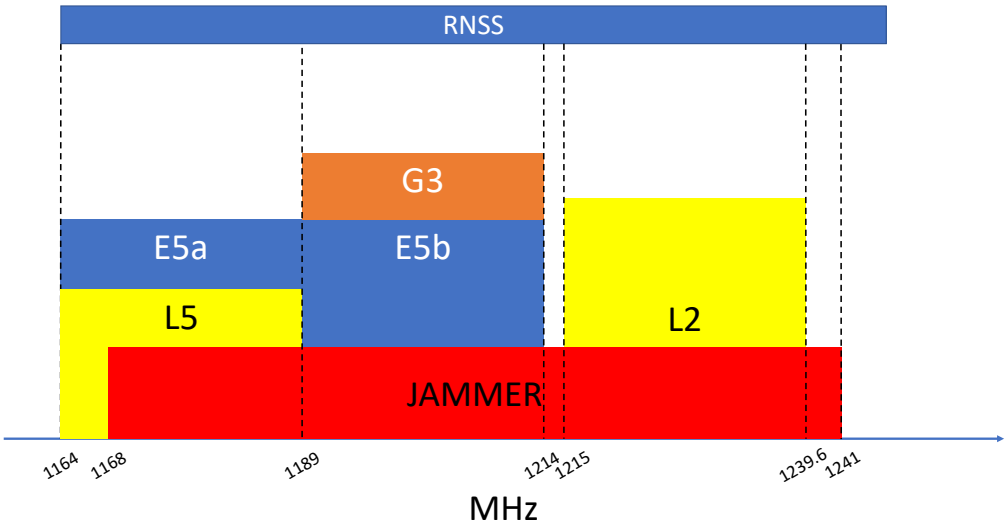


Figure 4.7: Jamming Bandwidth on L2/E5B

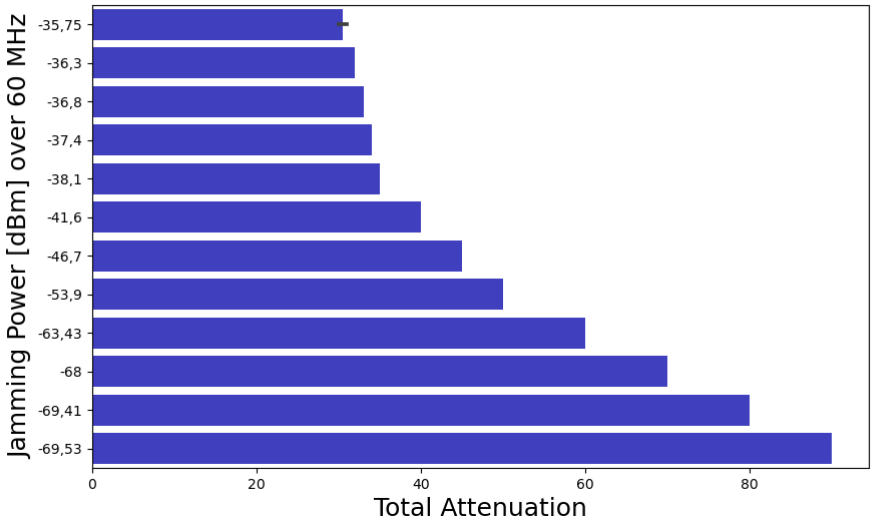


Figure 4.8: Jammer power levels in dBm for different attenuation levels, measured at injection point for the receiver

We can see in Figure 4.8 the different power levels that the jammer reaches for each value of attenuation chosen.

Jamming Procedure

The jamming test procedures are designed to analyze the receiver under different levels of jamming power. Three power levels of the jammer are chosen:

- one that provides negligible levels of interference that the receiver should easily be able to mitigate.
- the second where the jamming intensity is considered challenging by the receiver. This means that the interference is still managed, but legitimate signals result weaker and harder to track.
- the third level of interference should completely deny the receiver's capabilities of operation.
- After this period of denial of service a fourth period where no interference is applied is used to analyze the return to normal operation.

The operations to be performed are the following:

- Start observing variables of interest at T_0
- After 10 min, (T_0+10 min) switch on the jammer to the negligible configuration

- After 10 min, (T_0+20 min) set the variable attenuator to achieve the challenging configuration
- After 10 min, ($T_0 + 30$ min) set the variable attenuator to achieve the denial of service
- After 10 min, ($T_0 + 40$ min) switch off the jammer
- After 10 min, ($T_0 + 50$ min) stop observing effects and collecting measurements

4.5.2 Meaconing

For the meaconing test campaign the steps are similar to those of jamming. We begin by observing the normal operation of the receiver, then it is subject to the meaconing signal. The power level chosen should make the receiver track the delayed signals instead of the legitimate ones. The next step involves turning off the meaconing system and assessing the return to normal operation by the receiver. The objective is to introduce a fixed delay in the generation of the 1-PPS, once the receiver locks on to the delayed GNSS signals. The steps are:

- Start observing variables of interest at T_0
- After 10 min, ($T_0 + 10$ min) set the variable attenuator to achieve the takeover of the delayed signal
- After 10 min, ($T_0 + 20$ min) switch off the system
- After 10 min, ($T_0 + 30$ min) stop observing effects and collecting measurements

The setup utilized to perform the meaconing attacks involved the use of an additional amplifier and cable to introduce the time delay. The amplifier is introduced to compensate for the attenuation of the cable and adaptors used, and to have higher power, necessary to overcome that of the legitimate GNSS signals. In Figure 4.9 we can see the schema for the meaconing experiment, the signal is branched off from the main 4 way passive power splitter, passed through an amplifier, and then introduced to the system using the stepped variable attenuator.

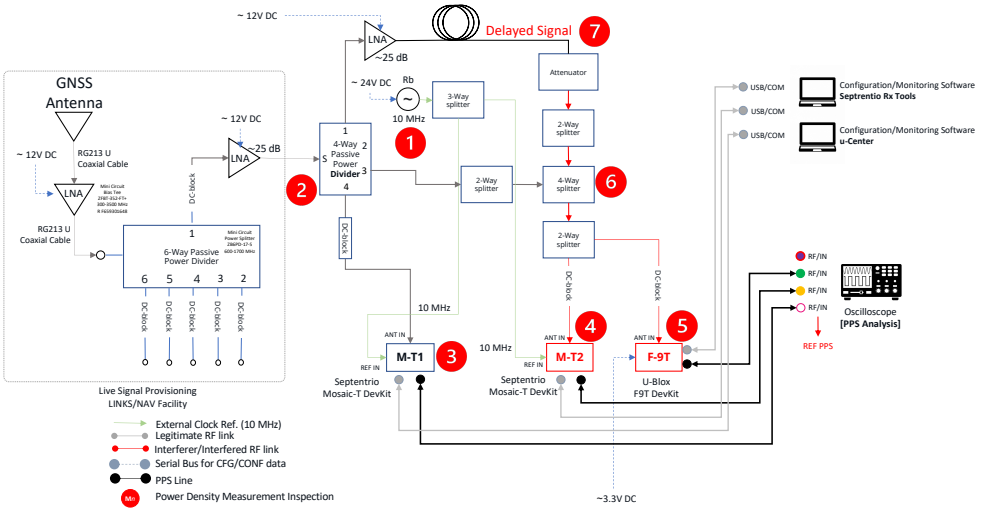


Figure 4.9: Meaconing experiment schema

4.5.3 Spoofing

The last type of attack campaign is the one for spoofing. We can see in Figure 4.10 a simplified model of the spoofing schema and in Figure 4.11 the full setup configuration. A pre-recorded scenario is reproduced through a programmable DAC converter, i.e. USRP N210, seen in Figure 4.15, with a different reference time with respect to the live GNSS signals. The malicious RF signals are combined to multi-frequency, multi-constellation, live GNSS signals to perform a simplistic spoofing attack. The recorded signal is sampled at 5M samples per second with an input gain of 100dB, these values are chosen by iteratively testing. In Figure 4.12 we can see the schema used to record an input signal using Gnuradio and the USRP N210. A USRP source element and file sink are needed, and for ease of use a GUI sink is used to visualize the incoming signal. Gain and sample rate are important variables, and need to be chosen carefully because there are no pre-defined values. The gain is chosen based on the signal power seen at the input of the USRP N210 and though a series of iterations is finely adjusted. The sample rate needs to be chosen based both on Nyquist's theorem and the write speeds to disk of the computer used, which can be a limitation, since overflow can create problems when writing the file. In Figure 4.14 we can see the transmission schema for the USRP N210. A file source to read from is used, along with the USRP Sink element and a GUI sink to visualize the signal. The sample rate in transmission needs to be set equal to that of the recorded file, in order to match. The transmission gain is set using a variable slider element, named QT GUI Range in the schema, in

order to have better control during the spoofing attacks. In Figure 4.16 we can see the transmission schema for the USRP B210, seen in Figure 4.16, that was used to generate continuous wave interference, as two sinusoids, placed near the L1 frequencies, respectively at 1.56 GHz and 1.61 GHz. The schema also allowed to change the carrier frequency of the two sinusoids, using the QT GUI Range element, this time for frequency. The spoofing campaigns are two fold, one type is designed with only spoofing in mind, while the other focuses on a combination of jamming and spoofing to achieve maximum results. Another test involved the use of additional CW Interference close to the L1 band, in an attempt to overwhelm the notch filters used by the mitigation system, using an additional USRP B210, that transmitted either a simple sine wave at a fixed frequency or a pre-recorded interference signal. The spoofing signal is created by recording the original signals using a USRP N210. Through the GnuRadio Companion software it is possible to control the USRP. This type of attack is called Record and Replay, where GNSS signals are recorded, and then replayed at a later date and time, usually with higher power than legitimate GNSS signals, in order to force the receiver to lock on. The danger of these attacks is analyzed in [51]. The spoofing test follows closely the structure of the previous attacks, and is:

- Start observing variables of interest at T_0
- After 10 min, ($T_0 + 10$ min) run signal generation on the spoofer software. Wait for spoofer boot and check RF output led on the USRP N210 to confirm for ongoing RF transmission. In case of a combined spoofing plus jamming attack, also switch on the jammer
- After 10 min, ($T_0 + 20$ min) set the variable attenuator to a level that should provide a higher signal power to the counterfeit signals with respect to the legitimate ones
- After 10 min, ($T_0 + 30$ min) switch off the spoofer and the jammer
- After 10 min, ($T_0 + 40$ min) stop observing effects and collecting measurements.

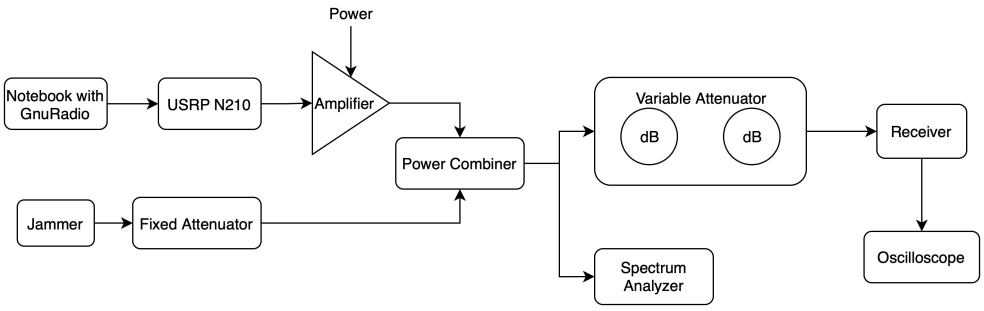


Figure 4.10: Spoofing experiment setup simplified schema

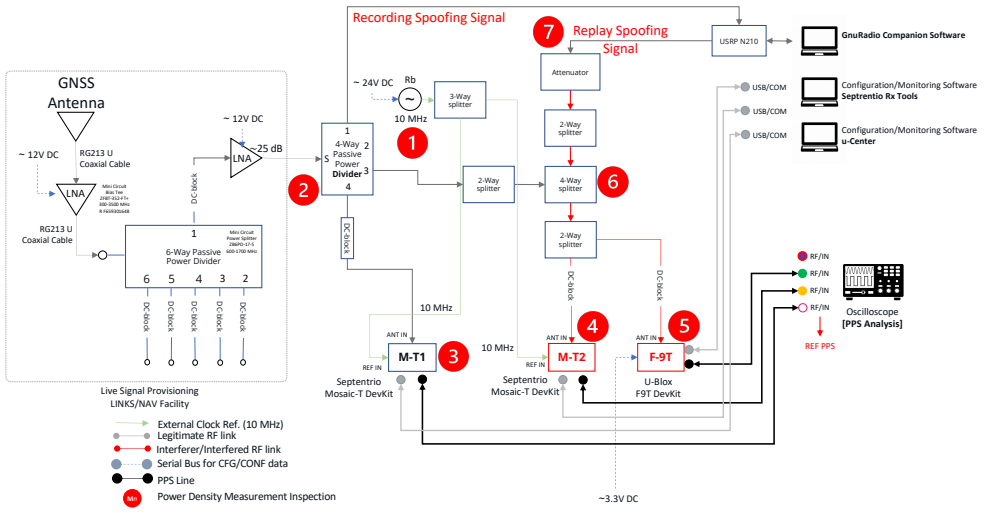


Figure 4.11: Spoofing experiment setup full schema

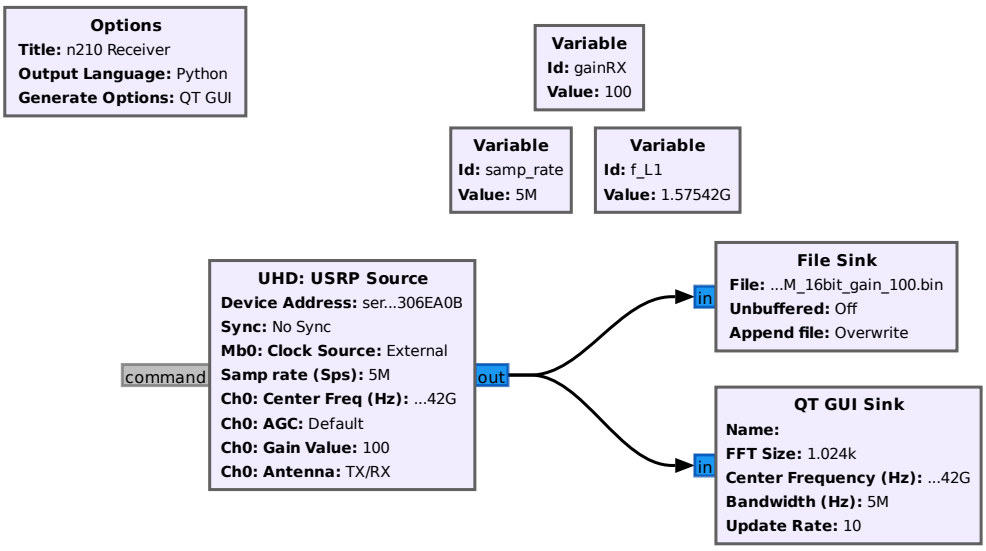


Figure 4.12: GnuRadio USRP N210 Receiver Configuration

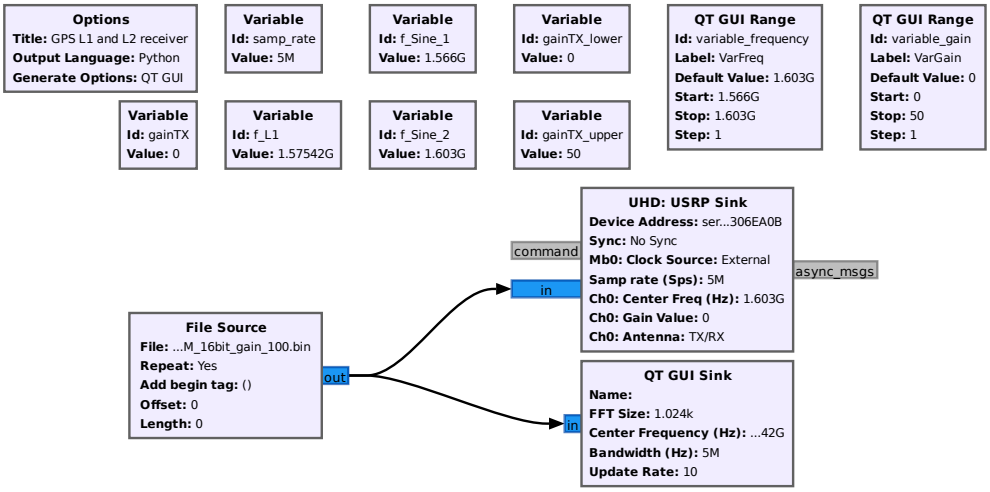


Figure 4.13: GnuRadio USRP N210 Transmitter Configuration

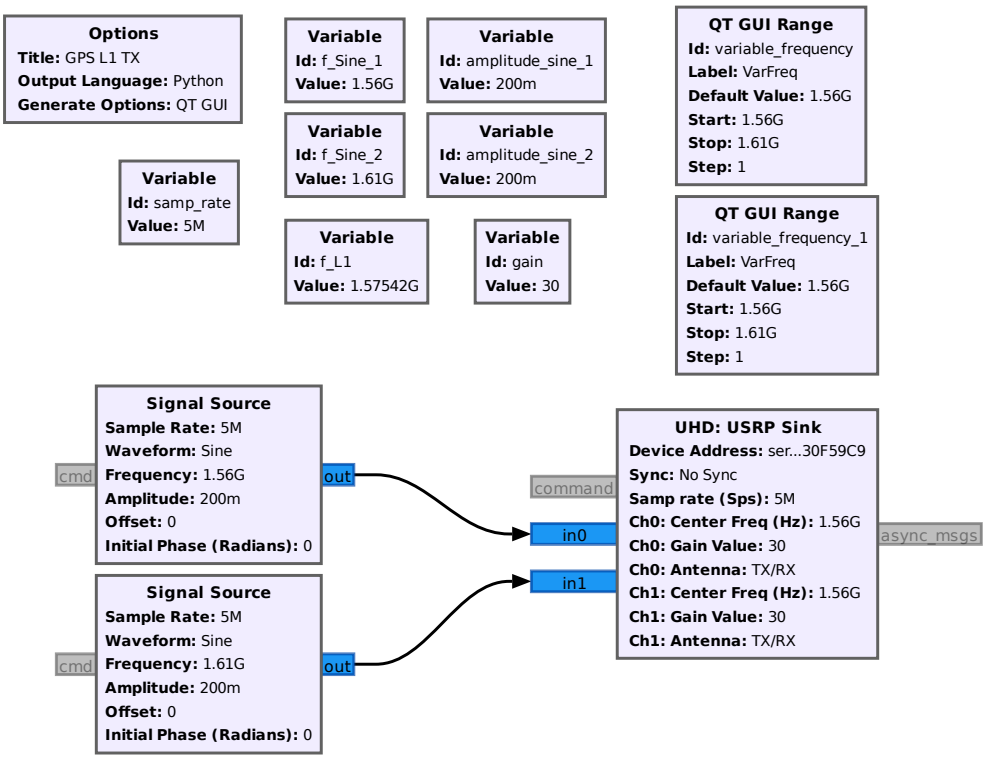


Figure 4.14: GnuRadio USRP B210 Transmitter Configuration

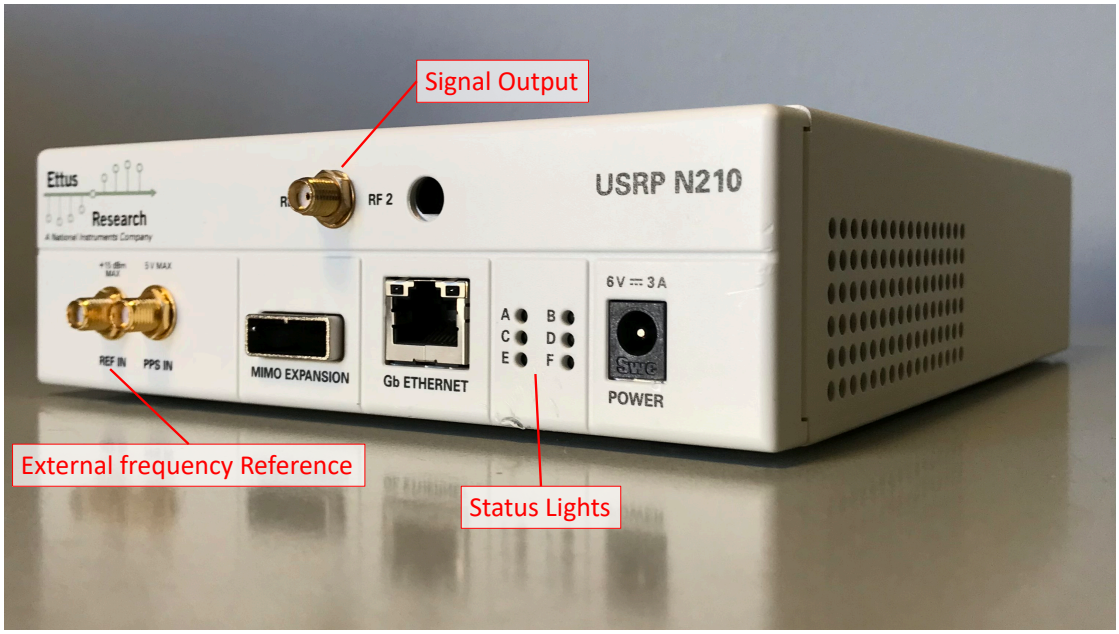


Figure 4.15: Ettus Research USRP N210

Figure 4.16: Ettus Research USRP B210

Chapter 5

Attacks and the Effects on the Receiver

In this chapter we analyze the results of the different attacks. The 1-PPS output is the main concern, but along with this element many other outputs are observed to understand the behaviour of the receiver. Some parameters of interest are the levels of C/N_0, receiver clock bias, satellite visibility and the receiver's own interference detection system.

5.1 Jamming Attack Results

One of the main effects of jamming seen on the receiver is the drop in power of the legitimate signals, due to different factors such as the AGC adjustment, since the noise floor is elevated by the jammer, and the ADC samples being restricted to less bits. In Figure 5.1 we can see for the GPS L1 band, how the satellite signal power decreases as the level of attenuation on the jammer power is lowered. From the data sheet [52], the manufacturer tells us that the minimum threshold for acquisition and tracking are respectively 20 dB-Hz and 33 dB-Hz. This means that during the high intensity jamming period, both acquisition and tracking of GPS L1 signals is not possible since their average is 17.57 dB/Hz as reported in Table 5.1. This does not apply to the previous jamming stages because there are at least four satellites above the 35 dB/Hz threshold as can be seen in Figure 5.1.

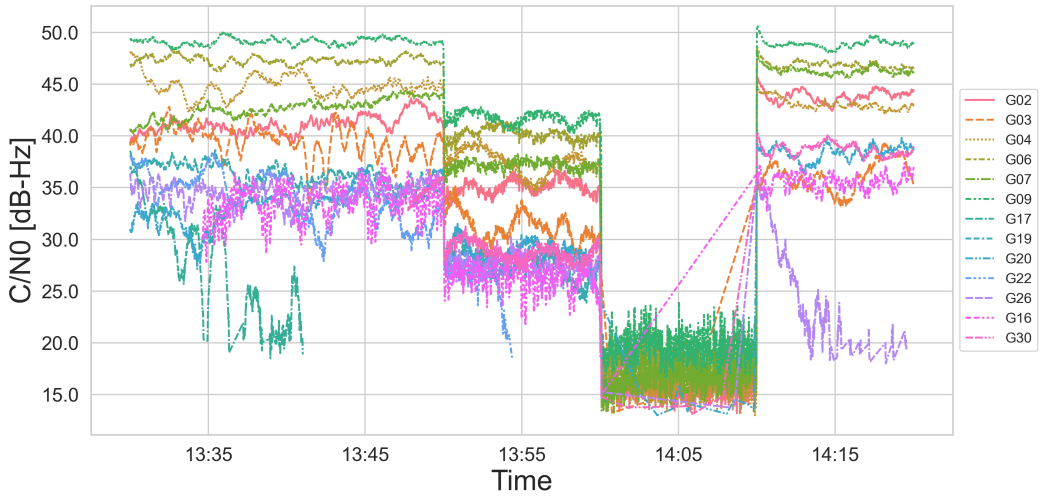


Figure 5.1: C/N_0 Levels of GPS L1 throughout an attack

In Figure 5.2 and in Table 5.1 we can see the average of the signal power and relative percentage drop with respect to nominal levels, the average C/N_0 is calculated over all the available signals for GPS L1, but can be extended to other constellations. The jammer is able to saturate the receiver front end, that stops tracking the satellites. When the receiver is initially configured, a maximum time-out value is chosen for when no signals are available, in order to quit the 1-PPS signal generation. During all jamming attacks, in the high intensity phase, the 1-PPS output was disabled after the time-out period of signal loss.

	Normal	Low	Medium	High
Average C/N_0 [dB/Hz]	40.04	39.39	32.67	17.57
Percentage Drop From Normal	0	-1.63	-18.41	-56.13

Table 5.1: Average C/N_0 per jamming period and relative percentage drop from normal operation

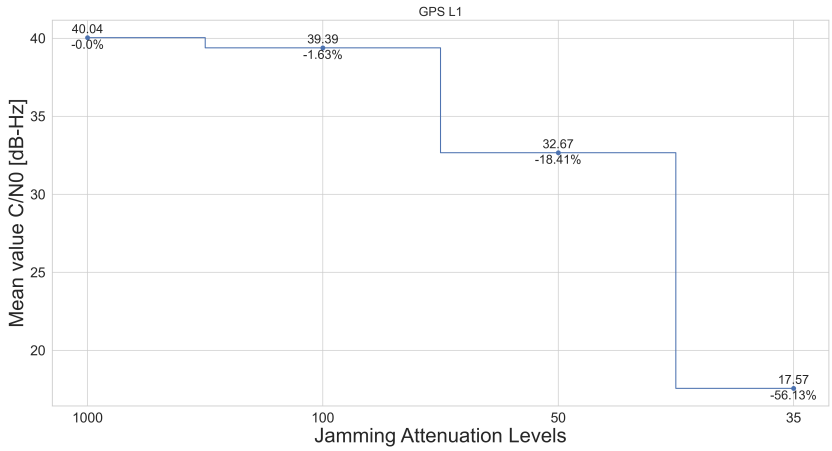
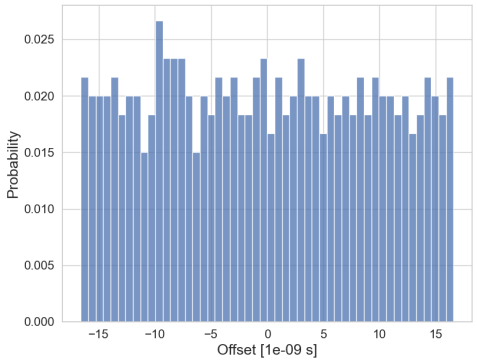
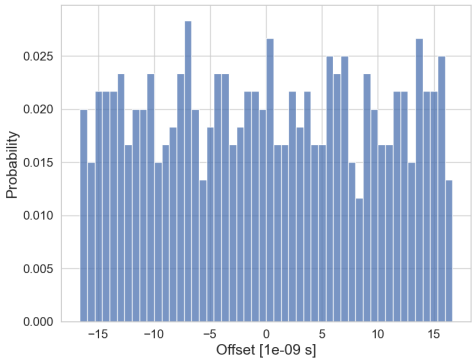


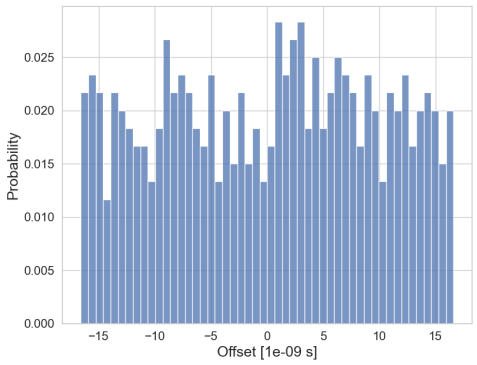
Figure 5.2: Average C/N_0 Levels of GPS L1 throughout an attack and relative percentage drop



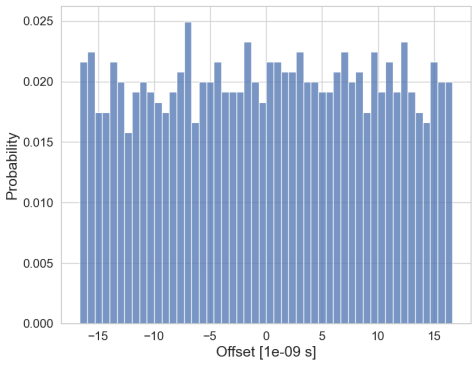
(a) 1-PPS distribution of the reference receiver in low intensity period



(b) 1-PPS probability distribution during the medium intensity jamming



(c) 1-PPS probability distribution during the high intensity jamming



(d) 1-PPS distribution of the reference receiver in the recovery period

Figure 5.3: Comparison between 1-PPS distributions for the two receivers

In Figures 5.3 we can see the 1-PPS distribution during four phases of the attack, in Figure 5.3a we find the distribution during the low intensity jamming, in Figure 5.3b we find the distribution during the intermediate intensity jamming, in 5.3c the distribution during high intensity and finally in Figure 5.3d the distribution for the recovery period. An important aspect is that in Figure 5.3c, the distribution does not represent the entire test time span, because the receiver terminates the 1-PPS generation when all signals are lost. Although the receiver should be able to obtain signals from the GLONASS constellation since the jammer is not able to affect the specific frequency range, but does not because the front end is saturated. As the main interest of the study is the 1-PPS output, we also want to analyze the behaviour of the internal clock that is used to generate it. In Figure 5.4 we can see the receiver clock bias in time, that presents significant jumps when the receiver both enters and exits the intense jamming periods. The effect of jamming on the receiver clock bias also affects the 1-PPS generation, leading to instability. We can see another important aspect in Figure 5.5, that is the estimate of the clock bias variance, that describes the error on the value calculated by the receiver. Under intense jamming the receiver struggles to keep the error estimate low. These effects combined increase the total jitter on the 1-PPS signal. An effort was made to obtain the jitter distribution from the oscilloscope used to monitor the 1-PPS, but software limitations prevented this operation.

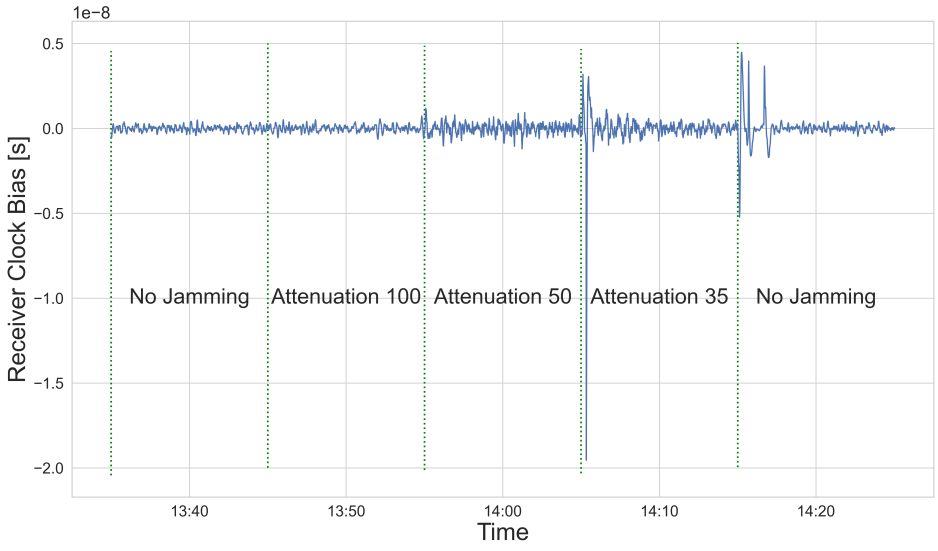


Figure 5.4: Receiver clock bias during the jamming attack

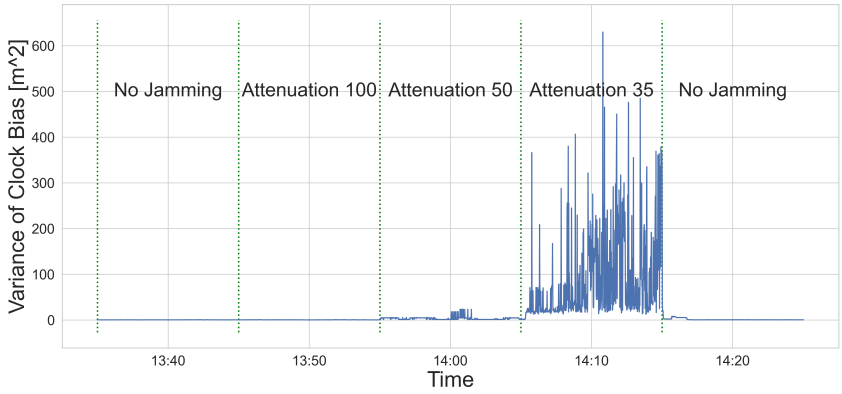


Figure 5.5: Receiver clock bias variance estimation during the jamming attack

5.2 Meaconing Attack Results

Meaconing signals are injected into the system with a higher power with respect to the legitimate GNSS signals. We can see this reflected in Figure 5.6 with the increase of C/N_0 values with respect to the legitimate GNSS signals. Compared to jamming we find an opposite reaction, since jamming introduces noise, while meaconing ideally delays the signals. Meaconing is seen by the receiver as multipath and does not apply any countermeasures, instead it locks on to the delayed signals. In Figure 5.7 we can see the multipath correction that the receiver calculates throughout the test, for satellites from the GPS constellation and L1 frequency. The first notable spike in the error corresponds to the meaconing signals being introduced to the system, with a power that fools the receiver to lock on to them. The second spike instead appears when the meaconing signals are removed. We can see a notable shift in the multipath error correction even after the interference is removed, that in average is 1.93 meters, with respect to the normal operation being 0.035 meters average. During the meaconing period the multipath correction reaches an average of -7.01 meters.

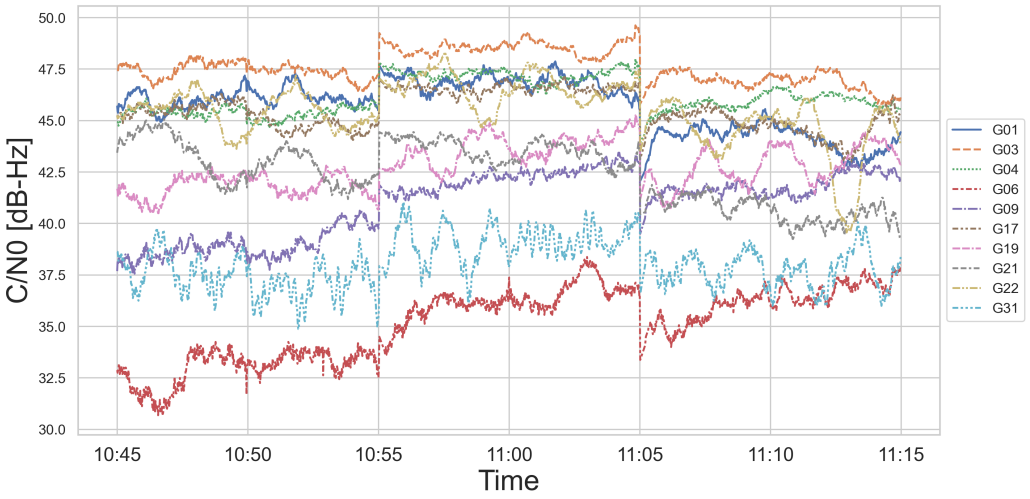


Figure 5.6: C/N_0 values of GPS L1 signals during a meaconing attack

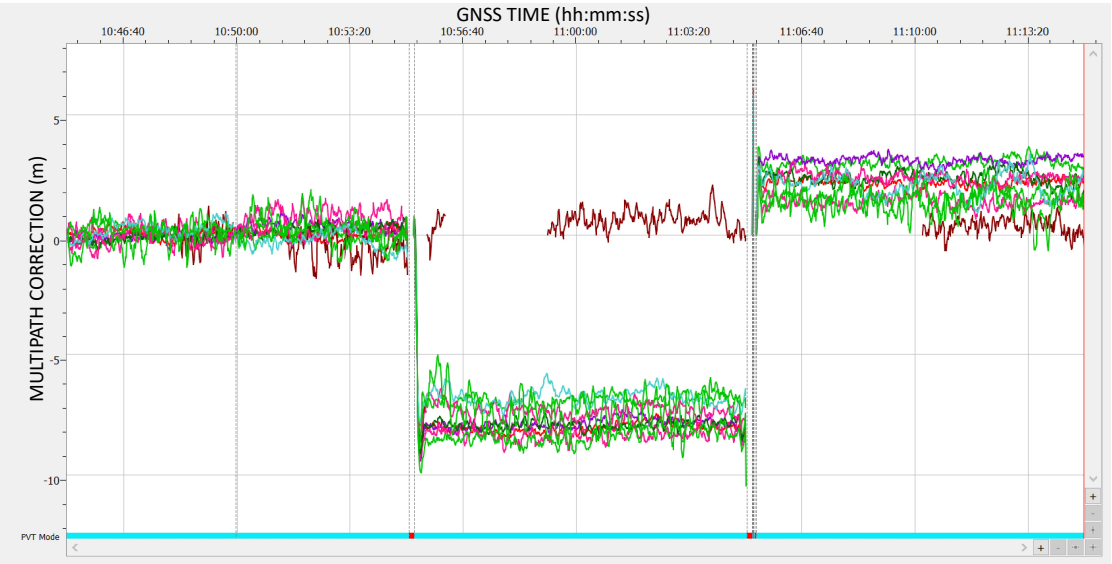


Figure 5.7: Multipath correction calculated by the receiver during the attack

We can observe the most notable failure of the receiver in Figure 5.8, where the clock bias follows the delayed signals during the full meaconing period, providing an erroneous synchronization source for the 1-PPS generation. The fact that the receiver clock bias is kept to zero with the delayed signals means that, in

combination with clock steering, both the PRN generators and the pulse generator, in charge of creating the 1-PPS, are misaligned with respect to the legitimate system time. As before we see two main spikes that correspond to the introduction and removal of the interfering signals.

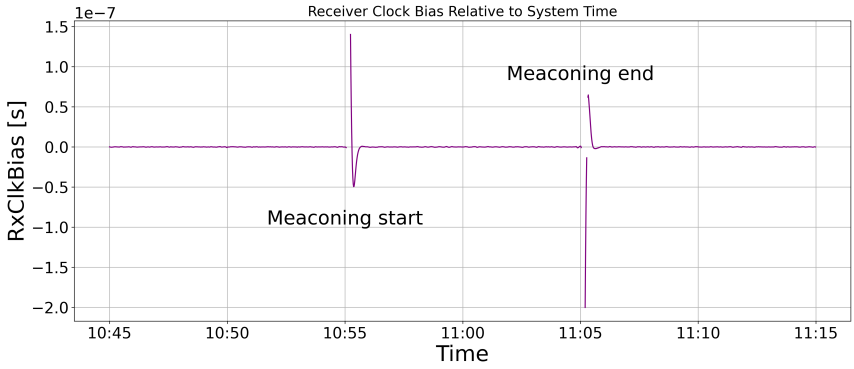


Figure 5.8: Receiver clock bias during the meaconing attack

In Figure 5.9 we can see, using the oscilloscope, the effect that meaconing has on the receiver. It introduces a delay of 200 ± 30 ns, that violates the requirements of phase synchronization chosen of 65 to 130 ns.

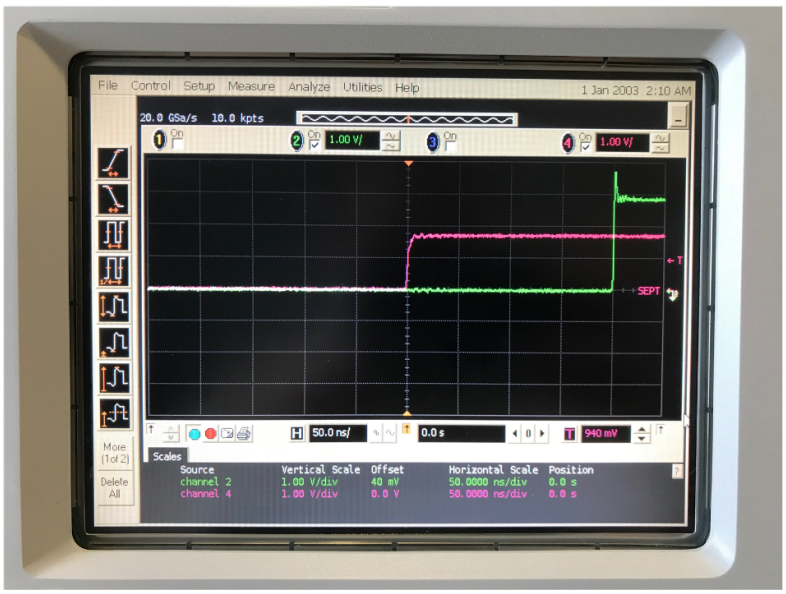


Figure 5.9: 1-PPS shift of the receiver under attack with respect to the reference receiver, seen through the oscilloscope

5.3 Simplistic Spoofing Attack Results

We found that if the receiver is already tracking the legitimate signals, any attempt of having the receiver lock on to the recorded signals failed, and was detected by the interference mitigation algorithms. If the power of the incoming spoofing signals exceeded a threshold, usually having twice the power of the legitimate signals, then the receiver classified it as interference and completely stopped any operation on the band under attack. The receiver can automatically place three notch filters as part of its interference mitigation capabilities, and any attempt at saturating them through additional interference resulted futile, as other systems still were able to identify the spoofing signals and allow the receiver to ignore them. In Figure 5.10 we can see the spectrum of the receiver under attack and notice how the center frequency of 1575.42 MHz has a notch filter applied, since the receiver identifies the incoming spoofed signal as interference.

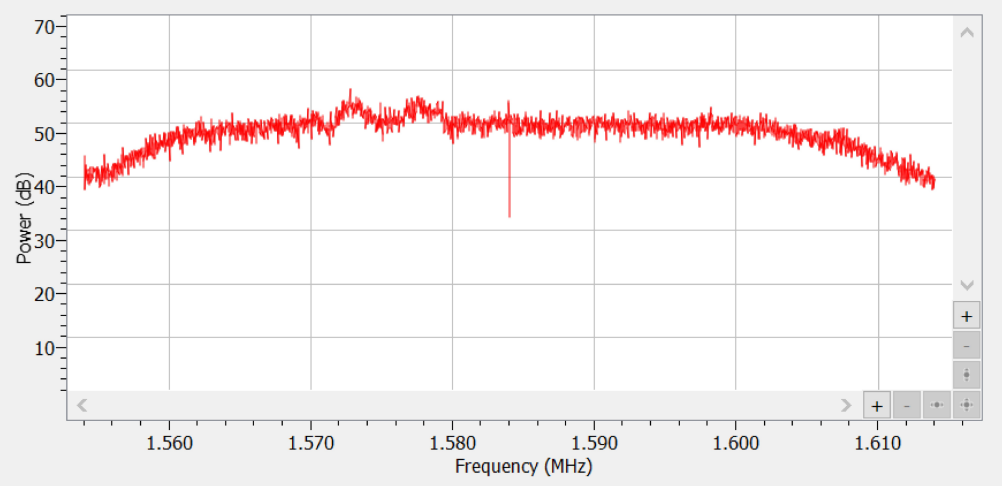


Figure 5.10: Spectrum of the receiver under a spoofing attack

When the power of the spoofing signal is increased, and an additional interference source is used we can observe a behaviour as seen in Figure 5.11. The high power makes the notch filter less effective, but the receiver still classifies the signals as interference.

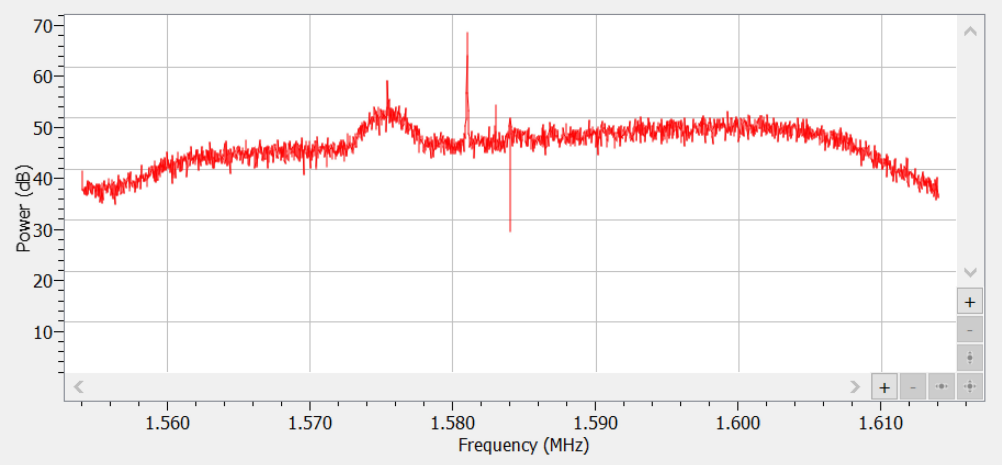


Figure 5.11: Spectrum with both high power spoofing signal and additional CW interference

In Figure 5.12 we can see how the receiver reacts when the spoofing signals are removed from the system. Since they are interpreted as interference by the receiver, when removed the legitimate GNSS signals receive a jump in C/N_0 value. This can be attributed to the adjustment of the AGC levels and the ADC returning to using the full bit range instead of a reduced one.

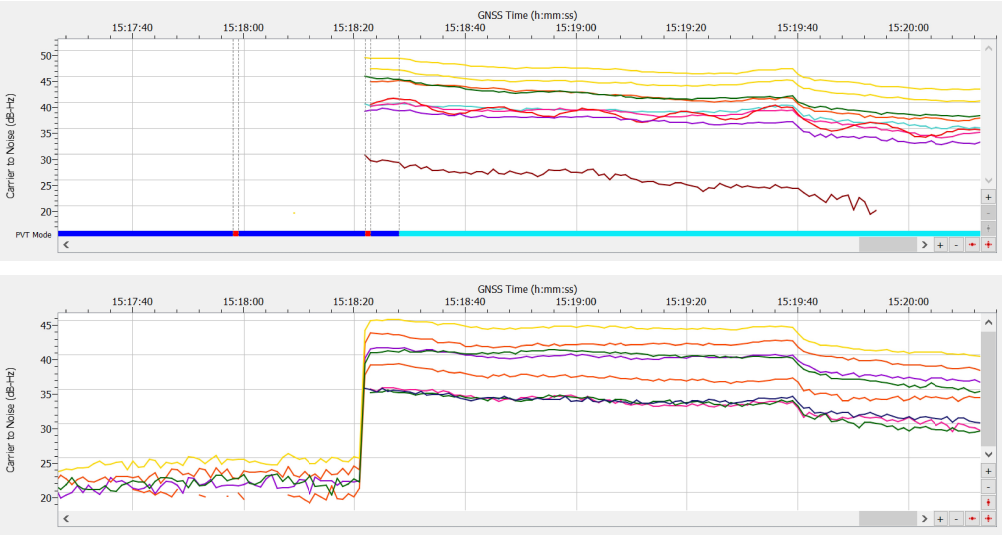


Figure 5.12: Removal of spoofing signal from the system and return to nominal operation

Chapter 6

Conclusions

GNSS is proposed as a tool to aid time synchronization for telecommunication networks, since each constellation can be seen as a synchronized clock in the sky. The 1-Pulse Per Second (1-PPS) signal generated by GNSS receivers would be adopted for its properties of low jitter and long term stability. Using GNSS to synchronize nodes of a network exposes it to possible attacks, being either radio frequency or cyber. The work of this thesis focused on the former of the two. Different types of attacks are explored that range in complexity and cost. The simplest and cheapest to perform by a member of the public is jamming, since jammers are easily acquirable on the internet at low cost, and no knowledge is required to operate them. Both meaconing and spoofing would require a user with the knowledge and the means necessary to efficiently and effectively carry out such attacks. In the experiments of this thesis, the cost of meaconing includes an RF receiver antenna, cable, amplifier and transmitter antenna. For a more complex meaconing attack, a software defined radio along with a portable computer would be necessary, along with the knowledge of operating such tools. As already stated, Spoofing attacks are the most complex, but also the most costly, as they involve the use of software defined radios, such as the USRP N210, and capable computer. To analyze these potential threats throughout this thesis a hardware testbed is designed, keeping in mind that all attacks must be done using cables and not wireless RF transmissions, as these would be illegal if done in the open. The testbed aimed to analyze the performance of a receiver under different attacks and compare it to that of one in its nominal state. Problems occurred where the jamming signal would reach the non-target receiver, and adjustments had to be made by introducing additional attenuation. With the purpose of evaluating the performance of the multi-band and multi-frequency receiver under different levels and conditions of attack, test procedures are designed with careful consideration. Different periods with varying intensity are proposed to efficiently analyze attacks

in time, and outputs from the receiver are analyzed both in real time and post-processed. The main objective of the test procedures is to find vulnerabilities in the GNSS receiver that would badly affect the generation of the 1-PPS. Considering that the 1-PPS is generated using the receiver's internal clock, any attack that modifies the behaviour of the time keeping of the receiver is a possible vulnerability. Of fundamental importance is the receiver clock bias, which is the difference in time between the local clock of the receiver and the GNSS system time. This element is used to steer the local oscillator and correct any drifts. If the receiver clock bias is compromised then also the 1-PPS generation loop undergoes negative effects. The effects observed on the receiver highlight the importance of the test procedure design. For jamming attacks, when a single frequency band is attacked the receiver is able to mitigate low intensity signals, but when higher power is used the band is completely obscured by noise, but the receiver is still able to utilize the other frequency bands and continues to output the 1-PPS without problems. When multi frequency jamming is adopted, at low power values the receiver is able to mitigate the interference and normally operate, but this changes when high power is introduced. Both L1/E1 and L5/E5 bands are subject to jamming and the receiver is completely saturated and the 1-PPS output is terminated after the pre-defined time period. Meaconing proved to be a very insidious attack, as the receiver mistakes the delayed signals as multipath. No interference mitigation is applied and the receiver clock bias is altered resulting in a dangerous shift of 200 ± 30 ns in the generation of the 1-PPS, violating the system requirements of phase synchronization. As the objective of the attacks it to disrupt the synchronization of one or more nodes of a telecom network, meaconing proved to be very effective in doing so. Considering that the receiver is static and possibly easy to approach, a malicious user could attack different nodes by placing meaconing "devices" near by. Since the receiver interprets the meaconing attack as multipath, this could be used as a mitigation strategy. As shown in chapter 5, the multipath corrections applied by the receiver jump from an average close to zero to an average of -7.01 meters, these sudden jumps could be used as flags to alert the operators of a possible attack on the receiver and switch the node to backup synchronization options. Simplistic spoofing attacks were not successful, as the receiver either interpreted the signals as interference or detected the spoofing and applied its mitigation strategies. The 1-PPS is not affected by the attacks and is continuously generated throughout the test procedure. Possibly more intricate attacks such as "Intermediate Attack via Portable Receiver-Spoofer" and "Sophisticated Attack via Multiple Phase-locked Portable Receiver-Spoofers" as proposed in [43], could circumvent the problems encountered with a simplistic approach, but attacks like these require advanced experience and hardware to be carried out.

Bibliography

[1] European Commission. *Smart Cities*. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en. Aug. 2021 (cit. on p. 1).

[2] CISA. *Time – The Invisible Utility*. https://us-cert.cisa.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf. Mar. 2019 (cit. on p. 1).

[3] Marco Pini and Alex Minetto et al. «Satellite-derived Time for Enhanced Telecom Networks Synchronization: the ROOT Project». In: *2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*. 2021. DOI: 10.1109/METROAEROSPACE51421.2021.9511780 (cit. on pp. 2–4, 32).

[4] GSMA. *5G TDD Synchronisation*. https://www.gsma.com/spectrum/resources/3-5-ghz-5g-tdd-synchronisation/. Apr. 2020 (cit. on p. 2).

[5] Wise Repeater. *4G LTE Bands and Frequencies*. https://www.wiserepeater.com/supports/4g-lte-bands-and-frequencies-tdd-fdd-lte/. Jan. 2017 (cit. on p. 2).

[6] Ericcson. *5G synchronization requirements and solutions*. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-synchronization-requirements-and-solutions. Jan. 2021 (cit. on p. 2).

[7] Han Li, Liuyan Han, Ran Duan, and Geoffrey M. Garner. «Analysis of the Synchronization Requirements of 5g and Corresponding Solutions». In: *Proc. IEEE IEEE Communications Standards Magazine*. Mar. 2017, pp. 52–58 (cit. on p. 2).

[8] J. Serrano M. Lipiński T. Włostowski and P. Alvarez. «White rabbit: a PTP application for robust sub-nanosecond synchronization». In: *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*. 2011, pp. 25–30. DOI: 10.1109/ISPCS.2011.6070148 (cit. on pp. 4, 5).

[9] Maciej Lipinski. *White Rabbit Switch*. https://ohwr.org/projects/white-rabbit/wiki/switch. Feb. 2021 (cit. on p. 4).

[10] Navigation National Coordination Office for Space-Based Positioning and Timing. *Space Segment*. https://www.gps.gov/systems/gps/space/. July 2021 (cit. on p. 6).

[11] *Galileo architecture*. 2021. URL: https://gssc.esa.int/navipedia/index.php/Galileo_Architecture (cit. on p. 6).

[12] *GLONASS architecture*. 2021. URL: https://gssc.esa.int/navipedia/index.php/GLONASS_Space_Segment (cit. on p. 6).

[13] Elliott D. Kaplan and Christopher J. Hegarty. *Understanding GPS Principles and Applications*. 685 Canton Street Norwood, MA 02062: ARTECH HOUSE, 1996 (cit. on pp. 6, 7, 9, 10).

[14] Stephen Muenstermann. *Interference and Security Considerations for Wireless Communications in an Industrial Environment*. 2021. URL: https://www.controlglobal.com/assets/Media/MediaManager/wp_06_033_honeywell_wireless.pdf (cit. on p. 7).

[15] Michael A. Lombardi. «The Use of GPS Disciplined Oscillators as Primary Frequency Standards for Calibration and Metrology Laboratories». In: *NCSLI Measure* 3.3 (Sept. 2008), pp. 56–65. ISSN: 1931-5775, 2381-0580. DOI: 10.1080/19315775.2008.11721437 (cit. on p. 7).

[16] *GNSS Signal*. https://gssc.esa.int/navipedia/index.php/GNSS_signal (cit. on p. 8).

[17] *GLONASS Signal Plan*. (cit. on p. 8).

[18] Apr. 2018. URL: https://gisgeography.com/trilateration-triangulation-gps/ (cit. on p. 9).

[19] Tushna Commissariat. *Atomic clock is smallest on the market*. https://physicsworld.com/a/atomic-clock-is-smallest-on-the-market/. May 2021 (cit. on p. 9).

[20] Tomislav Kos, Ivan Markezic, and Josip Pokrajcic. «Effects of multipath reception on GPS positioning performance». In: *Proceedings ELMAR-2010*. 2010, pp. 399–402 (cit. on p. 10).

[21] Navigation National Coordination Office for Space-Based Positioning and Timing. *Space Segment*. https://www.gps.gov/systems/gps/space. July 2021 (cit. on p. 11).

[22] GISGeography. *GPS Accuracy: HDOP, PDOP, GDOP, Multipath the Atmosphere*. Mar. 2017. URL: https://gisgeography.com/gps-accuracy-hdop-pdop-gdop-multipath/ (cit. on p. 15).

[23] Richard B Langley. *Time, CLocks, and GPS*. GPS World. Dec. 1991 (cit. on pp. 15, 17).

[24] Tavella P. and Petit G. *Precise time scales and navigation systems: mutual benefits of timekeeping and positioning.* Satell Navig 1. Oct. 2020 (cit. on p. 16).

[25] MGB Tech. *About the PPS Pulse*. http://pos.mgb-tech.com/insightpps/. Aug. 2021 (cit. on p. 17).

[26] L. Gasparini, O. Zadedyurina, G. Fontana, D. Macii, A. Boni, and Y. Ofek. «A Digital Circuit for Jitter Reduction of GPS-disciplined 1-pps Synchronization Signals». In: *2007 IEEE International Workshop on Advanced Methods for Uncertainty Estimation in Measurement*. 2007, pp. 84–88. DOI: 10.1109/AMUEM.2007.4362576 (cit. on p. 17).

[27] Vectron. *Jitter in Clock Sources*. https://www.vectron.com/products/literature_library/jitter_in_clock_sources.pdf. "" (Cit. on p. 17).

[28] X. Niu, K. Yan, and T. et al. Zhang. «Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers.» In: *GPS Solut* 19.19 (2015), pp. 141–150 (cit. on p. 18).

[29] *mosaic-T Reference Guide*. Septentrio. 2020 (cit. on pp. 18, 19).

[30] Orgiazzi. *PPS GPS Timing* (cit. on p. 20).

[31] *Radio Interference*. 2021. URL: https://www.itu.int/en/mediacentre/backgrounders/Pages/radio-interference.aspx (cit. on p. 28).

[32] Fabio Dovis, ed. *GNSS Interference Threats And Countermeasures*. 685 Canton Street Norwood, MA 02062: Artech House, 2015 (cit. on pp. 28, 30–33, 37–41).

[33] Charles Arthur and technology editor technology. *Thousands using GPS jammers on UK roads pose risks, say experts*. Feb. 2013. URL: https://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks (cit. on p. 28).

[34] Oksana Bedratenko. *Ben Gurion Incident Exposes West's Vulnerability to GPS Disruption*. URL: %5Curl%7Bhttps://www.voanews.com/a/silicon-valley-technology_ben-gurion-incident-exposes-wests-vulnerability-gps-disruption/6171113.html%7D (cit. on p. 29).

[35] Kyle Mizokami. *Russia Is Disrupting GPS Signals and It's Spilling into Israel*. July 2019. URL: https://www.popularmechanics.com/military/weapons/a28250133/russia-gps-signals-israel/ (cit. on p. 29).

[36] C4ADS. *Above Us Only Stars*. URL: https://www.c4reports.org/aboveusonlystars (cit. on p. 29).

[37] Oct. 2017. URL: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/ (cit. on p. 29).

[38] Glenn Witcher. *Electronic warfare systems "Pole-21" in the Russian army.* URL: https://en.topwar.ru/182196-kompleksy-rjeb-pole-21-v-rossijskoj-armii.html (cit. on p. 29).

[39] URL: https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense (cit. on p. 29).

[40] URL: https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/ (cit. on p. 29).

[41] Daniele Borio, Fabio Dovis, Heidi Kuusniemi, and Letizia Lo Presti. «Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers». In: *Proceedings of the IEEE* 104.6 (June 2016), pp. 1233–1245. ISSN: 0018-9219, 1558-2256. DOI: 10.1109/JPROC.2016.2543266 (cit. on p. 33).

[42] Daniel Marnach, Sjouke Mauw, Miguel Martins, and Carlo Harpes. «Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers». In: *Artificial Satellites* 48.2 (Jan. 2013). ISSN: 2083-6104, 0208-841X. DOI: 10.2478/arsa-2013-0006. URL: https://content.sciendo.com/doi/10.2478/arsa-2013-0006 (cit. on p. 34).

[43] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner Jr. *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.* 2008 ION GNSS Conference Savanna, GA. Sept. 2008 (cit. on pp. 34, 66).

[44] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. «GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques». In: *International Journal of Navigation and Observation* 2012 (July 2012), pp. 1–16. ISSN: 1687-5990, 1687-6008. DOI: 10.1155/2012/127072 (cit. on pp. 35, 36).

[45] Frédéric Bastide, Dennis Akos, Christophe Macabiau, and Benoit Roturier. «Automatic gain control (AGC) as an interference assessment tool». In: (2003), p. 13 (cit. on p. 38).

[46] Andreas Bauch and Peter Whibberley. «Reliable Time from GNSS Signals». In: (2017), p. 7 (cit. on p. 42).

[47] Patrizia Tavella and Gérard Petit. «Precise time scales and navigation systems: mutual benefits of timekeeping and positioning». In: *Satellite Navigation* 1.1 (Dec. 2020), p. 10. ISSN: 2662-1363. DOI: 10.1186/s43020-020-00012-0 (cit. on p. 42).

[48] Emanuela Falletti, Davide Margaria, Gianluca Marucco, Beatrice Motella, Mario Nicola, and Marco Pini. «Synchronization of Critical Infrastructures Dependent Upon GNSS: Current Vulnerabilities and Protection Provided by New Signals». In: *IEEE Systems Journal* 13.3 (Sept. 2019), pp. 2118–2129. ISSN: 1932-8184, 1937-9234, 2373-7816. DOI: 10.1109/JSYST.2018.2883752 (cit. on p. 42).

[49] Agilent Technologies. *Measurement Guide and Programming Examples*. English. Agilent Technologies. 346 pp. (cit. on p. 45).

[50] Agilent Technologies. *Optimizing Spectrum Analyzer Amplitude Accuracy*. English. 16 pp. (cit. on p. 45).

[51] Panagiotis Papadimitratos and Aleksandar Jovanovic. «Protection and fundamental vulnerability of GNSS». In: *2008 IEEE International Workshop on Satellite and Space Communications*. IEEE, Oct. 2008, pp. 167–171. ISBN: 978-1-4244-1947-0. DOI: 10.1109/IWSSC.2008.4656777. URL: http://ieeexplore.ieee.org/document/4656777/ (cit. on p. 52).

[52] URL: https://www.septentrio.com/en/products/gnss-receivers/rover-base-receivers/receivers-modules/mosaic-t (cit. on p. 56).