Master's Thesis

Master in telecommunication engineering

Analysis of GNSS replay-attack detectors exploiting unpredictable symbols

Rubén Morales Ferré

Thesis Advisor: Gonzalo Seco Granados

Department of Telecommunications and Systems Engineering

Universitat Autònoma de Barcelona

Bellaterra, February 2018

UAB

El sotasignant, *Gonzalo Seco Granados*, Professor de l'Escola Tècnica Superior d'Enginyeria (ETSE) de la Universitat Autònoma de Barcelona (UAB),

CERTIFICA:

Que el projecte presentat en aquesta memòria de Treball Final de Màster ha estat realitzat sota la seva direcció per l'alumne *Rubén Morales Ferré*.

I, perquè consti a tots els efectes, signa el present certificat.

Bellaterra, *07-02-2018*.

Signatura: Gonzalo Seco Granados

Summary:

Since its inception, GNSS (Global Navigation Satellite System) have become more popular year after year. GNSS is currently used in a wide variety of applications beyond the determination of the user position by means of a GNSS receiver. GNSS is used in sectors as different as finance, energy distribution or telecommunications. Due to this increase in popularity in the last years, GNSS has become objective of attacks, with the purpose of control the victim receiver and provide an erroneous PVT (Position, Time and Velocity) solution. In first place, in this document are described the basic concepts of GNSS, this means describe the elements that composes GNSS and how the PVT solution is determined by the receiver. Once are shown the basic concepts of GNSS, the attacks are presented. The state-of-the-art of the attacks against GNSS is described, with the objective of showing the wide variety of possibilities there are available. Next are explained in detail the SCER (Security Code Estimation and Replay) attacks based on the estimation of the impracticable bits. For this attack, are proposed three different strategies, two of them based on modifying the signal at chip level and a third one based on the modification of the bit amplitude, and four detection methods. Once there has been explained in detail in what consist each of them, a comparison of the different attacks and detection methods are carried out in order to determine which attack is the best (from the point of view of the attacker) and which detection method is more effective against each attack strategy.

Resum:
Des dels seus inicis, els sistemes de posicionament global per satèl·lit, o del anglès GNSS (Global Navigation Satellite System), han guanyat popularitat any rere any. Actualment, aquests sistemes són emprats en un gran número d'aplicacions, més enllà de determinar la posició del usuari mitjançant un receptor de GNSS. Actualment GNSS es utilitzat en sectors molt diversos com podrien ser les finances, la distribució d'energia o les telecomunicacions. Degut a aquest augment en popularitat en els darrer anys, els sistemes GNSS s'han convertit en objectiu d'atacs, amb la fi de controlar el receptor de la víctima i així proporcionar una solució PVT (Posició, Velocitat i Temps) errònia. En primer lloc, en aquest document es descriuen els conceptes bàsics dels sistemes GNSS, és a dir, quins elements els componen i com es determina la solució PVT en el receptor. Una vegada mostrades les bases dels sistemes GNSS, s'introdueixen els atacs. La descripció dels atacs comença amb un resum de l'estat de l'art dels tipus d'atacs contra els sistemes GNSS, amb l'objectiu de mostrar la gran varietat de possibilitats que n'hi han. Seguidament, es detallen els atacs de tipus SCER (del anglès Security Code Estimation and Replay) basats en l'estimació dels bits impredictibles. Per aquest tipus d'atacs es proposen tres estratègies d'atac, dues de les quals basades en la modificació del senyal a nivell de chip i una tercera basada en modificar l'amplitud del bit, i quatre mètodes de detecció. Una vegada detallat en que consisteixen cadascuna de les estratègies i els mètodes de detecció, es realitza una comparació amb l'objectiu de determinar quin atac és millor (des del punt de vista del atacant) i quin mètode de de detecció és més efectiu contra cadascuna de les estratègies d'atac.

Resumen:
Desde sus inicios, los sistemas de posicionamiento global por satélite, o del inglés GNSS (Global Navigation Satellite System), han ido ganando popularidad año tras año. En la actualidad, estos sistemas son usados en un gran número de aplicaciones, mas allá de solamente determinar la posición del usuario mediante un receptor de GNSS. Actualmente GNSS es usado en sectores tan diversos como las finanzas, la distribución de energía o las telecomunicaciones. Debido a este aumento en popularidad en los últimos años, los sistemas GNSS se han convertido en objetivo de ataques, con el fin de tomar el control del receptor de la víctima y así proporcionar una solución PVT (Posición, Velocidad y Tiempo) errónea. En primer lugar, en este documento se describen los conceptos básicos de los sistemas GNSS, es decir, que los componen y como se determina la solución PVT en el receptor. Tras conocer las bases de funcionamiento de los sistemas GNSS, se introducen los ataques. En un primer momento se describe el estado del arte de los ataques contra los sistemas GNSS, con el objetivo de mostrar la gran variedad de ataques que se pueden llevar a cabo. Tras esto, se detallan los ataques de tipo SCER (del ingles Security Code Estimation and Replay) basados en la estimación de los bits impredecibles. Para este tipo de ataques se proponen tres estrategias de ataque, dos de las cuales basadas en la modificación de la señal a nivel de chip y una tercera basada en la modificación de la amplitud del bit, y cuatro métodos de detección. Tras detallar en que consiste cada una de las estrategias y los métodos de detección, se realiza una comparación con el objetivo de determinar que ataque es mejor (desde el punto de vista del atacante) y que método de detección es mas efectivo contra cada uno de las estrategias de ataque.

Acknowledgement

This Master's dissertation puts an end to the period of my life as UAB student. In turn, it is the starting point of my closest future, the PhD. This year and a half has been the best period of my life since I started the university. This project is the cherry-on-top of this period, which I have really enjoyed because I have been doing what I liked the most.

In first place, I would like to thank my supervisor Prof. Gonzalo Seco Granados. Since I really met him during the BSc's thesis, he has not done another thing than help me when I needed him the most. I would like to thank his countless suggestions and corrections, as well as his support and guidance through both BSc's and MSc's thesis. I would also like to thank his help to get the opportunity to pursue a PhD.

In second place, I would like also to thank the colleagues of the SPCOMNAV group of the Department of Telecommunications at UAB; Vicente, Dani, Sergi, David, José del Peral, Toni and Yi. You had made me feel one of yours since the very beginning. I've really enjoyed those lunch times with interesting and fruitful conversations of any kind. And thanks also for helping me in any way you could.

Finally, last but not least important, I really like to thank the support provided by my parents and sister during all these years at the university.

Contents

List of Figures

List of Tables

1 Introduction

In the last few decades, Global Navigation Satellite Systems (GNSS) have become an indispensable element in our society. Currently, they are not only used to determine the user position, but they are used in a wide variety of sectors and situations, such as energy distribution (e.g. The power grid monitors), finance (e.g. The automated stock trading systems), transportation (e.g. Train monitoring or) or telecommunications (e.g. The cell phone towers). Due to their gain in popularity, GNSS have become target of attacks of diverse nature and motivations. Starting from knocking off the service that provides GNSS, until manipulating the GNSS signals to the attacker interests in order to cheat the PVT (Position, Velocity and Timing) solution. The consequences of such attacks could be disastrous, since critical infrastructures in key sectors of the economy rely partially or entirely on GNSS to its correct functioning.

Throughout the last years, the concern about GNSS spoofing has increased. One of the reasons is due to the availability of inexpensive programmable signal simulators that can be used to mount an attack. There are already available software-defined GPS signal simulators, such as one publicly posted in GitHub in 2015 [OSQ15]. This software can be downloaded and run on a wide number of general-purpose COTS (commercial-off-the-Shelf) RF generation platforms. The cost of these platforms is relatively cheap, and can be acquired for less than five thousand Dollars. These devices have already been tested, and have been verified that they can effectively work as a spoofer against a standard civil GPS receivers.

In the last few years, several attacks against GNSS have been documented. Some of these attacks were under controlled circumstances, and with an educational purpose. For example:

1. The capture and control of a drone [Ker14]. They took the control of a drone from forcing it to reacquire the satellites, and interposing counterfeit GPS signals. Once the drone was acquired the fake satellites, they had total control of the aircraft. They could drive it at any place chosen by the attackers, and the drone showed the expected position in which he should be located.

2. The steering of a yacht off its course [Bha17]. In this occasion, they took the control of a yacht by generating counterfeit GPS signals and forcing the yacht to acquire them. Once

they took the control of the watercraft, they could drive the yacht at any place they want, and the victim will not appreciate any deviation of established direction by the legitimate user.

There are also some other reported attacks with a non-educational or malicious purpose. For example:

1. The capture of a CIA drone by the Iranian military forces [DB11].
2. Jamming on the Korean peninsula carried out, supposedly, by the North Korea's regime [Sta12].
3. Spoofing in the Kremlin bordering area carried out, presumably, by the Russian Government [Seb16].
4. Or the most recent attack in the black sea reported by the USA government in which some ships were situated incorrectly over 32 km away from the true position [Gof17].

1.1 Motivation

The main focus of this thesis is showing that attacks against GNSS are real and a possible threat. Since they are feasible, a constant threat exists against GNSS systems and the dependant subsystems. Since the kinds of attacks against GNSS can be enormously wide, and they can exploit different vulnerabilities of GNSS, this document is centred on the SCER attacks, based on the unpredictable bits. Thus, the main objective of this document is showing that SCER attacks against GNSS are possible, specifically the based on unpredictable bits estimation, and are a feasible threat. The second objective of this thesis is to show that some techniques that can be used to detect the attacks.

1.2 Methodology

To obtain the results of this thesis, the work has been based on MATLAB and GNSS signals. The signals are recorded from authentic satellites, and created synthetically with a signal generator. The recorded signals have been useful to obtain the results based on real data. So the methodology of this thesis can be divided in the following steps:

1. Record the GNSS signals from real satellites. These records were previously recorded at UAB some time ago (July 2014). The signals were recorded at the faculty of Veterinary and at the faculty of Engineering.

2. With an existing Software-Receiver [1] developed in MATLAB the acquisition and tracking data of the recorded signals has been performed. So with this software receiver has been obtained the main parameters of the GNSS signals, such as the code delay or the Doppler frequency.

3. The attacks were performed with an existing Signal Generator [2] modified properly. From the tracking results obtained in step 2, the appropriate modifications were performed to a generated signal with the Signal Generator. As a result, a GNSS signal with no superficial differences compared with the originally recorded was obtained. But, this signal had an spoofer attack under the surface. Both signals the authentic and spoofer gave the same PVT solution, which demonstrates that they were almost the same signal, since the code delays were not modified.

4. Finally, some Matlab scripts to implement the spoofer detection techniques were developed. With these scripts the detection results were obtained.

1.3 Thesis Outline

In Chapter 1 an overview and some examples of applications of GNSS is introduced. In Chapter 1 some examples of GNSS attacks providing the references are given.

In Chapter 2 some GNSS fundamentals are introduced, focused above all in GPS and Galileo. In this chapter will also be given a few brush-strokes about GNSS history, among other things the segments in which they are composed and a brief comparison between the current deployed positioning systems. Next the GNSS signals will be described, focused on the GPS and Galileo signals. After that the Navigation Data of GPS will also be described. Finally, the receiver architecture and the positioning principle of GNSS will be explained.

In Chapter 3 the state-of-the-art about GNSS attacks is summarized. We will describe its general features, focusing the attention on the signal modifications. Then we will describe some countermeasures against these attacks, which are divided in encryption and non-encryption defence methods. Then, we will explain in what consists the Unpredictable Bit Estimation Attacks, which in fact is the main focus of this thesis. After describing the signal model and the main features of the purposed attacks, the authentic and counterfeit signals will be compared. Tp end this chapter we will carry out a simulation about the estimation performance of the symbol estimation depending on the level of noise in the signal.

In Chapter 4 the purposed detection methods against the Unpredictable Bit Estimation Attacks are described. Two methods are taken into account, showing its main features and also

[1] GPS Software Receiver in Matlab, Copyright (c) 2003-2013 David S. De Lorenzo

[2] Copyright (c) 2004-8 David S. De Lorenzo

describing its main actions.

In Chapter 5 the results obtained after apply the detection methods described in Chapter 4 against the Unpredictable Bit Estimation Attack strategies proposed in Chapter 3 are summarized. We analyse these results in order to verify that the spoofer tell-tale can be detected, and in what circumstances they can be detected.

Finally, in Chapter 6 the conclusions of this thesis are shown, based mainly on the results obtained in Chapter 5.

2 GNSS Fundamentals

2.1 Introduction

In ancient civilizations, positioning was based on the observation of celestial objects. To determine the position and the course, the travellers path was based on the position of the moon, sun, stars and other celestial bodies in a determined time of the day. These celestial bodies were the unique reference the travellers had when they travelled in isolated places as the sea or deserts. But they were not always visible (due to clouds, trees, etc.). Nowadays, the positioning and navigation discipline has suffered a striking evolution. This change has been lead by the discovery and use of radio-frequency signals. This advance in radio-frequency signals has lead us to the implementation of the Global Navigation Satellite System (GNSS) we can use nowadays placing artificial satellites in the space that are always visible (in terms of operation, there are always some of them visible in any place). These satellites based on radio-frequency are useful even when bad weather conditions occur, unlike with the celestial bodies used in the old days.

GNSS has military origins, as most of the current telecommunication systems currently used, such as the RADAR. In the early 1960s the U.S. Navy's navigation satellite system (also known as Transit) was launched to help the navigation of U.S. submarines. Its functioning was based on the Doppler effect, and it was composed by 5 or more satellites in a low polar orbit. With this system was required about one hour to determine the position. Transit soon became widely adopted by commercial marine navigators, and it was the precursor of the current NAVSTAR Global Position System (GPS). The soviet union also developed its own version of Transit. It was called TSIKADA. A few years later, in 1970s, GPS was developed by the U.S. Department of Defence. It took over 20 years to make it fully operational. It was composed by a constellation of nominally 24 satellites with accurate on-board clocks, spread-spectrum signals with pseudo-random codes and multiple carrier frequencies. At the same time the Soviet Union also developed its own GNSS system. It was called GLONASS. Currently, other countries and regions have also developed or are currently developing its own global or regional navigation systems such as Japan (QZSS), China (Beidou, or the second version called COMPASS, which is still in development) or India (IRNSS). In 2002 started the development of Galileo, the European GNSS system, which will be fully operational in 2020 (although it is already functional). Complementary to GNSS, augmentation satellite systems has been developed. This complementary systems are based on a geostationary earth orbit (GEO) constellation of satellites that co-work with GNSS. They are mainly, but not only used for aviation. The most important are: WAAS (U.S.), EGNOS (Europe), MSAS (Japan), or SDCM (Russia).

In the present chapter we will introduce the GNSS fundamentals, in particular GPS fundamentals. Although most of the explanations can be extrapolated to the other GNSS such as Galileo. This fundamentals of GNSS will be specially important to understand the attacks described in Chapter 3. In Section 2.2 the principle of operation and the system architecture of GNSS is explained, focused mainly on GPS and Galileo. In Section 2.3 the signals that compose GPS and Galileo are explained. In Section 2.4 some details about the blocks that composes most of GPS receivers are given. Finally, in Section 2.5 we explain the principle by which the user position is determined. The present chapter is mainly based in references [Kap06] and [PM06].

2.2 GNSS Architecture

In this Section the architecture of the currently deployed GNSS is described. GNSS is composed basically by three segments: The Space Segment, The Control Segment and The User Segment. The Space Segment comprises the satellites in the space and the Control Segment deals with the management of the satellite operations. On its behalf the User Segment covers the equipment required (e.g. receivers). Therefore, each of the segments has a determined role in the resulting PVT (Position, Velocity and Time) solution. In Figure 2.1 the three segments that compose any GNSS are depicted.

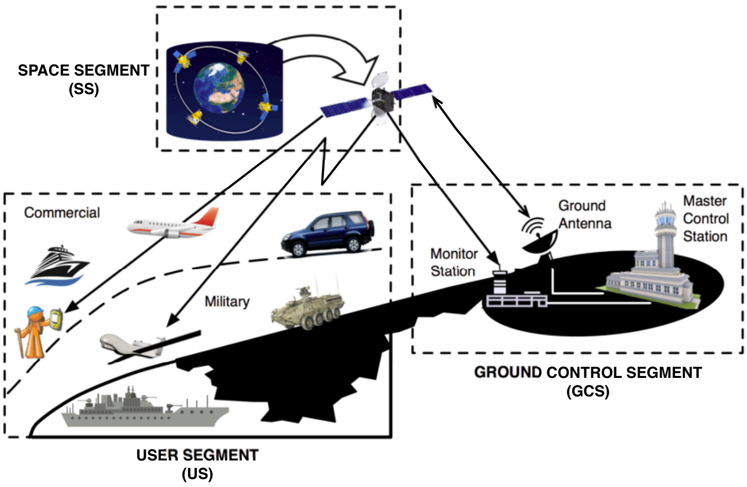
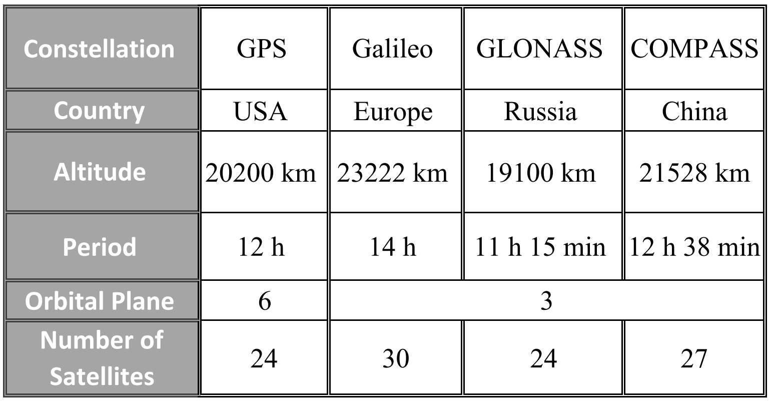


Figure 2.1: GNSS Segments in GPS (Image taken from [ER17]).

2.2.1 Space Segment (SS)

The SS is composed by the total set of satellites (between 24 and 30, depending on the GNSS considered) placed in a determined orbit around the earth. The satellites are placed in the MEO (Medium Earth Orbit) orbit, between 19000 and 24000 km of altitude. This altitude depends on the considered GNSS. The period (the time it takes the satellite to give a complete orbit cycle) is between 11 to 14 hours. The set of satellites are arranged in 3 or 6 orbital planes. In Table 2.1 are summarized the SS for the most common GNSS.

With the set of satellites placed around the earth, almost all users with a clear view of the sky have a minimum of 4 satellites in view. Usually the user has more in view, given the interoperability of some GNSS, such as GPS and Galileo, which are interoperable at system level. The satellites broadcast the ranging signals and navigation data to the user equipment, which allows to measure their pseudoranges and determine their position. The communication is unidirectional, the user receiver is passive (only receives the broadcast signal and do not transmit any).



Constellation	GPS	Galileo	GLONASS	COMPASS
Country	USA	Europe	Russia	China
Altitude	20200 km	23222 km	19100 km	21528 km
Period	12 h	14 h	11 h 15 min	12 h 38 min
Orbital Plane	6	3		
Number of Satellites	24	30	24	27

Table 2.1: GNSS Space Segment comparison.

2.2.2 Control Segment (CS)

The CS is composed by a set of control stations located in different places of the earth. The control stations in GPS are divided in the Master Control Station (MSC) and Monitor Station (MS). In GPS the MCS is placed in Schriever, in an AIR Force Base near Colorado Springs (Colorado). This MCS is responsible of operate the system, and provide command and control functions. The specific functions are:

- Monitor the satellite orbits.
- Monitor and maintain the satellite health.

- Maintain GPS time.
- Predict satellite ephemerides and clock parameters.
- Update satellite navigation messages.
- Command small orbit corrections on the satellites, in order to compensate possible non-alignments in the orbit.

The MS's of GPS are composed by a set of stations spread around the earth. The monitor stations are operated remotely by the MSC. The MS's are responsible of:

- Watching and monitoring each satellite.
- Receiving telemetry from the satellites of their status.
- Uplinking commands to the satellites.
- Uploading the data to update the navigation messages that will be broadcast by the satellites (at least once a day).

Some monitor stations (located in Ascension, Diego Garcia and Kwajalein) are equipped with GPS receivers, meteorological instruments and a dedicated communications infrastructure to transmit its measurements to the MSC or the satellites.

On its behalf, the Galileo control segment consists of two Galileo Control Centres (GCC) situated in Oberpfaffenhofen (Germany) and Fucino (Italy). Each one of the GCC has different tasks:

- The one based in Fucino is called Ground Mission Segment (GMS), and it determines the navigation and timing data part of the navigation messages by means of the network of sixteen Galileo Sensor Stations (GSS). Each GSS collects and forwards the Galileo measurements and data to the GCCs in real time
- The one based in Oberpfaffenhofen is called Ground Control Segment (GCS), and it is responsible for the satellite constellation control and management of the different satellites. It provides the telemetry, telecommand and control function by means of the Telemetry Tracking and Control (TT&C) stations. These stations collect and forwards the telemetry data generated by the Galileo satellites. It also distributes and uplinks the control commands to the satellites.

2.2.3 User Segment (US)

The US consists of the user receivers. Their main function is to receive the GNSS signals, determine the pseudoranges, and solve the navigation equations in order to determine the PVT solution. The basic elements of the most common GNSS Receivers are: an antenna with pre-amplification, an L-band radio frequency section, a microprocessor, an intermediate-precision oscillator, a feeding source, some memory for data storage and an interface with the user.

2.3 GNSS Signals

2.3.1 GPS Signal Architecture

Each GPS satellite transmits in three different L-band frequencies, between 1 GHz and 2 GHz. In particular, the GPS frequencies are:

- L1: $f_{L1} = 1575.42MHz$,
- L2: $f_{L2} = 1227.60MHz$,
- L5: $f_{L5} = 1176.45MHz$,

On L1 two signals are transmitted, one for civil use and other for the USA Department-of-Defence authorised users. On L2 is only transmitted the Department-of-Defence authorised users signal. The L5 band is used to provide a means of radio-navigation secure and robust enough for life critical applications, such as aircraft precision approach guidance. This section will be focused in L1 and L2 bands.

The GPS signals consists on three components:

- A Carrier: It is a Radio Frequency sinusoidal that supports the signal information at a determined frequency bands (the frequencies L1, L2 or L5). This frequency bands are chosen to limit the impact of the signal propagation channel (e.g. the attenuation due to atmosphere) and to limit the size of antennas, since as lower is the frequency the waves better in terms of attenuation, but the antennas needs to be bigger.
- The Ranging Code (or Spreading Code): It is a family of binary codes called pseudo-random noise (PRN) sequences or simply PRN codes. These codes behaves statistically as white noise. This means that the PRN codes are orthogonal between them, which means that the cross-correlation (the correlation between two different PRN codes) is minimum (zero), and the autocorrelation (The correlation between a certain PRN code with itself)

is maximum (if both codes are perfectly aligned). This spreading codes allows the different satellites to transmit at the same time and at the same frequency. Its transmissions will be differentiated by the spreading code used. These code also allows precise range measurements, and mitigate most of the undesired effects of reflections and interfering signals received by a GPS antenna. The codes for the Standard Positioning Service (Civil use) are called Coarse/Acquisition codes (C/A codes), and the codes for the Precise Positioning Service are called Precision (encrypted) Codes (P(Y) codes). Each satellite transmits a unique C/A code on L1 and an unique P(Y) code on both L1 and L2.

Each C/A code is composed by an specific sequence of 1023 bits (which are known as *chips*). This sequence of chips is repeated each millisecond. Therefore, the rate of the C/A Code (or Chipping rate) is 1.023 MHz (or Mega Chips/second).

The P(Y)-code is an extremely long ($\approx 10^{14}$ chips) PRN sequence, with a Chipping Rate of 10.23 MHz (ten times greater than the C/A code). The P(Y)-codes are repeated once a week. Currently, the satellites transmits the P(Y) code encrypted, and it is called Y-code.

- The Navigation Data: It is a message that contains the satellite health status, ephemeris (satellite position and velocity), clock bias and almanac (a reduced-precision ephemeris). The navigation message uses a BPSK (Binary Phase Shift Keying) modulation (in L1 and L2 bands) and its bit rate is 50 bits per second, much smaller than the chipping rate of the code. The bit duration is 20 ms, and it takes 12.5 minutes to receive an entire navigation message.

The L1 and L2 signals leaving the k-th satellite described above can be modelled as

$$\begin{gathered} s_{L1}^{(k)}(t) = \sqrt{2P_c}C^{(k)}(t)D^{(k)}cos(2\pi f_{L1}t\theta_{L1})+ \\ +\sqrt{2P_{P_{L1}}}P^{(k)}(t)D^{(k)}sin(2\pi f_{L1}t+\theta_{L1}), \\ \\ s_{L2}^{(k)}(t) = \sqrt{2P_{P_{L2}}}P^{(k)}(t)D^{(k)}sin(2\pi f_{L2}t+\theta_{L2}), \end{gathered} \tag{2.1}$$

where P_c, is the signal power for the signal carrying the C/A code on L1; $P_{P_{L1}}$ and $P_{P_{L2}}$ are the signal powers for signals carrying the P(Y) code on L1 and L2, respectively; $C^{(k)}$ and $P^{(k)}$ are the C/A and P(Y) code sequences for the k-th satellite; $D^{(k)}$ is the navigation data for the k-th satellite; f_{L1}, f_{L2}, θ_{L1} and θ_{L2} are the carrier frequencies and the phase offsets corresponding to L1 and L2, respectively.

2.3.2 Galileo Signal Design

One of the main characteristics of Galileo is its interoperability with GPS. Thus, its signals must not interfere with the GPS signals. Galileo will provide three navigation signals (One of them divided in two sub-bands) in the next frequencies:

- E1 band: $f_{E1} = 1575.42$ MHz,
- E5 band: $f_{E5} = 1191.795$ MHz,
- E5a band: $f_{E5a} = 1176.45$ MHz,
- E5b band: $f_{E5b} = 1176.14$ MHz,
- E6 band: $f_{E6} = 1278.75$ MHz,

2.4 Receivers Architecture

The main objective of GNSS receivers is to determine the user position based on the received signals coming from the constellation of different satellites in view. Figure 2.2 shows the block diagram of a typical GNSS receiver. It is basically composed of:

- **Front-End**: It is the first block, just after the GNSS antenna. It is typically composed of a band-pass filter, a low-noise amplifier, a base-band converter and an analog-to-digital converter (ADC). Thus, this module is the responsible for carrying out the analog signal conditioning for the next blocks.
- **Signal Processing Module**: This block can be divided in two sub-blocks: the Acquisition Module and the Tracking Module. The aim of the Acquisition Module is to detect and identify the satellites in view. On its behalf, the aim of the Tracking Module is to track the variations on the acquired signals. More details about these two blocks are given in Section 2.4.1 and Section 2.4.2.
- **Navigation Module**: The aim of the Navigation module is to solve the user PVT solution, based on the procedures presented in Section 2.5.

Looking at Figure 2.2 we observe that the bigger module, and in fact the most important module, is the Signal Processing Module, which is divided in the Acquisition and Tracking modules. The aim of this module is to process the received signals for each satellite simultaneously, demodulate the system data, generate reference PRN code for each signal and acquire and track the different satellite signals. The outputs of the Signal Processing Module are basically pseudo-ranges, carrier phase measurements and the demodulated Navigation Message, which are used by the Navigation Module to obtain the user PVT solution. In Sections 2.4.1 and 2.4.2 are described the main two blocks of the Signal Processing Module.

2.4.1 Acquisition Module

At the output of the Front End Module, the GNSS signal has been conditioned for the acquisition Module, whose main task is to detect the satellites that are present in the signal. The first objective of the Acquisition Module is to determine the satellites present in the received signal, and to calculate a rough estimate of the time-delay from the satellite to the receiver and the Doppler shift of the available satellites. In order to do it, the correlation between the received signal and the PRN code replica sequence generated in the receiver is performed. One correlation by each satellite that composes the constellation is carried out. After this correlation, a set of correlation values are obtained. To determine if the satellite is currently in view, a certain threshold is declared. All the satellites whose correlation value is higher than a given threshold are considered in view, and therefore acquired. On the contrary, if the correlation value is lower than the threshold, the satellites are considered not in view, and hence are discarded. The acquisition code-delay and Doppler shift estimates are those values where the magnitude of the correlation gives the largest peak. This correlation peak is depicted at the top part of Figure 2.3. This Figure shows the 3D representation of the correlation in both frequency and time domain. Figure 2.3 shows as the biggest peak represents the Doppler frequency and delay of the acquired satellite. There can be determined the code delay in chips and the Doppler shift in Hz. In the bottom part is shown the correlation result in the time domain, which shows a clear peak that determines the code delay of the acquired satellite.

2.4.2 Tracking Module

The main goal of the tracking module is to refine the time-delay and Doppler shift initial estimates provided by the acquisition module, and to continuously track any change in any of these values. Figure 2.4 shows the different blocks by which is composed the Tracking Module.

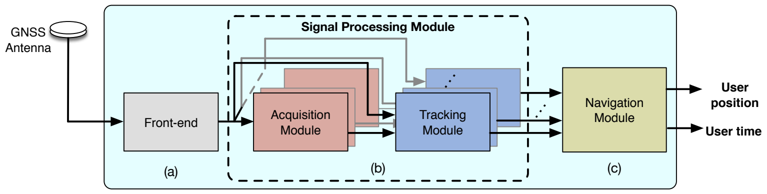


Figure 2.2: General receiver architecture ([ER17]).

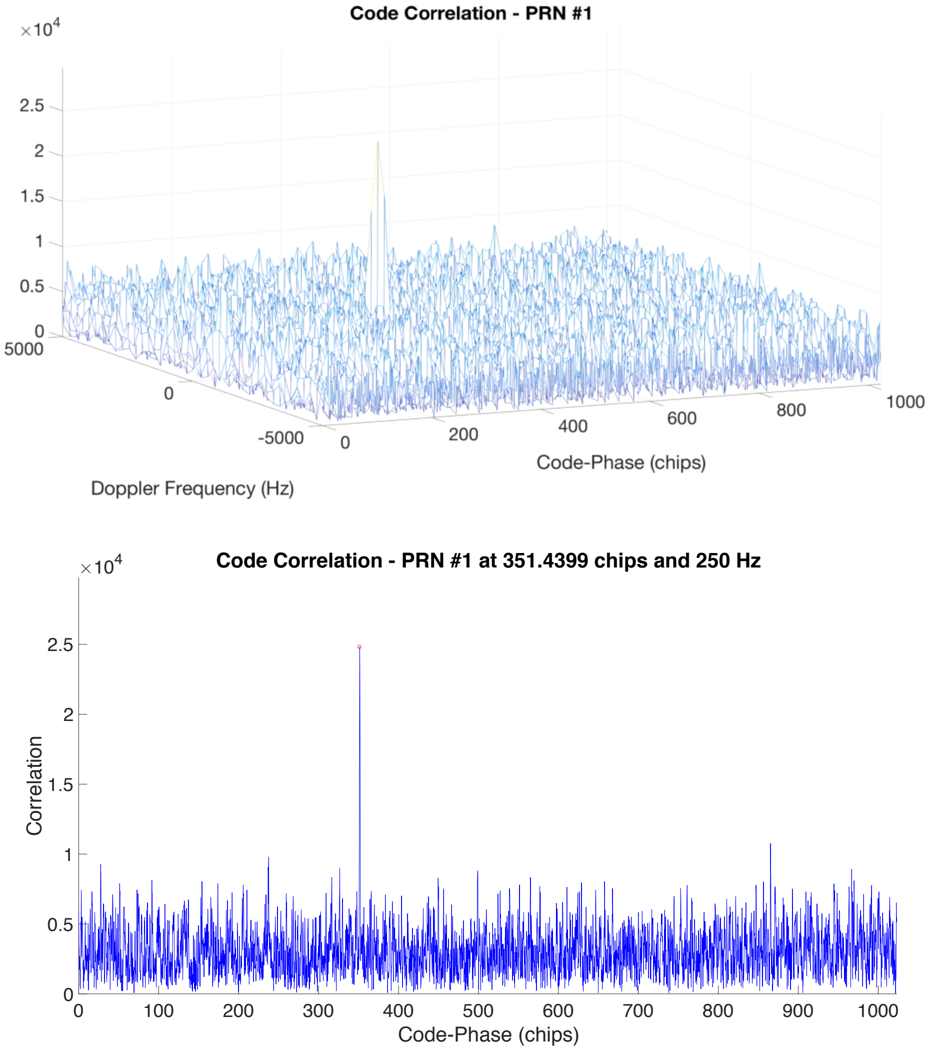


Figure 2.3: Time-Frequency representation of the correlation peak during the acquisition process. At the top is shown the Time-Frequency 3D correlation peak. At the bottom is shown the correlation result that determines the code delay.

It is divided in Code tracking and Carrier tracking loops. During the code tracking, the time-delay of the replica PRN is refined and continuously tracked in order to be aligned with the incoming code of the received signal. During the Carrier tracking any variation of the Doppler frequency is refined and continuously tracked. This continuous track is performed by means of the corresponding tracking loops. The loops are called Delay-Lock Loop (DLL) for the code-delay tracking, and Phase-Lock Loop (PLL) for the carrier tracking.

Following the scheme shown in Figure 2.4, the Front-end output enters to the code tracking. Particularly it enters to the Early-Late code tracking. The Early-Late code tracking shows that three correlations are indeed performed for code tracking: One computed at the prompt correlation (i.e. located at the code-delay estimate), and the other two located symmetrically before and after the prompt one, which are called early and late correlators, respectively. This kind of configuration leads to the early-late methods, where the discriminator output is obtained by comparing in some way or another the early and late correlators. At the output of the DLL discriminator are provided the estimation error values in the code-delay, which are introduced to the DLL Loop Filter. In the DLL loop Filter the measurement from the DLL discriminator is filtered with the aim of reducing the noise at the input of the NCO, and avoid instabilities. At the output of the NCO (Numerical Controlled Oscillator) DLL is obtained the current code-delay that must be introduced in the PRN Code Generator in order to generate an aligned copy

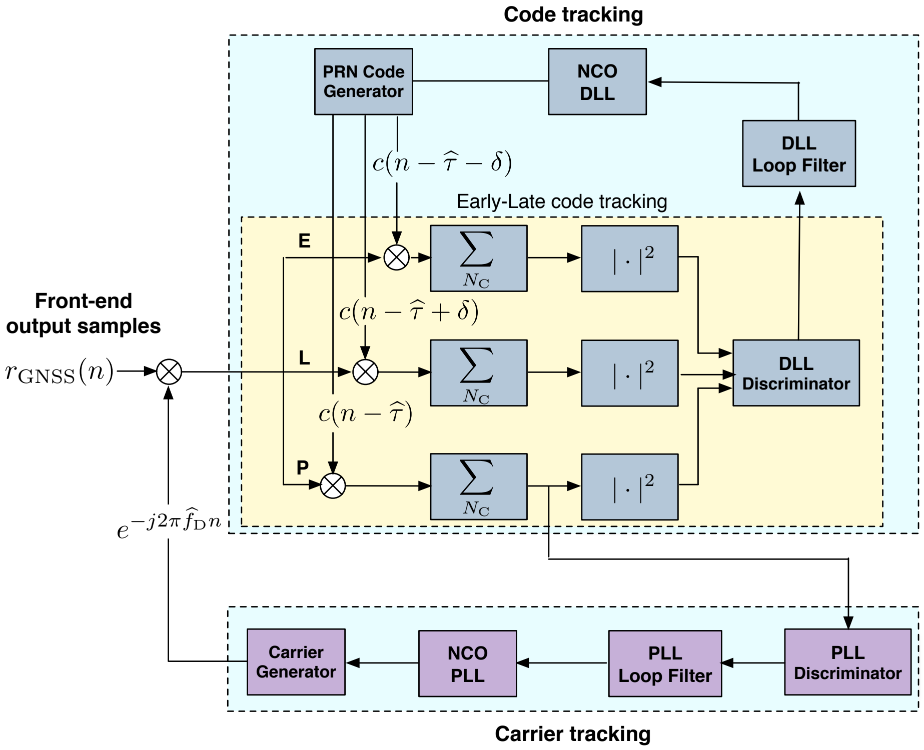


Figure 2.4: General architecture of the tracking module of a typical GNSS receiver ([ER17]).

of the PRN code. With this perfectly aligned copy of the code the receiver is able to despread the incoming signal with no errors due to misalignments of the code (since if the code is not perfectly aligned it behaves as if it were a different code).

On its behalf the Carrier tracking loop starts with the output of the prompt correlator. This value enters to the PLL discriminator, which provides a measurable value of the Doppler frequency error estimate. This value is introduced into the PLL Loop Filter, in order to filter the noise and obtain an smoother version of the value. At the output of the PLL NCO is converted the filtered discriminator output into a frequency that controls the generation of the local carrier replica.

Nowadays there are more recent tracking schemes based on the use of adaptive Kalman Filter techniques [LS16], providing better robustness compared to the conventional DLL/PLL-based techniques described above under harsh environments.

2.5 Navigation Module: Positioning Principle

GPS positioning is based on distance measurements referred to as trilateration, when three measurements are used, or multilateration, when more than three measurements are used. In order to determine the user position in three dimensions at least four satellites (one satellite for each unknown, three for coordinates and one for time) are needed, resulting in the following system of equations

$$r^{(k)} = c \cdot \Delta t^{(k)}, \tag{2.2}$$

where $r^{(k)}$ is the range distance between the k-th satellite and the user receiver, c is the speed of light and $\Delta t^{(k)}$ is the time it takes the signal to arrive to the user receiver from the k-th satellite. Thus, the distance $r^{(k)}$ is computed by measuring the propagation time required for the satellite ranging code to arrive to the user receiver antenna. The process of measuring this propagation time is depicted in Figure 2.5.

In Figure 2.5 is shown the code generated by a certain satellite, starting in t_1. At the receiver, this code arrives at the time instant t_2, with a certain delay due to propagation, which is represented by Δt. In the receiver, an identical code is generated at t (being the receiver clock the time reference, not necessarily being t_1). This replica code is shifted until both replica codes are perfectly aligned (both codes are correlated, and when this correlation is maximum means that both codes are aligned). If the satellite clock and the receiver clock were perfectly synchronized, the correlation process would give us the true propagation time. The problem is that the clocks of the satellite and the user receiver are not perfectly synchronized.

The receiver clock will generally have a bias error from system time called τ_u, which is in principle unknown. In addition, the satellite clock also has a certain error offset (even using highly accurate atomic clocks), composed of bias (mainly due to the relativistic effects) and drift contributions, represented by τ_s. This τ_s is assumed that it is compensated, since the GPS ground-monitoring network determines the required corrections and transmits it to the satellites, which includes this information in the navigation message. So, the corrections are applied by the user receiver and τ_s is compensated.

Due to the unknown error τ_u, the range found using Equation 2.2 is called *pseudorange*, represented by ρ, which means that this is not the true range but quite similar. After obtaining the pseudoranges for the k satellites, the position of the receiver can be determined using the next system of equations

$$\rho^{(k)} = \sqrt{(x^{(k)} - x_u)^2 + (y^{(k)} - y_u)^2 + (z^{(k)} - z_u)^2} + c \cdot \tau_u, \tag{2.3}$$

where $\rho^{(k)}$ denotes the pseudorange for the k-th satellite, determined using Equation 2.2; where $(x^{(k)}, y^{(k)}, z^{(k)})$ denote the k-th satellite's position in three dimensions; (x_u, y_u, z_u) is the user position; c is the speed of light; and τ_u is the user time offset (the time offset between the receiver and satellites clocks). Being (x_u, y_u, z_u) and τ_u the four unknowns to solve with these equations. The satellites position $(x^{(k)}, y^{(k)}, z^{(k)})$ are included in the navigation message (in the ephemeris data), so it is not an unknown.

These non-linear equations can be solved for the unknowns by employing either closed-form solutions, iterative techniques based on linearisation or Kalman Filter. From 2.3, the receiver position is given in Cartesian coordinates. These Cartesian coordinates are transformed to

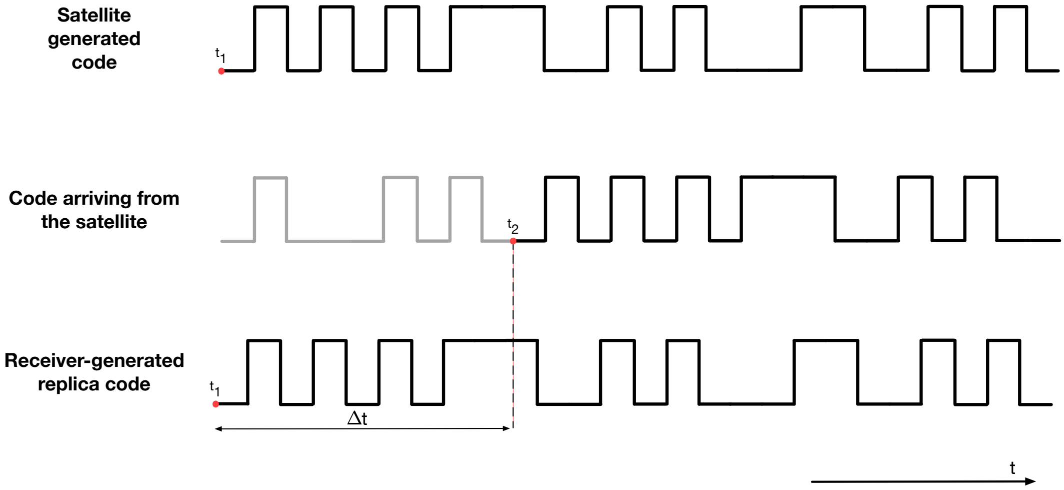

Satellite generated code
t_1
Code arriving from the satellite
t_2
Receiver-generated replica code
t_1
Δt
t

Figure 2.5: Use of the replica code to determine the satellite code transmission time.

geodetic coordinates; the geodetic system presents the location on the earth by its latitude, longitude and height.

3 Attacks Against GNSS

There is a wide variety of possible attacks against GNSS. Nowadays there is not a clear classification for them. A possible classification could be based on: The motivation of the attack (if it tries to deny the GNSS service or tries to impersonate the real satellite), the attack manipulation (if the attacker tries to manipulate the signal to his interests or only replay it) or the attack manipulation objective (if the attacker manipulates the signal, the transmitted symbols, etc.). However in [Hum09] is proposed a more clear classification, grouped in: Simplistic, Intermediate and Sophisticated, depending on their complexity and on the difficulties to detect and to apply countermeasures.

With the objective of having a more clear vision of the great quantity of possible attacks against GNSS, in Section 3.1 is carried out an overview of the most common attacks against GNSS described in previous works [Hum09] [Psi16] [Sch16] [JJ12], showing its key features and possible countermeasures. Section 3.2 will be focus on the unpredictable bits estimation attacks. Such attacks try to estimate the unpredictable bits of the navigation message, with the objective of obtaining a replica as similar as possible of the real signal sent by the satellite. Finally, in Section 3.4 will be shown a brief study of how much time requires the spoofer to estimate correctly these unpredictable bits in different conditions of C/No.

3.1 GNSS Attacks Overview

3.1.1 Spoofing Attacks Classification

In [Hum09] is proposed a possible classification of spoofing attacks against GNSS. They are divided in three categories:

- **Simplistic Spoofing Attacks**: The simplest spoofer attacks in GNSS are composed by a signal generator connected to a transmitting antenna. This attack can be easily detected, since generally it is not able to synchronize the signals with the satellites in view, and the pseudorange, C/N_o and Doppler jumps will occur. A receiver could be fooled by a GNSS signal generator, specially if the target receiver is jammed and forced to reacquire the satellites. This spoofing attacks are quite expensive, due to they require specific hardware such as a GNSS signal generator, which is expensive (about $ 400k) and it is not portable.

- **Intermediate Spoofing Attacks**: This attack category contains more complex attacks than the previous one. this attack combine a GNSS receiver with a transmitting RF front-end. This type of spoofer is able to synchronize the frequency and align the code-phase between the real and the counterfeit signals. When the signals from the satellites are tracked by the attacker receiver, it has a perfect knowledge of both the Doppler shift and the spreading code delay. Most of the receivers correctly modified can be converted into spoofer devices, reverting the receiving chain, adding some offsets to each satellite signal and broadcasting a modified version of the received signal in the air. This type of spoofer is able to modify the signal strength of the counterfeit signal, in order to simulate that the signal comes from the satellite (and its strength is extremely lower, compared to a transmission coming from the earth). The victim receiver is not able to distinguish the counterfeit signal from the genuine, since the spoofer accurately reproduce the code phase, frequency and navigation data bits. This last thing requires a bit prediction and estimation procedure to attack in real-time. In Figure 3.1 the general procedures in Intermediate Spoofing Attacks are depicted.

  The intermediate spoofing attacks can be built with software parts, RF components that anyone can download and buy by a very reduced cost (a few hundred dollars). To perform this attack is required a deep knowledge of GNSS signal processing. This document will be focused in this kind of attacks.

- **Sophisticated Spoofing Attacks**: The Sophisticated Spoofing Attacks consists of a coordinated and synchronized attack carried out by different spoofing devices. This type of attack is the most complex to implement and deploy, and the most expensive and difficult to perform. These attacks are also the hardest to defend against. In this attack the spoofing devices act as a Beamforming antenna array, simulating the different angles of arrival for different satellites. This can be accomplished either by keeping each spoofer

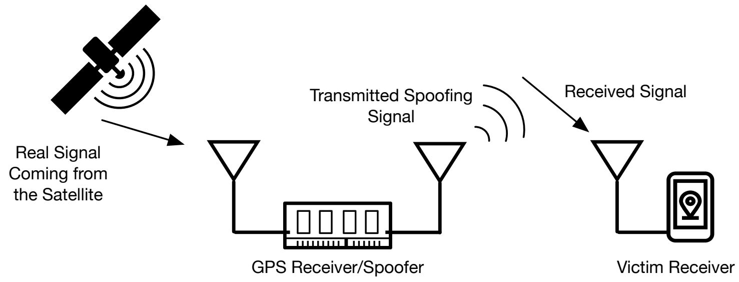


Figure 3.1: Illustration of a typical Intermediate Spoofing Attack.

fixed and transmitting the signals of all satellites with appropriately calculated delays, or by having each spoofer transmitting the signal of exactly one satellite and mechanically moving the spoofer around the target receiver. Implementing sophisticated spoofer based on GNSS receivers is possible but technically unmanageable.

On the following lines will described some state-of-the-art attacks and countermeasures, in order to introduce some of the key aspects of spoofing attacks and have a general idea of how can be attacked.

3.1.2 Jamming Attacks

The most simple attack against GNSS is Jamming [AR15]. GNSS jammers broadcast an interference signal (typically white noise) in the frequency band used for the satellite. This attack can be categorized as Denial of Service (DoS attack), since the GNSS is still available but the signal is masked by the jammer power (whose power is diverse orders of magnitude higher than the signal coming from the satellite, which is under the noise level). In Figure 3.2 shows some jammer devices acquired by Fraunhofer IIS. The devices are portable and can be feed even by the car cigarette lighter receptacle.

3.1.3 Meaconing Attacks

Meaconing attack [AR15] consists on the interception and rebroadcast of true GNSS signals (or the recording and playback) with enough gain to overwhelm the true signal at the target antenna. This attack does not modify the signals, so the target receiver's PVT (Position,

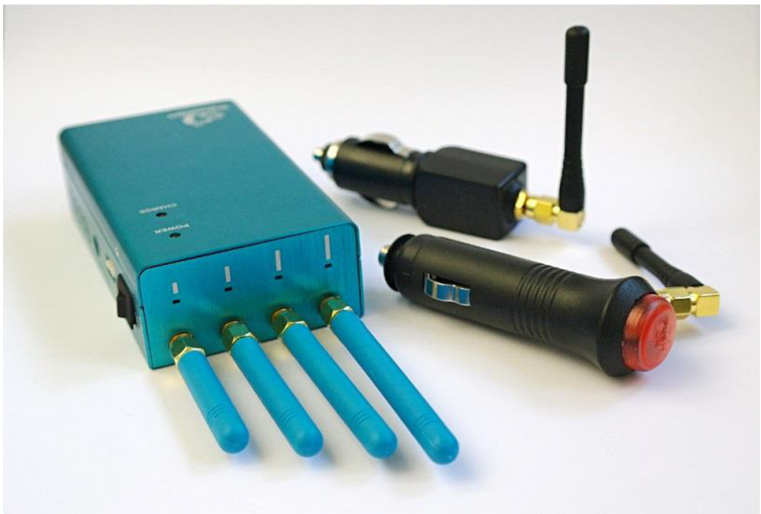


Figure 3.2: Commercial jammers acquired by Fraunhofer IIS (Figure taken from [AR15]).

Velocity and Time) solution is not modified directly, but the arrival of the signal at the target GNSS receiver is delayed, producing the victim not being able to compute its true PVT solution. Through a meaconing attack, even an encrypted GNSS signal (as the military L2 in GPS or the Commercial Service in Galileo) can be attacked, since meaconing attack only rebroadcasts the authentic signals. This attack is extremely easy to implement, since it only requires a few RF components. Figure 3.3 summarizes the steps of replay attacks. The adversary captures and replays the signal after a certain time, with a minimum delay called t_replay due to the rebroadcast RF generation. The signal arrives to the victim receiver with a certain delay, due to the time the spoofer needs to rebroadcast the signal (t_replay) plus the propagation time between the spoofer and victim receiver.

3.1.4 SCER (Security Code Estimation and Replay) attacks

SCER attacks are close related to Meaconing attacks. The main difference is that SCER attacks allow greater flexibility than Meaconing attacks, since the target receiver PVT solution can be manipulated. The attacker needs to despread, estimate and modify the signal at the same time that is transmitted. In Section 3.1.4 these attacks are fully described.

3.1.5 Non-encryption Based Defences Against GNSS Attacks

3.1.5.1 Spatial Processing Techniques

Spoofing transmitters usually transmit several counterfeit signals from the same location, while the authentic signals are transmitted from different satellites with different Direction of Arrival. Therefore, a spatial processing technique such as beamforming can be employed [McD07]. The receiver can use an antenna array and concentrate its radiation pattern in the direction of the

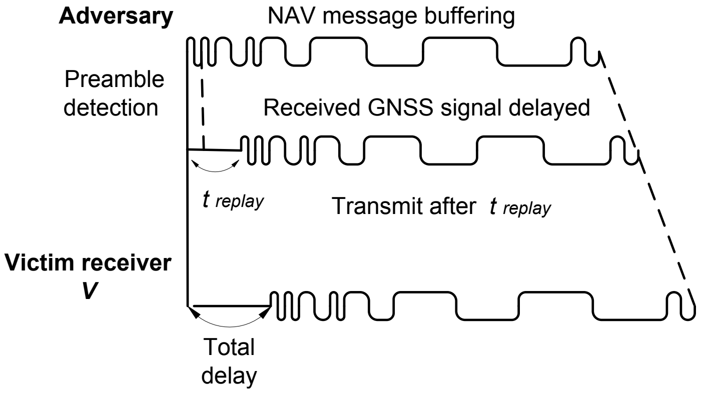


Figure 3.3: Illustration of a general Meaconing attacks (Image obtained from [AR15].

satellites, increasing the desired signal strength and attenuating the unwanted signals. Beamforming can also be used to estimate the Direction of Arrival (DoA) of the interference signal and try to avoid them. This process is called Angle of Arrival (AoA) discrimination.

Another method based on spatial processing can be performed comparing the phase difference between two fixed antennas [Mon09] for a certain time (e.g. an hour). Knowing the position of the antenna array and the satellites movement trajectory, the theoretical phase differences can be calculated and compared to the practical phase difference observed by the antenna array in order to discriminate the spoofer. The main drawbacks of comparing the phases is that it requires a long time (about 1 hour) and a perfectly calibrated and known orientation antenna array. A multiple-antenna spoofer might be able to defeat the multiple-antenna spoofing discrimination techniques depending on the number of transmit antennas, the number of receiver antennas, and the geometry of spoofer antennas with respect to the target receiver antennas. However, sophisticated spoofing scenario may be impractical to realize.

3.1.5.2 Clock bias or Time of Arrival (ToA) Monitoring

The basis of this method is the assumption that range code transmitted to a distant receiver by the spoofer will induce a time offset equal to the time required to transmit the signal to the target [JJ13]. Even if the spoofer adds a time offset to coincide with the target's local time, anomalous variations in the clock bias will reveal the presence of a spoofer. This delay can be observed in the PRN code offset and in unusual data bit transition boundaries. However, this method will only be useful if the target is moving in relation to the spoofer, otherwise this defence will be ineffective.

3.1.5.3 Received Power Monitoring (RPM)

This technique looks at the total received power in an absolute scale. This requires looking at all the received amplitudes and at the receiver RF front end's automatic gain control (AGC) set point [Ako12], which has low computational complexity. The total power might increase at the inception of an attack if the spoofer required a substantial power advantage respect to the original GNSS signal. The risk of false alarms would be a serious problem for this technique, since signal levels vary due to atmospheric and solar interference.

3.1.5.4 C/No Monitoring

The basis of this detection method relies on monitor and detect sudden or unusual variations in the C/No, which would mean an spoofer attack [JJ12]. In open sky conditions C/No might show smooth changes in the received signal power due to satellite movement and ionosphere variations, and sudden changes due to the presence of spoofer attack, since the spoofer transmission is considered interference to the real GNSS signal, which will decrease the C/No of the authentic signal. C/No is easily computable, and most of the GNSS receivers employ C/No measurements as a parameter that characterizes the received signal quality, which could be used for detecting an attack. However, this method may be sensible to multipath signals, which signal may increase the interference and decrease the C/No at the receiver.

3.1.5.5 Received Power and C/No Variations Related to Movement and Position

A different way to analyse the C/No could rely on the fact that the spoofer is transmitting all the PRN signals from the same place, and from a certain distance much smaller than the distance to the satellites located on the earth instead of the space [Jua11]. Therefore, if the receiver moves on the earth surface in low multipath open sky environments, no considerable changes in the received power from authentic satellites should be observed other than the deterministic losses occurring at lower elevation due to free space signal propagation. However, since the spoofing signal is usually transmitted from a single directional antenna located much closer to the receiver compared to the GPS satellites, the movement of the receiver relative to the spoofer antenna can considerably change the C/N0 received from spoofing signals.

This occurs because when the spoofer is very close to the target receiver, even a slight movement between spoofer and the target receiver can considerably affect the received spoofing signal C/No, due to the fact that as spoofing signals are usually transmitted from the same antenna, all experience the same propagation medium and similar channel. Therefore, variations of all spoofing signals will be the same regardless of the receiver movement and multipath effects.

This method is a low-complexity spoofing defence technique that does not require extensive hardware or software modifications to the GPS receiver. However, since the receiver does not necessarily knows the position of the spoofer antenna and the distance variations with respect to the receiver antenna, there is no guarantee that the receiver movement considerably changes the received C/No. Another drawback of this technique is that it cannot be employed for the case of static GPS receivers.

3.1.5.6 L1/L2 Power Level Comparison

Many GPS receivers are able to monitor both L1 and L2 signals which has a predefined power level difference [Wen17]. A low-complexity spoofer may only be able to generate the L1 signal. Thus, if L2 signal is not received, it can reveal the presence of spoofer. The main problem is that most of the civil GPS receivers do not have the ability to monitor both L1 and L2 frequency bands and this discrimination technique imposes additional hardware complexity to the GPS receiver.

3.1.5.7 Doppler Shift Detection

The defence based on method relies on detecting anomalies in Doppler frequency, specifically Doppler shift between real and simulated constellations. This means compare the Doppler effect measured in the receiver, with the simulated, in order to observe any trace of the spoofer's presence [FP03] [Sch16].

3.1.5.8 Complex Correlation Function

This method consists in looking at the complex correlation function from which a receiver synthesizes discriminators for its tracking loops [Psi14]. During the initial drag-off of the signal in a spoofing attack, misalignments between the true and spoofed code and carrier phases might occur, which result in distorted autocorrelation functions. Plotting the In-phase (I) vs Quadrature (Q) accumulations view of the complex correlation function, can be observed as the interaction of a spoofer signal will distort this picture, and instead of observe a straight line, it will be opened, and we will observe it distorted, since the autocorrelation will not be planar.

The detection method that looks at the complex correlation function has two main drawbacks. In first place, natural multipath signals produce similar results. So, a spoofing detector would need to verify if the observed distortion was not produced by mere multipath. The second problem is that this method might have a poor performance if the spoofer greatly overpowers the true signal. In this case, very little distortion occurs because, the true signal is too much smaller than the spoofed signal.

3.1.5.9 Reacquisition Technique

This method can work long after drag-off. This technique constantly attempts to reacquire all the tracked signals [Psi16]. This method performs a brute-force search for each signal over the entire range of possible code phases and carrier Doppler shifts. A brute-force acquisition search requires a heavy signal processing load on the receiver. A different strategy could be to search sequentially for additional instances of the tracked signals, one signal at a time. Then, if a second version of any received signal is detected, the receiver could then attempt to sort out the true signal versions from the spoofed ones in hopes of recovering its true navigation functionality.

However, this technique could be defeated by an overly powerful spoofer. Part of its effect could be to jam the true signals, making them undetectable during the reacquisition search.

3.1.5.10 Received Ephemeris Consistency Check

The navigation message of each satellite contains some ephemeris information corresponding to the position of other GPS satellites. This information can be obtained from other sources and compared. if any inconsistency among these ephemeris data is present, this can alert of spoofing attack [JJ12].

3.1.5.11 GPS Clock Consistency Check

The GPS clock information is contained in the navigation message of each PRN signal. The GPS clock obtained from the different satellites should be consistent enough. However, the GPS time extracted from an unsynchronized spoofer might not be consistent with the GPS time extracted from other satellites and this can alert the presence of a spoofing attack [JJ12].

3.1.5.12 Vestigial Signal Detection

In most cases, after successful spoofing attack, a vestige of the authentic signal can be used for spoofing detection and mitigation [EH08]. In this technique the receiver copies the incoming digitized front-end data into a buffer memory. Then, the receiver selects one of the GPS signals being tracked and removes the locally regenerated version of this signal from the buffered signal. Finally, the receiver performs acquisition for the same PRN signal on the buffered data.

The main drawback of the vestigial signal detection is that it increases the hardware and processing complexity of the receivers because this technique requires additional tracking channels to track both authentic and spoofing signals. In addition, in the presence of high power spoofing signals the authentic vestige might not still be detectable.

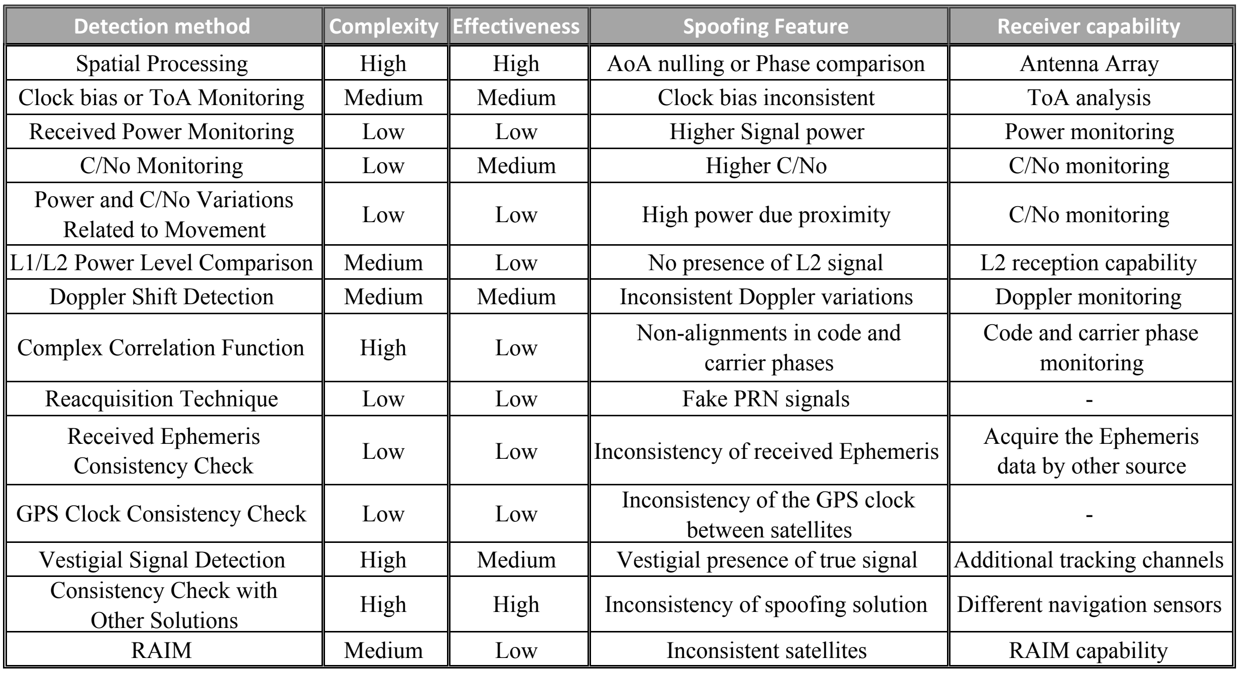
3.1.5.13 Consistency Check with Other Navigation and Positioning Technologies

The GPS receiver can compare the solution extracted by received GPS signals to the other position and navigation solutions obtained by mobile networks (3G/4G/5G) or WiFi stations [JJ12]. Therefore, if the solution provided does not coincide, there is a high likelihood of a spoofing condition. Employing this spoofing detection technique increases the hardware and software complexity of GPS receiver. In addition, alternative positioning technologies such as cellular networks do not usually provide position solutions as accurate as GPS signals, and the coverage is reduced.

3.1.5.14 Receiver autonomous integrity monitoring (RAIM)

This method is the oldest and the most widely used anti-spoofing strategy in GNSS receivers. This method checks all available GNSS signals for spatial consistency, and can exclude erroneous satellites [Kuu07]. For example, the ephemeris data predicts the location of satellites in advance, and this should closely agree with their reported position in the navigation message and external sources. In the case of authentic signals, the frequency changes due to the Doppler effect, and the PRN code is delayed to maintain signal lock. A low-quality spoofer might not be able to keep this correlation. Another RAIM procedure could be looking for clock consistency times with other satellites not currently being tracked.

The main weakness of RAIM is that it assumes that any spoofing attack will be confined to one or two satellites, not the entire constellation.



Detection method	Complexity	Effectiveness	Spoofing Feature	Receiver capability
Spatial Processing	High	High	AoA nulling or Phase comparison	Antenna Array
Clock bias or ToA Monitoring	Medium	Medium	Clock bias inconsistent	ToA analysis
Received Power Monitoring	Low	Low	Higher Signal power	Power monitoring
C/No Monitoring	Low	Medium	Higher C/No	C/No monitoring
Power and C/No Variations Related to Movement	Low	Low	High power due proximity	C/No monitoring
L1/L2 Power Level Comparison	Medium	Low	No presence of L2 signal	L2 reception capability
Doppler Shift Detection	Medium	Medium	Inconsistent Doppler variations	Doppler monitoring
Complex Correlation Function	High	Low	Non-alignments in code and carrier phases	Code and carrier phase monitoring
Reacquisition Technique	Low	Low	Fake PRN signals	-
Received Ephemeris Consistency Check	Low	Low	Inconsistency of received Ephemeris	Acquire the Ephemeris data by other source
GPS Clock Consistency Check	Low	Low	Inconsistency of the GPS clock between satellites	-
Vestigial Signal Detection	High	Medium	Vestigial presence of true signal	Additional tracking channels
Consistency Check with Other Solutions	High	High	Inconsistency of spoofing solution	Different navigation sensors
RAIM	Medium	Low	Inconsistent satellites	RAIM capability

Table 3.1: Summary of the spoofing detection methods key features.

3.1.6 Encryption Based Defences Against GNSS Attacks: Navigation Message Authentication (NMA)

Cryptography has often been proposed as a solution to attacks against GNSS. Encryption introduces unpredictability in the navigation message, so that producing a counterfeit signal would be more difficult. The encryption can be performed at chip level [Poz10] or at data level [FH16] [Lev11] [O'H10] [Cur17] [Cap17]. However, most of the devices use the unencrypted civilian signals, and adding any form of encryption to those public protocols is not possible, due to the fact that most of the receivers would not be used any more because they will require critical modifications. Another serious limitation of cryptographic methods is that they are not very useful against replay attacks such as meaconing or SCER, since the encryption method can be replayed or estimated.

Navigation message authentication (NMA) generally refers to encryption protocols that provide authentication and integrity protection to the Navigation Message. The user can check if the received Navigation Message is authentic and it has not been intercepted and modified by an attacker. To add authentication and integrity to the Navigation Message can be performed by Symmetric Key Encryption, Asymmetric Key Encryption, Digital Signature, etc. It can also be performed by more complex key systems, such as Timed Efficient Stream Loss-Tolerant Authentication (TESLA). On the following lines are described the different procedures mentioned before.

3.1.6.1 Symmetric Encryption

This method consists in encrypt the Navigation Message (although the key could be instead applied to the spreading code, encrypting the entire signal) with a certain private key, which is shared to the receivers (symmetric encryption), similar to which is done in military applications [Sch16]. Only the receivers that have the key are able to decrypt the Navigation Message. The receivers that does not have it, will not be able to decrypt the Message, and thus by any way modify it. The key authenticates the Navigation Message, since ideally only the satellite and authorised receivers can manage the key.

If the key is applied to the spreading code the spoofer would need first to decrypt the signal under the noise level to be able to modify and rebroadcast the authentic GNSS signal.

Symmetric encryption, although providing a very high level of resistance to spoofing, are impractical for a civilian receiver due to the required level of secrecy in the key and necessary modifications (which in fact could need to be renewed) in the receivers.

3.1.6.2 Asymmetric Encryption

The main difference of asymmetric encryption is that a pair of associated keys are generated instead of a single one. One of them is kept private and the other is become of public domain. The key-pair completely reverses to each other in the process of encryption and decryption. Before the satellite sends the Navigation Data, it is encrypted using the private key. At the user receiver, the public key is used to decrypt the message and be able to read it. By this procedure the navigation data is authenticated, since the only key that could encrypt the message is the private key embedded in the satellites.

The main drawback, as most of the cryptographic techniques, is that the main structure of GPS signals is changed, and in consequence the receivers. Asymmetric encryption would require a modification of the current GPS receivers, which would have to store the public key and include the decrypt process. Moreover, asymmetric keys must be longer than symmetric keys to provide the same level of security, which requires a higher computational capacity during the encryption/decryption process.

3.1.6.3 Timed Efficient Stream Loss-Tolerant Authentication (TESLA)

TESLA uses a delayed key disclosure scheme to provide authentication and integrity of messages [Her15] [Per02]. With TESLA are generated an extremely long key-chain of length L, by choosing a random secret key k_L (first key), and it is recursively applied a one-way function $F(\cdot)$ by which if $F(A) \rightarrow \mathcal{B}$, $F(B) \nrightarrow \mathcal{A}$, until the last key k_0 (root key) is obtained. These generated keys are then used by the satellite in reverse order to sign the message. Due to the one-way property of the key-chain, knowing k_i does not give any information on key k_{i+j} $\forall j > 0$ since they are sent in reverse order. The receiver is thus able to authenticate the key by applying the one-way function i times to recover the root key. This root key must be previously authenticated by other means, such as digital signature. The receiver might not need to perform the one-way function i times until reach the root key, it only needs to reach the last authenticated key k_j ($F^{i-j}(k_i)$ with $j < i$).

TESLA uses the keys from the key-chain described above for building the MAC's (Message Authentication Code). If the satellite at the time instant i wants to send the message M_i, then could be used the key k_i to compute the MAC as $MAC_i = S(M_i, k_i)$ (where S is the authenticating algorithm). The packet transmitted is composed by $P_i = [M_i, MAC_i, K_{i-d}]$ with $d > 0$.

The receiver is not able to authenticate the received packet $P_i = [M_i, MAC_i, K_{i-d}]$ instantaneously, because it does not know the value of K_i, which has been used to compute the MAC. So the receiver has to wait d time instants to receive K_i. Once it has been received, the receiver checks if the received key k_i is valid. In case it is correct, the receiver will be able to compute the MAC for the received data with K_i, and determine if this MAC is equal to the received one by doing $MAC_i = S(\hat{M_i}, \hat{k_i}) = \widehat{MAC_i}$ (where the received parameters are depicted with a $\widehat{\ }$)

3.2 Unpredictable Bit Estimation Attacks

First of all, in Section 3.2.1 the received signal model is described, which will be useful to describe the SCER attack strategies and the counterfeit techniques. In Section 3.2.2 the Forward Estimation Attacks (FEA) are explained, and how they are related to NMA. Then in Section 3.2.3 are described the SCER attacks under NMA. Two different strategies are described by which the spoofer can estimate the unpredictable bits of the Navigation Message in order to perform a zero-delay SCER attack under NMA. In Section 3.2.4 a possible strategy of FEA attack is described, showing its peculiarities.

In Section 3.3 a comparison between a recorded real signal and a synthetically generated spoofing signal (based on the authentic) is shown, demonstrating that both of them are practically identical. Finally, in Section 3.4 the efficiency in the symbol estimation of the spoofer under different conditions of C/No is shown.

3.2.1 Received Signal Model

The received signal (considering only the L1 C/A code) by the spoofer (or in fact by any receiver) after being down-converted (to intermediate frequency), filtered and transformed to the digital domain with an Analog to Digital Converter (ADC) can be written as

$$Y(n) = \sum_{k=1}^{N} A_k S_k(n - \tau_k) e^{j2\pi(f_{IF} - f_k)n + \varphi_k} + W_k(n), \tag{3.1}$$

where A_k is the carrier amplitude, $S_k(n)$ is the useful signal, τ_k is the code delay, f_k is the Doppler frequency and φ_k the complex random phase of the k-th satellite from the total set of N that are in view; f_{IF} is the receiver Intermediate Frequency and $W_k(n)$ is the AWGN (Additive White Gaussian Noise) noise for the k-th satellite. n denotes discrete-time domain. $S_k(n)$ is the useful data signal transmitted by the k-th satellite and can be expressed as

$$S_k(n) = \sum_{l=-\infty}^{\infty} D_l \sum_{i=0}^{N_r - 1} C_k(n - iT_{code} - lT_d), \tag{3.2}$$

where $D_l = \{-1, 1\}$ are the possible data symbols (considering BPSK modulation) at a rate of $R_d = 1/T_d$ bits per second (R_d =50 bps in L1 C/A code) that constitutes the Navigation Message, $C_k(n) = \{-1, 1\}$ is the spreading code or PRN sequence for the k-th satellite, T_{code} is the total time duration of the spreading code (1 ms in L1 C/A code) and N_r is the total number of times $Tcode$ is repeated within each bit interval.

3.2.2 Forward Estimation Attacks (FEA)

FEA attacks [Cur17] exploits the redundancy of some of the symbols transmitted by the satellites. This redundancy may be mainly due to two reasons. The first reason is due to the redundancy introduced by channel coding in the transmission of the Navigation Data. The Navigation Data can be coded before being transmitted in order to be able to recover the transmitted bits even when some of them are received corrupted. For example, if the Navigation data is coded with a Rate 1/2, this means that by each symbol of real data, the transmitter (in this case the satellite) will transmit two symbols. This produces that twice the number of the necessary bits are transmitted. With this coding rate half of the bits are unnecessary to decode the entire codeword in good transmission conditions. With the channel coding, the attacker does not need to predict perfectly all the symbols. The attacker may send random bits to the victim at the beginning, when the attacker doesn't have a reliable codeword estimate. Forward Error Correction (FEC) in the victim receiver will most likely correct the wrong symbols. Since FEC corrects the wrong bits, the victim will think that the received message is authentic, since on the surface there are no differences between the real and counterfeit signals.

The second reason of redundancy is due to the Navigation Data itself. Navigation Data contains some information, such as Ephemeris and Almanacs that can be obtained by other means since they are of public domain. With this information the attacker has information about the Navigation message that has not even been received, so some of the information transmitted by the satellite can be predicted by the spoofer. With those predicted bits the spoofer can perform an attack such as shown in Section 3.2.4.

3.2.3 Zero-delay SCER Attacks Under NMA

NMA introduces unpredictability in the data stream (this is explained in Section 3.2.2) or at the chip level. In [DW12] is proposed a general model for zero-delay SCER attacks under NMA based on a GNSS signal protected by some security code W_k. We can modify (3.1) to introduce the W_k code as:

$$Y(n) = \sum_{k=1}^{N} W_k A_k S_k(n - \tau_k) e^{j2\pi(f_{IF} - f_k)n + \varphi_k} + W(n), \tag{3.3}$$

where $W = \{-1, 1\}$ is a certain security sequence with time length T_w that protects the signal. The protection relies on the spreading code W_k, which is required in reception after being applied before transmission to be able to obtain the signal correctly, which in fact is the same that happens with any other spreading code.

The proposed model in (3.3) is based on that the GNSS signal transmitted by the satellites is protected by a certain W_k spreading code (with a certain code rate) composed by unpredictable chips, which is a secondary code similar as the PRN codes of the SV's. The spoofer receives and tracks the real signal coming from the satellite, and attempts to estimate the unpredictable security code chips on-the-fly in order to by able to reproduce the signal. These W_k chips are required to despread the received signal, and adds an extra protection to the GNSS signal, since the signal can only be despreaded with the associated W_k code. After those security code chips are estimated, the spoofer reconstitutes a GNSS signal, with the security code chips estimate taken the place of the authentic codes, and rebroadcast this signal to the victim receiver.

The real process will consist in estimate chip-by-chip the received symbol in order to be able to reconstruct the signal as if this signal were the authentic. The security code W_k in (3.3) is useful to model the chip uncertainty produced by NMA.

The new generated signal after estimating the W_k chips will have unavoidably a certain delay due to the estimation process (also the time it takes the spoofer to modify the position and timing offsets of the signal, in order to modify the PVT solution) and transmission delay. Although this delay can be neglected if the spoofer is close enough to the victim and the estimation-rebroadcast process is done on-the-fly (as soon as the samples arrives the spoofer are rebroadcast). Depending on the delay of the rebroadcast signal, the spoofer will have to force to reacquire the signal in the victim receiver. If this delay is shorter than a code chip interval, the spoofer will be able to dislodge the target receiver's tracking loops without forcing reacquisition. On the contrary, if the delay of the retransmitted signal is greater than the spreading code chip, the spoofer must first jam or obstruct the incoming GNSS signal to force the victim to reacquire the satellites.

Based on the circumstances described above, in Section 3.2.3.1 and Section 3.2.3.2 two strategies the spoofer can consider to estimate W_k from the transmitted symbols in (3.3) are described and how the signal can be reconstructed as soon as possible.

3.2.3.1 Chip-By-Chip Estimation Strategy

The first spoofer strategy to determine the symbol sent by the satellite consists in estimate and rebroadcast the received samples on-the-fly. Since this attack is a zero-delay attack, the spoofer cannot wait to receive the whole bit to perform the symbol estimation previous step to send it back as if this symbol were the real bit. If the spoofer did that, it would produce a minimum delay of 20 ms, which is the time duration of a single bit in GPS L1 C/A code signal. Since the estimation process cannot have estimation delays, the counterfeit bit has to be sent back at the same time the spoofer is receiving the original.

To estimate the data symbols $\hat{D}_l$, the spoofer needs first to despread the received signal with the aligned version of the code replica C_k from the output of the tracking loops. Then the spoofer needs to accumulate the received samples and estimate the symbol in each time instant

n. In order to do so, the spoofer applies

$$\hat{D}_l(N_s) = sign\left(\sum_{n=1}^{N_s} Y(n)\right), \tag{3.4}$$

where N_s is the total number samples received containing a single bit (with a maximum value of $20ms \cdot F_s$, where F_s is the sampling frequency of the receiver), $sign(\cdot)$ is the sign function (its output is +1 if the input is positive, or -1 if the input is negative). $\hat{D}_l(N_s) = \{-1, 1\}$ represents the estimated symbol in the time-instant N_s.

According to (3.4), after each time-instant is obtained an estimation of $\hat{D}_l$, which takes a value of ±1, depending on the sign of the accumulated received samples. The signal is then rebuilt and sent back to the victim, including the bit estimation $\hat{D}_l$, along with the rest of parameters obtained from the tracking loops, such as the Doppler frequency or code phase delay. As a result, the counterfeit signal will be exactly equal as the real, as long as the estimation $\hat{D}_l$ is correct. This estimation may vary along the time, since it is very dependant on the quality of the received signal (e.g How noisy the received samples are). This variation of $\hat{D}_l$ ends once has been received enough samples to estimate correctly the received bit. In Section 3.4 a set of simulations are carried out in order to determine the influence of the noise in the time of estimation of the bit. In Figure 3.4 a few ms of the beginning of the bit are shown, in which is depicted the bit estimation process. Figure 3.4 shows that during the first μs, there is a recognizable pattern in the estimated samples. The first samples vary significantly quick until it reaches a steady value. This variation of the estimation in the beginning of the bits is produced basically by the presence of noise in the received samples. This noise hides the real bit sent by the satellite and adds the spoofer more difficulties to get a quick and trustworthy estimation. Once the spoofer has accumulated enough samples, the symbol sent back by the spoofer is the correct and it is maintained along the remaining samples of the bit, with no more polarity variations.

It should be noted that the first estimation sample of $\hat{D}_l$, must be generated before the first sample of the signal coming from the satellite reaches the spoofer receiver. The performed attack is a zero-delay attack, and thus the samples must reach the victim receiver at the same time the satellite samples reaches the spoofer. Therefore, the spoofer needs to determine the estimation of the bit polarity before the information has been received from the satellite. The spoofer does not have any other option that try to guess the bit polarity by sending a certain BPSK symbol among the two possible. So, the spoofer sends a ±1 symbol sample, which could be right or wrong. When the second sample has to be sent back, the spoofer is able to estimate the bit with the sample received in the first time instant. The estimation process will not be too reliable, since it has only available a single sample to estimate the bit, and it may be very noisy. The spoofer makes this process continuously. So, the attacker accumulates the received

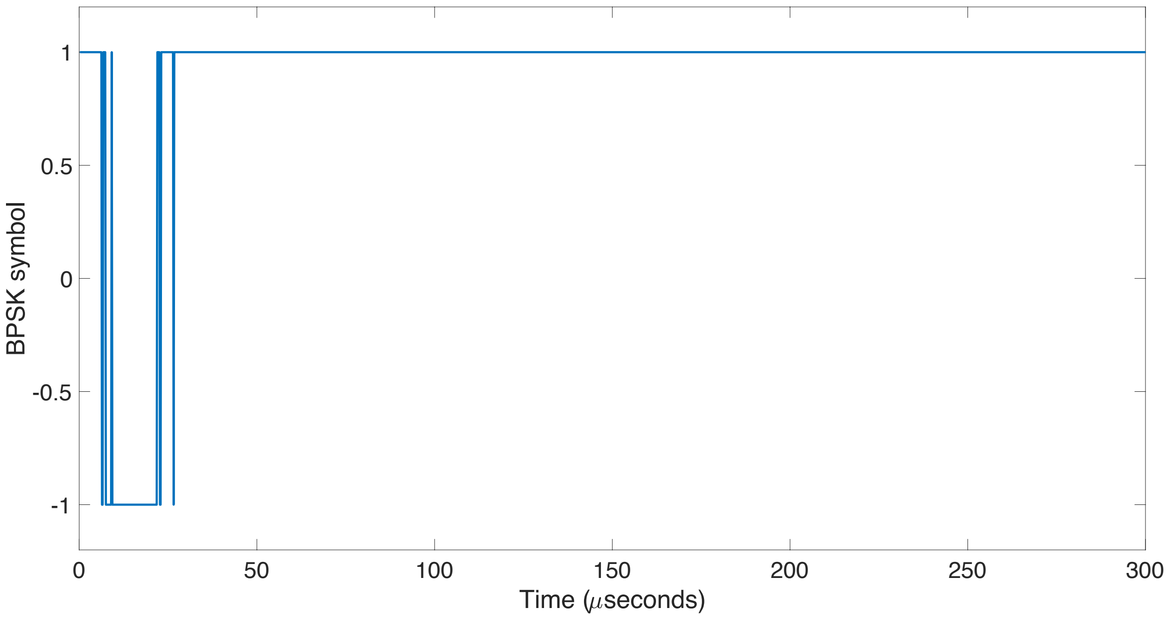


Figure 3.4: Chip-by-Chip estimation process of a bit.

samples, and estimates the bit in each time instant using the total amount of available received samples.

3.2.3.2 Bit-Guess Estimation Strategy

This second proposed strategy attack has some similarities with the described in first place. This attack is a zero-delay attack as well as the previous one, and it also estimates the real bit by accumulating the received samples in each time instant. But the main difference with the attack proposed in Section 3.2.3.1 is in the first milliseconds of transmission process, while the estimation process is carried out and there is no certainty of the right polarity of the bit that has been sent by the satellite. In this attack, the spoofer does not rebroadcast the bit estimation sample-by-sample, as in the previous one. The spoofer does not send the bit estimation until it is highly probable that the estimation is correct (or at least the spoofer is almost sure that the estimated polarity of the bit is right). The spoofer waits a prudent time or waits until the estimated polarity is repeated a certain number of times. Instead of sending the current estimation of the bit sample-by-sample, the spoofer has to determine the symbol polarity to transmit. This symbol polarity can be chosen by chance, or the spoofer might predict them (before receiving them from the navigation message) as good as possible with some logic, for example predicting the transmitted information. For example, the Ephemeris data can be obtained publicly from other sources such as the Internet. With all the information that the spoofer can get from other sources different than the real signal transmitted by the satellite, the spoofer is able to build a fake navigation message similar to the real one. This tampered Navigation Message is then modulated using BPSK modulation and used to determine the symbol to transmit in the first milliseconds of the counterfeit signal rebroadcast. The process of choosing the symbol to send cannot produce any delay in the rebroadcast process, since this attack is also a zero-delay attack. This predicted polarity is maintained until the estimation carried out in background is likely to be correct. Once the estimation of the bit is finished, the spoofer changes the polarity of the bit if needed. In Figure 3.5 this process is depicted, with an example where the symbol polarity determined at the beginning of the bit is needed to be modified after knowing that it was incorrect.

After the estimation process is complete, and the bit is totally rebroadcast to the victim, two options can occur:

- The first case to consider is when the bit random guess made by the spoofer has been right. In this case, the entire bit will be correct, and exactly equal as the sent by the satellite, since no sample will have different polarity compared with the real signal. In addition, this bit will be received with no delay, or at least this delay can be considered negligible. In this case the spoofer will be harder to detect.

- The second case is when the bit random guess made by the spoofer is wrong. If the random guess is wrong, the first samples and the last ones of the transmitted symbol will have the polarity inverted. This happens because one of the edges of the bit will be transmitting one of the two possible symbols, and the other edge the other one, due to the fact that

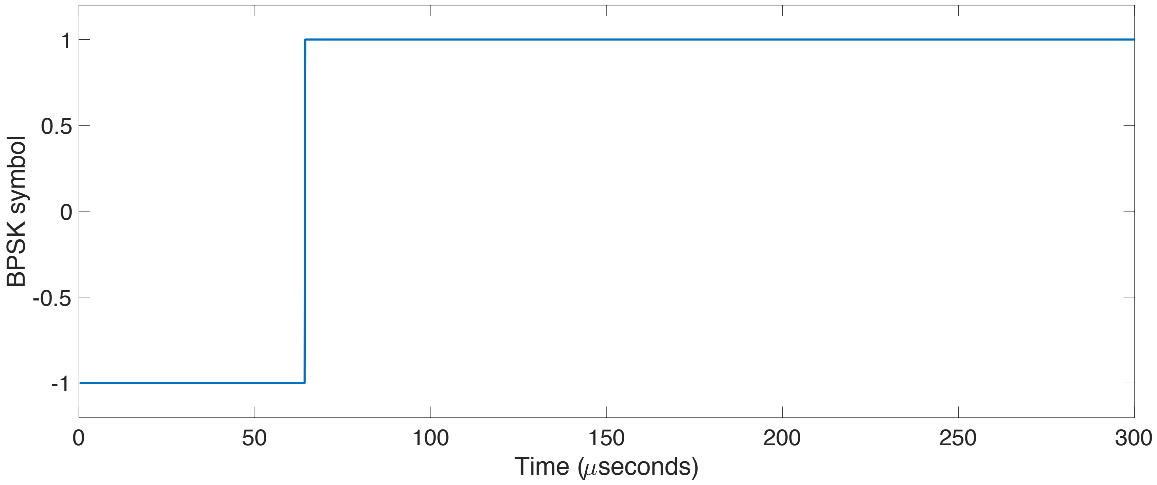


Figure 3.5: Bit-guess estimation process of a single bit.

the only possible symbols are 1, since the transmission modulation is a BPSK. This means that the beginning and the ending of the bit will have different sign. In addition, the total energy of the bit will be lower than an ordinary bit transmission, since some of the energy will be wasted on sending the wrong bit guess on the first samples. Analysing this two features, the sign and the energy, can be detected if a certain signal is the original or not, as it will be shown afterwards.

3.2.4 FEA Strategies

The third attack considered in this document follows a completely different approach compared with the attacks described above [Cur17]. In this attack the spoofer does not sent the estimation of the real bit at any moment. This time the spoofer does not estimate the real symbol in order to send a reliable copy of the bit. In this occasion the attacker makes a guess at the beginning of the symbol and this guess is maintained all along the entire transmitted symbol. This guess may be based on some prediction, so the guess may be carried out with some logic. However, the real bit transmitted by the satellite is estimated anyway in order to know if the choice made at the beginning of the transmission has been right or wrong. Then, this information can be used by the spoofer to try to compensate the mistake.

This attack starts by transmitting a certain symbol by selecting one of the two possible by chance (since a BPSK modulation is used), or by building a counterfeit Navigation Message. If all the bits are chosen by chance, the Navigation Data received by the victim will usually not be consistent, since no real data has been modulated and the information, such as the Ephemerides or clocks, will not show the current position or real offsets of the acquired satellites. This might be solved by generating a manipulated Navigation Message with consistent data, obtaining the data to transmit from other sources.

The peculiarity of this attack respect to the shown in Section 3.2.3.2 is that the amplitudes of the transmitted bits are sometimes not steady all along the entire bit period. In this attack the amplitude of the first μs of the bit , depicted as T_v, is increased above the rest in the following symbol after a wrong transmitted symbol. It means that during a few μs the amplitude increased is higher than the usual amplitude of the symbol. For example, if the transmitted symbol is a +1 symbol, and the amplitude should be +1, in this few μs it will be larger than 1. The window of time T_v where the amplitude is increased is determined by the amount of observation time it is taken by the defendant receiver. Therefore the attacker is free to chose any value of T_v, but the attacker should take into account that as shorter is T_v, the difference between the maximum and minimum amplitude of the signal will be bigger, since the total energy must be the same. After the first samples are increased, the amplitude of the rest of them is reduced below the required level in order to maintain the energy of the transmitted bit equal as if no modification of the signal has been carried out. This procedure is depicted in Figure 3.6. In this Figure Is shown as the amplitude in the first ms has been increased, and after that, the amplitude does not return to 1, but it goes under 1 to maintain the energy of the bit the same as if no modification has been performed.

In Figure 3.7 is represented the form it takes the signal when this attack is performed. We shown as with this attack is performed, there is no constant amplitude of ±1 symbols. The amplitudes takes different values depending on the number of consecutive mistakes, and the signal looks irregular at the beginning of certain symbols.

In parallel of the process of sending a certain symbol, the spoofer estimates in the background the real bit sent by the satellite. After a certain time, the spoofer knows if the bit transmitted by it has been right or wrong. The spoofer then uses this information in the subsequent counterfeit symbols. Of course, this information cannot be used to decide the next symbol, but it can be useful to determine an appropriate amplitude in the first samples of the following symbol. After each wrong guess, the amplitude of the first samples in the next symbol will be doubled (not exactly doubled as it will be shown in the following lines). This means that after two consecutive wrong guesses, the amplitude of the first samples in the next symbol will be increased four times. So, the amplitude will grow exponentially after failing consecutively. After each right guess, the

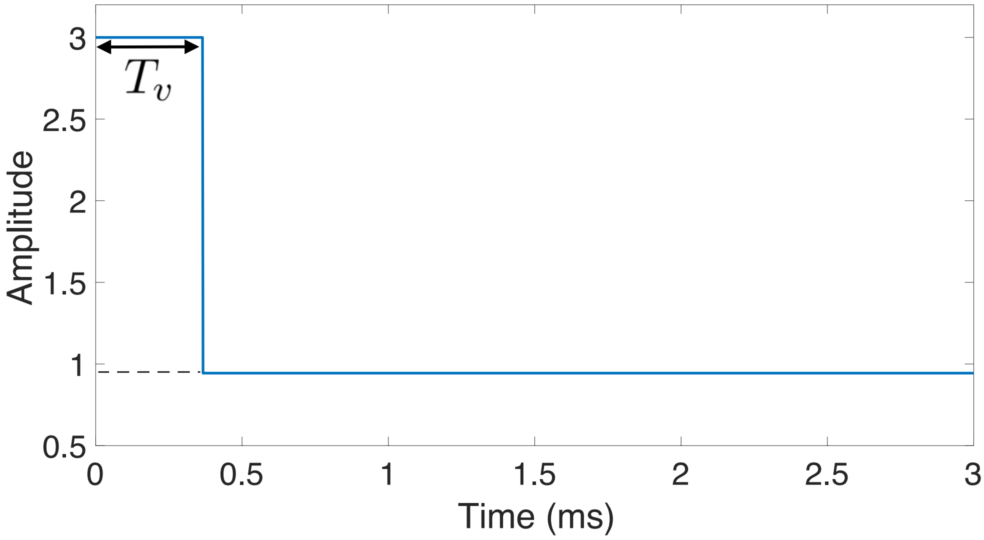


Figure 3.6: Single symbol transmission with increased amplitude and no modification of the energy of the bit.

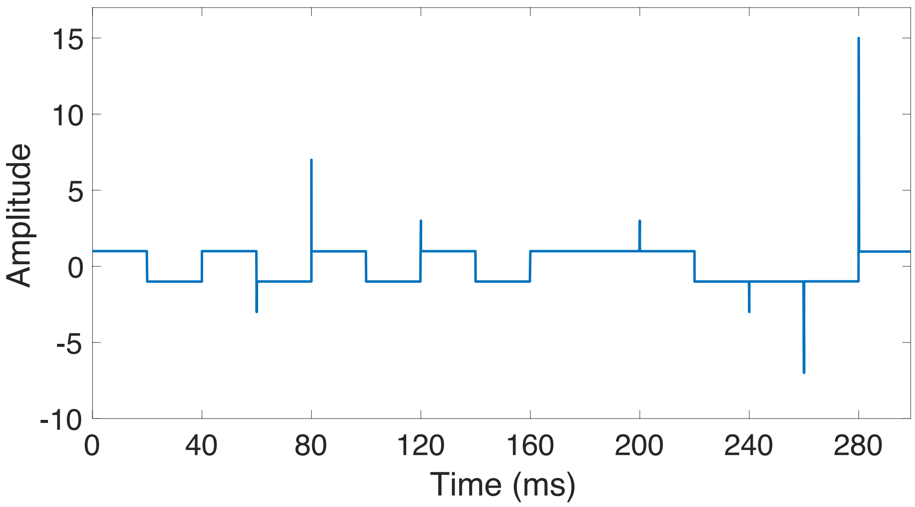


Figure 3.7: Shape of the transmitted signal when the attack Bit-Guess Estimation Technique With Adaptable Amplitude is performed..

amplitude of the subsequent symbol will be restored to the usual amplitude.

In Figure 3.8 an example of this increased amplitude is depicted. Figure 3.8 shows as symbols 1 and 2 are guessed correctly, and no modification of the amplitude in the subsequent bit is required. However, symbol 3 is guessed wrong, and the amplitude of the counterfeit symbol 4 is increased to 3. This value comes from the fact that the new amplitude must compensate the previous errors. For example, in that case we have sent 3 symbols, the last of them wrong, the amplitude of the fourth symbol should be compensated. Therefore, the received energy will be $1 + 1 + 1 - 1 = 2$ due the error, instead of $1 + 1 + 1 + 1 = 4$. If we want to compensate this error, the amplitude of the last symbol should be 3 since $1 + 1 - 1 + 3 = 4$ maintains the same energy as if no mistake has been made. The new amplitude follows the next expression: $2^{(\Delta_E+1)} - 1$, where $\Delta_E = 1, 2, 3, ...$ are the accumulated symbol errors. The amplitudes then fill follow the sequence $1, 3, 7, 15, ...$ if $0, 1, 2, 3, ...$ errors has been made respectively. Following with Figure 3.8, symbol 4 is then guessed correctly, and since the amplitude has been increased by the necessary amount , the error in symbol 3 has been compensated. In symbols 5, 6, 7 and 8 is shown the effect of consecutive wrong guesses. It these cases the amplitude is increased further almost exponentially after each wrong guess.

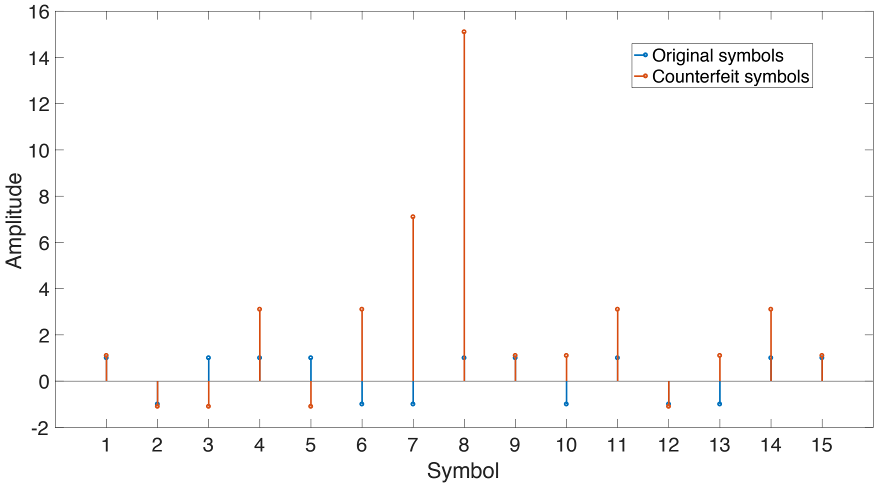
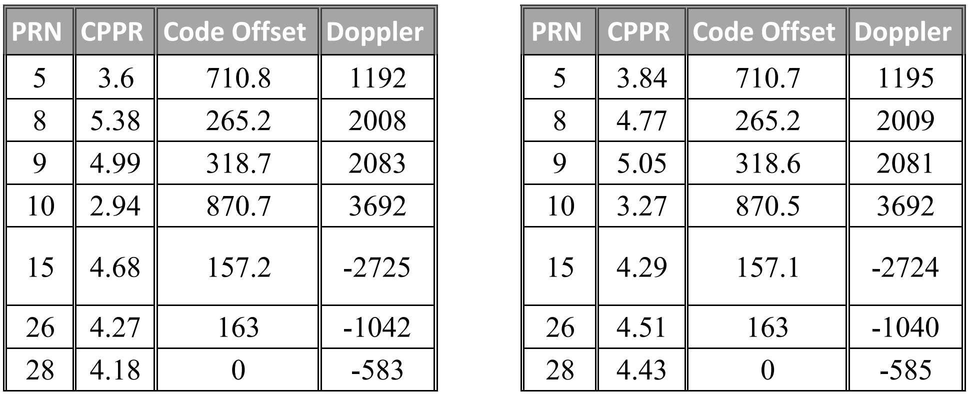


Figure 3.8: Example of increased consecutive symbol amplitudes after wrong bit guesses.

3.3 Counterfeit Signal vs Authentic Signal

In this section are compared the features of the real recorded signal against the spoofer synthetically generated signal of the same recorded signal. The real signal was recorded in the geodesic point located at the Faculty of Veterinary Medicine of the Autonomous University of Barcelona [41° 30′ 14.67152″N, 2° 5′ 57.26627″E] the 12th February 2014. The signal was recorded with a SiGe GN3S Sampler v3 and a computer. Once the signal was recorded, the GPS Software receiver in MATLAB developed by David S. De Lorenzo was used to carry out the acquisition and tracking process. The position solution was determined from the tracking results. To generate the Spoofing signal the GPS Signal Simulator was used, also developed by David S. De Lorenzo, but properly modified to generate the spoofing signal chip-by-chip.

In first place we compare the results after the acquisition process, when as input of the Software receiver are placed the authentic and spoofer signals. In the left part of Table 3.2 are summarized the acquisition results for the authentic signal. Table 3.2 shows the PRN of the satellites acquired, the CPPR (correlation peak to next peak ratio) for each PRN and a first approximation of the code offsets and Doppler frequencies of each acquired satellite for both the authentic and synthetic signal. Comparing both Tables can be observed as the values obtained after the acquisition are very similar in both cases. In both cases has been acquired the same SV with similar CPPR, code offset and Doppler frequency values.



PRN	CPPR	Code Offset	Doppler
5	3.6	710.8	1192
8	5.38	265.2	2008
9	4.99	318.7	2083
10	2.94	870.7	3692
15	4.68	157.2	-2725
26	4.27	163	-1042
28	4.18	0	-583

PRN	CPPR	Code Offset	Doppler
5	3.84	710.7	1195
8	4.77	265.2	2009
9	5.05	318.6	2081
10	3.27	870.5	3692
15	4.29	157.1	-2724
26	4.51	163	-1040
28	4.43	0	-585

Table 3.2: Authentic (left) and spoofing (right) signal Acquisition results.

Regarding the tracking results, Figure 3.9 shows a summary of the main parameters after the tracking process. In Figure 3.9 has only been considered the PRN 10 satellite signal as an example. Comparing both results we can determine that after a certain transition time at the beginning, both signals are practically identical, specially the code offset. The main difference resides on that the C/No level in the spoofer signal is slightly higher. Although the C/No can be controlled by the spoofer. But anyway, in general, both tracking results are practically identical.

Finally, the position solution obtained from the tracking data of the Software Receiver is compared. Comparing the geodesic point coordinates where the data was collected with the coordinates obtained using the tracking data from the Software Receiver can be observed as with both signals are obtained similar results. With the real signal we obtain the position in the coordinates 41° 30 14.7374N 2° 5 57.1472E, and with the spoofer signal in 41° 30 14.6801N 2° 5 57.4565E. Calculating the deviation respect to the real position given by the geodesic point, it gives a deviation of about 2 m in both cases.

In short we could say that both signals are practically identical on the surface, but as we will observe in Chapter 4, the spoofer is under the appearance of normality.

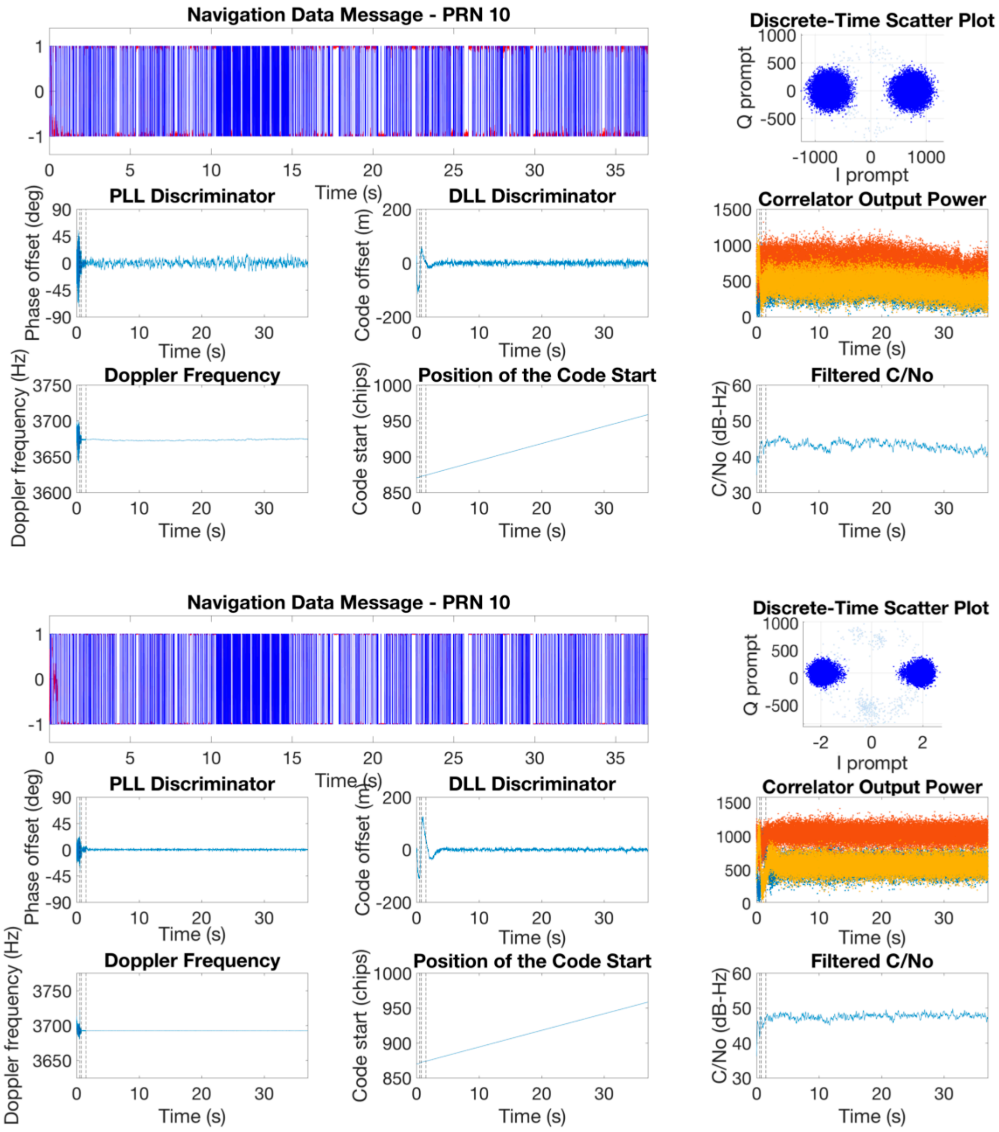


Figure 3.9: Tracking results for the authentic (top) and Spoofing (bottom) PRN 10 signal.

3.4 Symbol Estimation Performance

In this section is presented a brief study about the time required by the spoofer to successfully estimate an unpredictable bit, such as described in Section 3.2 attacks. In Section 3.2 were shown the two symbol estimation strategies that will be taken into account in this document. In the first one, the spoofer estimates the received bits and rebroadcast them back to the victim receiver as soon as the estimation was performed. On the contrary, in the second strategy the spoofer chose randomly (or based on some logic) the bit to send the first N samples, until the bit is likely to be correct. In both cases the estimation process is the same (estimating in the background or using the current estimation), so the results presented in this section are equally valid.

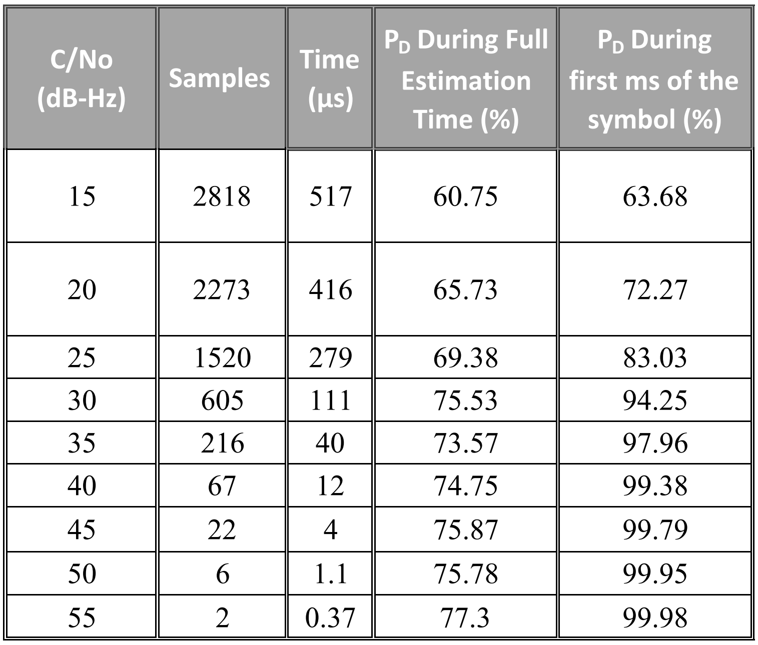
Table 3.3 summarizes the estimation times and number of samples (taking into account the sampling frequency of the receiver, which is 5.456 MHz) needed by the spoofer to successfully estimate D_l. Table 3.3 also shows the probability of correct symbol polarity detection (or probability of Detection, P_d) during the time required to obtain a steady estimation of the symbol and the detection probability during the first millisecond of symbol for different values of C/No.

Table 3.3 shows as in low C/No levels (from 15 to 25 dB-Hz, which can be considered indoor environments [SG12]) the required time for the correct estimation of the symbol sent by the satellite can seem high. The spoofer needs about 2.8-5 ms, depending on the C/No level. But taking into account that a whole bit transmission goes on for 20 ms, the required time actually is quite low, since it only needs to receive less than 25% of the bit transmission in the worse case C/No scenario to estimate the bit correctly. The P_d is about 60-70 % during the time required to make the estimation steady, and between 60-80 % during the first millisecond. All this shows a quite acceptable performance taking into account the low C/No level.

In medium C/No levels (between 25 to 35 dB-Hz, which can be considered soft indoor environments [SG12]) the spoofer needs considerably less time, about 1.5-0.4 ms to estimate correctly the bit, which is translated to about 7.5 % of the total bit transmission time. The P_d in this C/No levels is around 75 % during the time required to make the estimation steady and between 94-99 % during the first millisecond.

Finally, in high C/No (starting from about 35 dB-Hz, which can be considered outdoor environments [SG12]) the required time is really low. The spoofer can determine the transmitted symbol by the satellite in about 1 μs or even less. This time is less than 5 % of the whole bit duration. The P_d is maintained about 75 % during the time required to make the estimation steady, quite similar to lower C/No. However, the P_d is more than 99 % during the first millisecond of transmission. This means that in the first millisecond, almost all the samples will be estimated correctly.

These results shows as an spoofer can estimate correctly and quite quick the symbol transmitted by a satellite, even in indoor environments, where the C/No is relatively low. Table 3.3 also shows that when the spoofer is located in outdoor environments, the required time to estimate the correct symbol is extremely low, since with less than 1 millisecond the spoofer can determine the correct symbol with an excellent P_d of 99 %.



C/No (dB-Hz)	Samples	Time (µs)	P_D During Full Estimation Time (%)	P_D During first ms of the symbol (%)
15	2818	517	60.75	63.68
20	2273	416	65.73	72.27
25	1520	279	69.38	83.03
30	605	111	75.53	94.25
35	216	40	73.57	97.96
40	67	12	74.75	99.38
45	22	4	75.87	99.79
50	6	1.1	75.78	99.95
55	2	0.37	77.3	99.98

Table 3.3: Estimation time for different levels of C/No.

4 Detection Methods

In this section two different detectors are proposed. These defences are focused at signal level, in particular at chip level. They are thought as countermeasures against the attack strategies described in Section 3.2, which are also attacks that modifies the signal at chip level. The detection process is described step-by-step, in order to show the full process a receiver should follow in order to implement the detectors. The first detection technique is described in Section 4.1, and consists in analyse the sign of the accumulated correlation value. The main difference between the first and second technique described in Section 4.2 is that in this case is analysed the full correlation value instead just the sign.

The detection process is summarized in Figure 4.1. Basically the steps consist in:

1. The signal coming from te satellite is received by the attacker receiver. In this receiver is performed the attack, where the bits are estimated if apply. For more information about the attacks see Chapter 3. After modify the signal, the attacker rebroadcasts the signal to the victim.

2. After the signal reaches the victim's receiver, it stores a certain number of samples of the beginning and ending of each received bit. Or in other words, it stores the first and last portion of each bit. This is shown in step 1 of Figure 4.1, where a coloured dashed line corresponds to the amount time the victim is storing. This time-window is chosen by the victim depending on its capabilities and the performance that wants to be achieved. The time-window could be a few μs or even some ms. As well as the portions of signal are stored, the associated locally generated PRN code replica is also stored, which will be used to despread the signal further.

3. The received signal is despread using the associated PRN local replica. After despreading the signal we get a value for each bit, as shown in step 2 of Figure 4.1. This is done separately for both the first and last part of each bit, obtaining a value for each part.

4. Then each value of β is correlated with the bit after 20 ms estimation, which in fact is the true bit transmitted by the satellite.

5. In step 4 of Figure 4.1, the detection method, which will be described next, is applied.

6. Finally, in step 5 of Figure 4.1 the results to determine if the signal is likely to be authentic or counterfeit are analysed. If the mean of Ω is close to 1 will mean that is likely the signal is authentic, since there are very few differences between both edges of the bit. On the contrary, as closer Ω is from zero will mean that the probability that the signal is counterfeit is higher.

4.1 Detection Method 1: Sign Correlation Ratio (SCR) Detection Technique

This detection method is based on the knowledge of the bit once it has completely been received. Since the bit is known, it can be correlated by the sign of the first an last correlation values of each received bit. First of all we need to obtain the correlation values for each bit as

$$\begin{aligned} \beta_{First} &= \sum_{n=1}^{N_W} Y_{First}(n) C_{First}(n), \\ \beta_{Last} &= \sum_{n=1}^{N_W} Y_{Last}(n) C_{Last}(n), \end{aligned} \tag{4.1}$$

Where $Y_{First}(n)$ and $Y_{Last}(n)$ are the part of the received down-converted signal corresponding to the first and last part of the bit, and $C_{First}(n)$ and $C_{Last}(n)$ corresponds to the matched aligned PRN code replica for a single satellite from the total set of N satellites. N_w is the number of samples the receiver stores for each edge of the bit. N_{Bit} is the total number of samples per bit ($N_{Bit} = \frac{F_s}{1e{-}3} \cdot 20$ [samples/millisecond], where F_s is the sampling frequency of the receiver and 20 samples/millisecond is due to the duration of a single bit in ms) and $T = N_{Bit} - N_W$ is the number of samples stored in the final part of the bit. This initial process corresponds to steps 1 and 2 of Figure **??**, where the process is depicted for some bits with different colours for the first and last part of each bit.

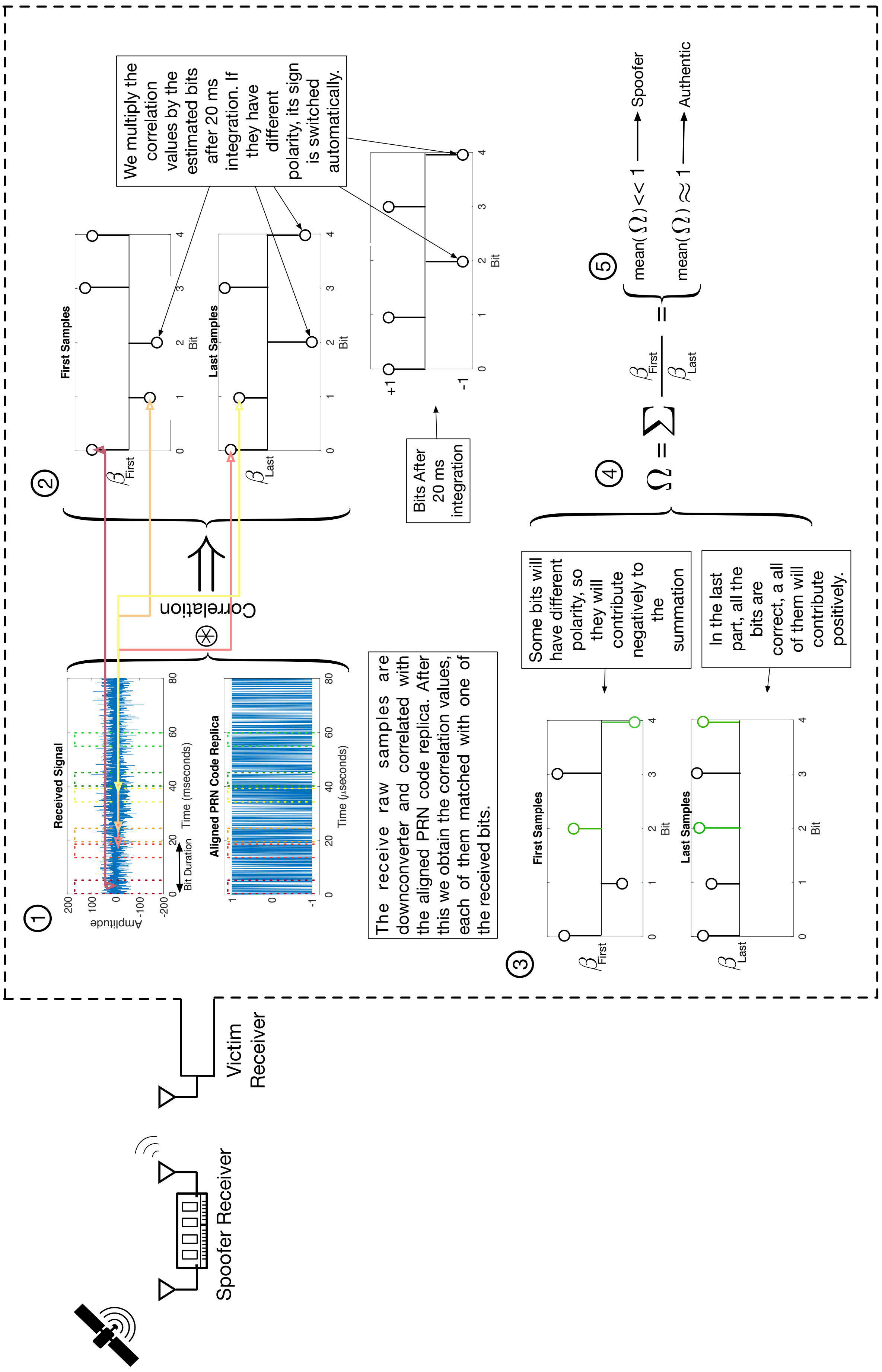
After this, the spoofer correlates the values β_{First} and β_{Last} by the estimated bit after 20 ms integration, which in fact is the true bit transmitted by the satellite. With this correlation by the true bit what we achieve is that if the sign of β_{First} and β_{Last} is wrong, these values will contribute negatively to the detection. On the contrary the bits that has the same sign will contribute positively. This process can be summarized as

$$\Omega = \sum_{b=1}^{B} \frac{\sum_{n=1}^{N_W} sign\left(\beta_{First}(n)^{(b)}\right) \cdot \mu^{(b)}}{\sum_{n=1}^{N_W} sign\left(\beta_{Last}(n)^{(b)}\right) \cdot \mu^{(b)}}, \tag{4.2}$$

where $\mu^{(b)}$ corresponds to the set of received bits -1, 1, $b = 1, 2, 3...B$ is the number of bits and $sign(\cdot)$ is the sign function, whose output is 1 if the input value is positive, or -1 if the input value is negative.

Checking the value Ω takes we can be determine the presence of spoofer. If Ω is close to 1 means that, in principle, the signal is authentic, since most of the sign of both edges of the analysed bits will be approximately the same. On the contrary, if Ω is much lower than 1 means that the signal is likely to be counterfeit. During the correlation by $\mu^{(b)}$, if the signal is authentic the result will be approximately to the number of bits B considered in the correlation. So both numerator and denominator will be approximately B. On the contrary, if the signal is counterfeit, the denominator will be approximately B (since the bit in this point is equal as the authentic), but the numerator will be far below from this value.

The correlation in 4.2 carried out for B bits, could be performed for a reduced number defined as P $P = \frac{B}{J}$, giving as a results some values of Ω. For example considering $B = 2000$, we could determine that $J = 100$, and then instead of receive a single value of Ω after correlate B bits, we would obtain P values of Ω. With this set of Ω's we can be perform a statistical analysis to determine the presence of spoofer based on an hypothesis test. The values of Ω can be fitted in a Gaussian Probability Density Function (PDF), in which can be computed the Detection and False Alarm Probabilities (P_D and P_{FA}, respectively). This will be described in Section 4.3.



The receive raw samples are downconverter and correlated with the aligned PRN code replica. After this we obtain the correlation values, each of them matched with one of the received bits.

We multiply the correlation values by the estimated bits after 20 ms integration. If they have different polarity, its sign is switched automatically.

Bits After 20 ms integration

Some bits will have different polarity, so they will contribute negatively to the summation

In the last part, all the bits are correct, a all of them will contribute positively.

$$\Omega = \sum \frac{\beta_{\text{First}}}{\beta_{\text{Last}}} = \begin{cases} \text{mean}(\Omega) << 1 \longrightarrow \text{Spoofer} \\ \text{mean}(\Omega) \approx 1 \longrightarrow \text{Authentic} \end{cases}$$

Figure 4.1: Illustration of the steps to implement the Detectors 2 and 3.

4.2 Detection Method 2: Total Correlation Ratio (TCR) Detection Technique

This method is very similar to the presented in last Section 4.1. Actually, the only difference with the last one is the use of the full information provided by the correlation value, instead of using only the sign information. Removing the $sign(\cdot)$ function in (4.2) we obtain

$$\Omega = \sum_{b=1}^{B} \frac{\sum_{n=1}^{N_W} \beta_{First}(n)^{(b)} \cdot \mu^{(b)}}{\sum_{n=1}^{N_W} \beta_{Last}(n)^{(b)} \cdot \mu^{(b)}}, \tag{4.3}$$

Similarly as before, if the value of Ω is close to 1, both correlation values are approximately equal, and therefore the bit has no instabilities. On the contrary, if the value of Ω is much lower than 1, the magnitude of both correlation values is much different, and thus the signal has been probably modified. In this case the correlation makes use of the full information provided by the amplitude, not just the sign.

4.3 Gaussian PDF Detection Process

The set of values in the vector Ω can be fitted into a Gaussian PDF, as has been already said in previous Sections. The average process is done in order to obtain smoother values of mean and sigma to compute the PDF. The most likely value (the mean of the Gaussian PDF) corresponds to mean value of Ω. Figure 4.2) shows two examples of PDF fitting for two different signals. In the top plot is depicted an example where the spoofer cannot be detected. The green area, which is the Detection probability (P_D) is very low compared to the False Alarm probability (P_{FA}) depicted in Orange. In turn, the probability of Missed Detection (depicted in blue, which in fact is $P_D -$ 1) is very big. Thus, the spoofer cannot be detected with enough certainty. On the contrary, in the example on the bottom part is depicted an example where the spoofer can easily be detected. The example on the bottom part shows as the mean of the spoofer PDF is close to zero, far away from the mean of the reference PDF that is close to 1. The P_D is larger than the P_{FA}, and hence the spoofer can be detected better than in previous case. The threshold has been set in the middle of both PDF's only as an example. This threshold can be moved along the different values, producing that P_D and P_{FA} vary as well.

The two hypothesis to detect the spoofer are the next

$$x \sim \begin{cases} H_0 : f_0(x) \rightarrow Spoofer\ Detected \\ H_1 : f_1(x) \rightarrow Spoofer\ Not\ Detected\ (Authentic\ Signal) \end{cases}, \tag{4.4}$$

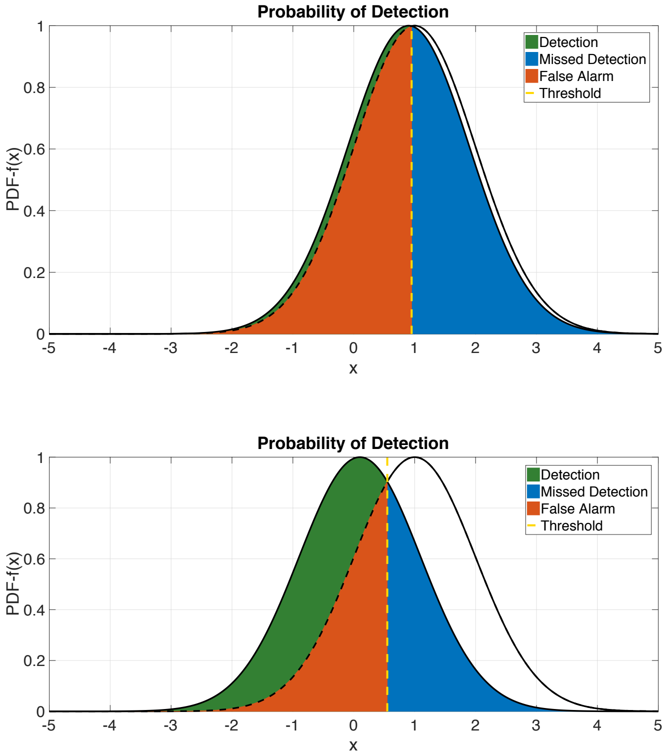


Figure 4.2: PDF comparison fitted from Ω. In the top are compared two authentic signals. On the bottom are compared the spoofer signal and and authentic signal.

where x denotes the data set; H_0 and H_1 are the two hypothesis; and f_0 and f_1 are the PDF's obtained from Ω when the signal contains spoofer and when it is authentic.

5 Results

In this section is analysed the accuracy of the detection methods described in Chapter 4 applying the attack strategies described in Section 3.2. The performance of the detectors is tested in a wide variety of conditions and situations. First of all, in Section 5.1 the results of the detection methods described in Chapter 4 when they are applied to an authentic signal are summarized. This results considers different levels of C/No and number of satellites in the signal, as well as different victim's receiver observation times. The results from the authentic signal will give us a reference to compare when the detection methods are carried out against counterfeit signals.

Then, in the following sections are summarized the results using the same detection techniques, but this time against signals under the attacks described in Section 3.2. The results are summarized in Section 5.2. For each case are considered different levels of C/No, number of satellites in the signal, different observation times of the victim receiver and different C/No levels of the attacker. The attacker C/No contributes enormously to the accuracy and quickness of the estimation time of the bits, as it is shown in Section 3.2.

For both cases, the spoofer and authentic signal, the same parameters has been taken into account to analyse the signal:

- C/No levels: We have chosen the following C/No levels: 45 dB-Hz, 40 dB-Hz, 35 dB-Hz and 30 dB-Hz. These C/No levels are used in both the spoofer and victim receivers. These values has been chosen since they represent common values in outdoor environments, in good (40 dB-Hz and 45 dB-Hz) and bad conditions (35 dB-Hz and 30 dB-Hz) [SG12]. Depending on the C/No level in the spoofer receiver, the spoofer will be able to estimate better or worse the received bits, since the attacker's C/No contributes enormously to the accuracy and quickness of the estimation time of the bits. This is shown in Section 3.2. The different C/No levels in the victim receiver will show the effect of the noise in the detection performance.
- Number of satellites present in the signal: We have taken into account three cases. When there are present 1, 3 and 6 SV's in the analysed signal. This is done with the objective of showing the cross correlation effects in the detection performance by increasing the

number of PRN sequences.

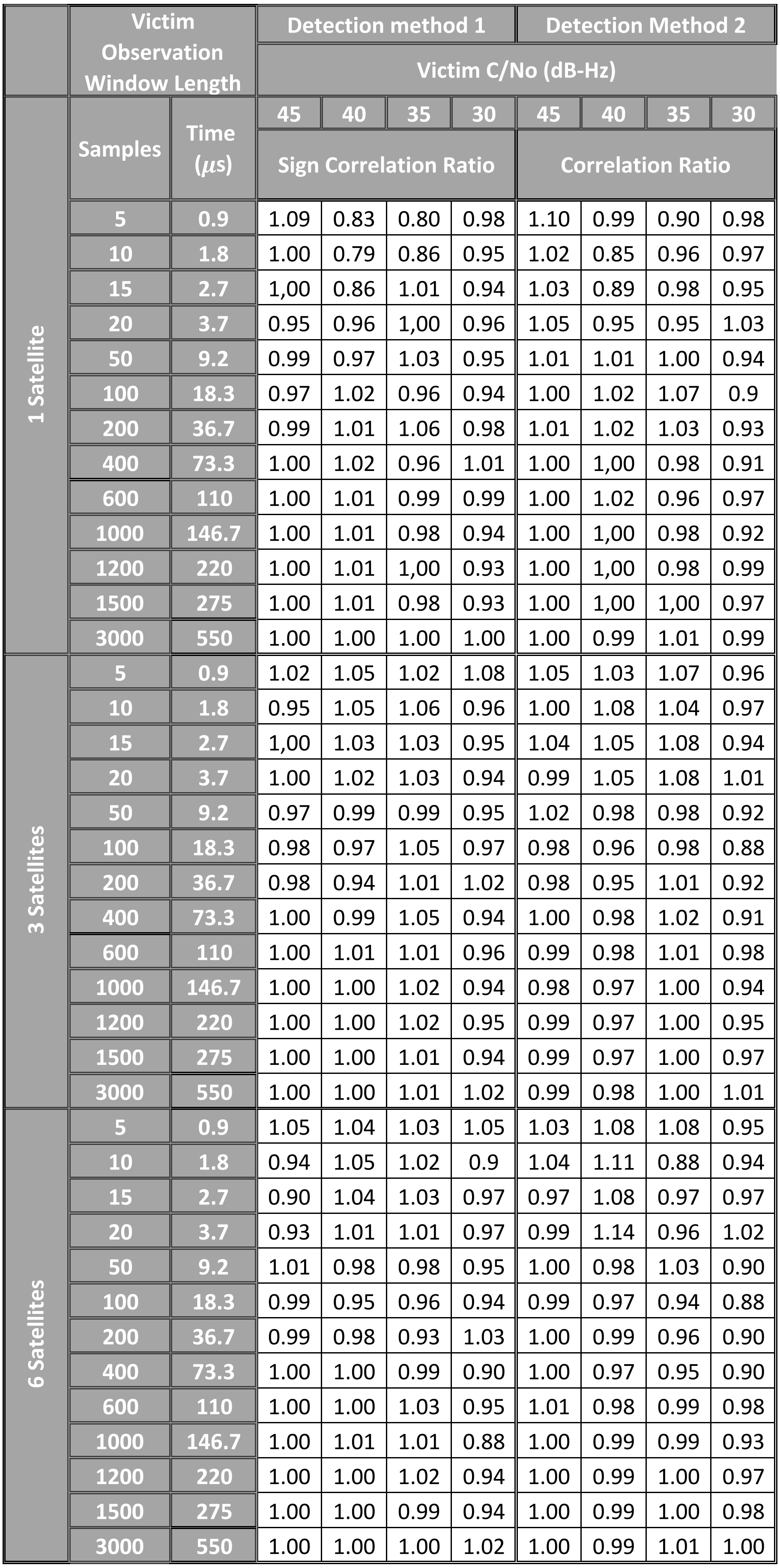
- Victim observation time: Different observation times has been taken into account, starting from only 0.9 μs (5 samples) to 550 μs (3000 samples). This observation time means the number of samples the victim receiver will store in order to carry out the detection techniques and be able to detect the spoofer presence. The reason of using this wide variety of observation times is because we want to show the trade off between the accuracy of the detection method and the accuracy of the bit estimation from the received samples.
- Number of Bits: To obtain the results has been taken into account 2000 bits (B=2000). The results have been averaged in blocks of 100 bits when the average process is performed.

Finally, in Section 5.3 the ROC (Receiver Operation Characteristic) for some of the detectors obtained from detection method 1 is shown.

5.1 Reference Performance: Results Against Authentic Signals

Table 5.1 summarizes the results of the different detection methods against an authentic signal. Table 5.1 shows the reference values, which we can compare later to the obtained against the spoofer, in order to determine if an attacker is present in the analysed signal. In Table 5.1 we observe the following features:

- **Detection Technique 1:** The first detection method makes use of the symbol received and the sign of the correlation value. This method correlates and accumulates both along the B bits received. Against an authentic signal this method shows In all the cases a ratio around 1, which means that the signal is authentic. Since both correlation values have the same sign, the accumulation of thee values will give as a results a similar value, whose ratio is about 1.
- **Detection Technique 2:** This method differed from the last one in the use of the full accumulated correlation value, instead of only the sign. The results against an authentic signal shows again that the ratio should be about 1, as expected, since both values will be similar in magnitude, since the signal has not been modified.



	Victim Observation Window Length		Detection method 1				Detection Method 2			
			Victim C/No (dB-Hz)							
	Samples	Time (μs)	45	40	35	30	45	40	35	30
			Sign Correlation Ratio				Correlation Ratio			
1 Satellite	5	0.9	1.09	0.83	0.80	0.98	1.10	0.99	0.90	0.98
	10	1.8	1.00	0.79	0.86	0.95	1.02	0.85	0.96	0.97
	15	2.7	1,00	0.86	1.01	0.94	1.03	0.89	0.98	0.95
	20	3.7	0.95	0.96	1,00	0.96	1.05	0.95	0.95	1.03
	50	9.2	0.99	0.97	1.03	0.95	1.01	1.01	1.00	0.94
	100	18.3	0.97	1.02	0.96	0.94	1.00	1.02	1.07	0.9
	200	36.7	0.99	1.01	1.06	0.98	1.01	1.02	1.03	0.93
	400	73.3	1.00	1.02	0.96	1.01	1.00	1,00	0.98	0.91
	600	110	1.00	1.01	0.99	0.99	1.00	1.02	0.96	0.97
	1000	146.7	1.00	1.01	0.98	0.94	1.00	1,00	0.98	0.92
	1200	220	1.00	1.01	1,00	0.93	1.00	1,00	0.98	0.99
	1500	275	1.00	1.01	0.98	0.93	1.00	1,00	1,00	0.97
	3000	550	1.00	1.00	1.00	1.00	1.00	0.99	1.01	0.99
3 Satellites	5	0.9	1.02	1.05	1.02	1.08	1.05	1.03	1.07	0.96
	10	1.8	0.95	1.05	1.06	0.96	1.00	1.08	1.04	0.97
	15	2.7	1,00	1.03	1.03	0.95	1.04	1.05	1.08	0.94
	20	3.7	1.00	1.02	1.03	0.94	0.99	1.05	1.08	1.01
	50	9.2	0.97	0.99	0.99	0.95	1.02	0.98	0.98	0.92
	100	18.3	0.98	0.97	1.05	0.97	0.98	0.96	0.98	0.88
	200	36.7	0.98	0.94	1.01	1.02	0.98	0.95	1.01	0.92
	400	73.3	1.00	0.99	1.05	0.94	1.00	0.98	1.02	0.91
	600	110	1.00	1.01	1.01	0.96	0.99	0.98	1.01	0.98
	1000	146.7	1.00	1.00	1.02	0.94	0.98	0.97	1.00	0.94
	1200	220	1.00	1.00	1.02	0.95	0.99	0.97	1.00	0.95
	1500	275	1.00	1.00	1.01	0.94	0.99	0.97	1.00	0.97
	3000	550	1.00	1.00	1.01	1.02	0.99	0.98	1.00	1.01
6 Satellites	5	0.9	1.05	1.04	1.03	1.05	1.03	1.08	1.08	0.95
	10	1.8	0.94	1.05	1.02	0.9	1.04	1.11	0.88	0.94
	15	2.7	0.90	1.04	1.03	0.97	0.97	1.08	0.97	0.97
	20	3.7	0.93	1.01	1.01	0.97	0.99	1.14	0.96	1.02
	50	9.2	1.01	0.98	0.98	0.95	1.00	0.98	1.03	0.90
	100	18.3	0.99	0.95	0.96	0.94	0.99	0.97	0.94	0.88
	200	36.7	0.99	0.98	0.93	1.03	1.00	0.99	0.96	0.90
	400	73.3	1.00	1.00	0.99	0.90	1.00	0.97	0.95	0.90
	600	110	1.00	1.00	1.03	0.95	1.01	0.98	0.99	0.98
	1000	146.7	1.00	1.01	1.01	0.88	1.00	0.99	0.99	0.93
	1200	220	1.00	1.00	1.02	0.94	1.00	0.99	1.00	0.97
	1500	275	1.00	1.00	0.99	0.94	1.00	0.99	1.00	0.98
	3000	550	1.00	1.00	1.00	1.02	1.00	0.99	1.01	1.00

5.2 Performance Results Against Counterfeit Signals

In this section the results for the different detection techniques described in Chapter 4 against the attack strategies described in Chapter 3 are depicted. In each one of the Tables 5.2 -5.4 and 5.6 - 5.8 the same parameters are considered as the used in Section 5.1, except that in this case is added a new one, which is named attacker C/No. This attacker C/No represents the C/No level of the signal received by the spoofer. Depending on this value, the spoofer will be able to estimate the received symbols quicker or slower, such as is described in Section 3.4.

Each value in the Tables 5.2 -5.4 and 5.6 - 5.8 match to a different simulation that corresponds to a certain level of Spoofer C/No, victim C/No and victim observation time. Each value is plotted in three different colours, depending on the detection performance achieved. This is done in order to make the tables more readable. Red values mean that in such cases cannot be determined the presence or not presence of spoofer in the signal. This means that in the conditions with red numbers, the spoofer could not be detected. Orange means that there is only slightly differences between the results with and without spoofer, and that thus it is highly probable to consider a real signal when it is a counterfeit signal and the other way around. Finally, the green values mean that the spoofer can be detected with a high degree of success.

5.2.1 Detection Technique 1: Total Sign Correlation Ratio Detection Technique Results

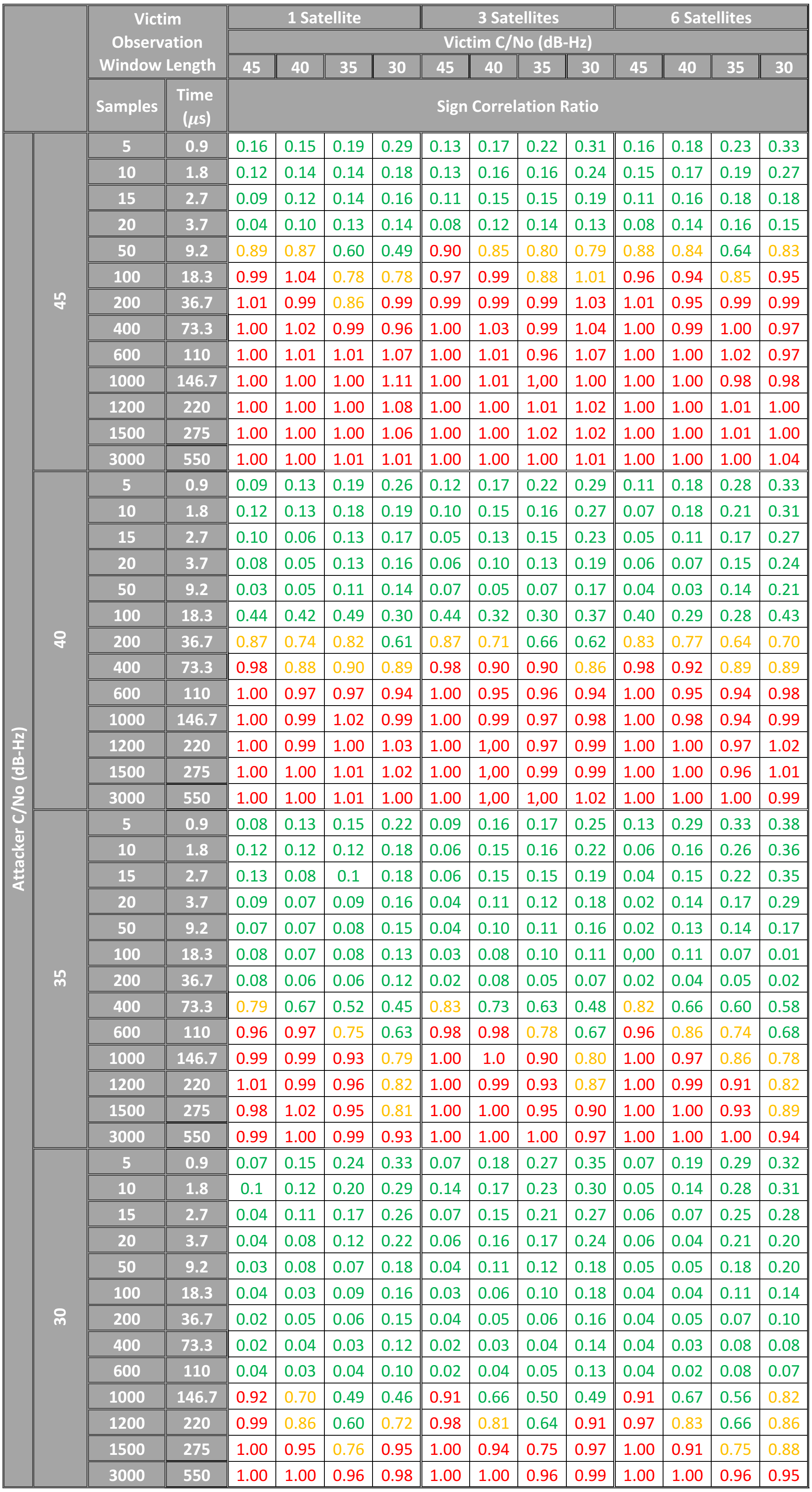
In Tables 5.2, 5.3 and 5.4 the results against the attack Chip-By-Chip Estimation, Bit Guess Estimation and FEA attack, respectively, are summarized against the Total Sign Correlation Ratio Detection Technique. In such Tables, the mean of the Gaussian PDF obtained after applying the process described in Section 4.1 is shown. The values of sigma σ^2 are not present in Tables 5.2-5.4, since they are all very similar (between 0.3 and 0.01, depending on the window length used (σ^2 is lower as the window length becomes larger).

Table 5.2 summarizes the results against the attack Chip-By-Chip Estimation. The victim is able to detect the attack even when the attacker is well placed (and has a high C/No) and his estimation is very quick. In this case the victim can detect the attack during approximately the first 50 μs. During this time the ratio falls to about 0.1, instead of 1 when the signal is authentic. At the same time that the spoofer C/No gets lower, the observation time by which the victim is able to detect the attack gets larger. For example when the attacker C/No is 40 dB-Hz, the victim has about 70 μs to detect te attack. When the attacker C/No is the lowest of the considered, the victim is able to detect the attack during almost 1000 μs. Considering that it takes 100 μs about to estimate the bit an attacker with 30 dB-Hz of C/No, the attack can be detected far beyond the modified samples. Looking at Table 5.2 we observe that in general, the best window length the victim uses is the one that stores the full amount of time where the spoofer still does not know which polarity should send, since the bit has still not been estimated correctly, and the attacker is sending both at the same time (some samples with one polarity, and some other samples with the other). This occurs because when the victim stores the full unsteady transmission of the spoofer, the summation of the samples are minimum and the samples are practically compensated one each other (since the mean value is asymptotically close zero). So the ratio between the first an last samples is minimum. On the contrary, if the selected window goes far beyond the spoofer unsteady transmission, the spoofer effect starts to disappear because the victim stores more steady samples with the correct bit than unsteady ones. In addition, looking at Table 5.2 we do not observe too much differences between having 1 or 6 satellites in the signal. So the cross-correlation effects does not affects too much the detection performance. The differences between having 1 or 6 satellites turns out into an increase of the ratio lower than 0.1.

Table 5.3 gathers the detection results against attack strategy Bit Guess Estimation. This method shows similar results compared with the detection performance obtained against the Chip-By-Chip Estimation strategy showed in Table 5.2.

Finally, Table 5.4 shows the results of this detection method against FEA. By looking at the results superficially, we observe that the detection performance is not very high. The main problem with this attack and detection technique is that we are only taking the sign of the correlation values, disregarding the amplitude. So we are losing some valuable information, more important in this attack than in the others. We also observe that this time the ratios are much larger than 1. The reason of it is because during the FEA attacks, the attacker increases the amplitude of the following bit after each incorrect guessed symbol (only during the beginning of the symbol, see Section 3.2.4 for more details). As the spoofer increases the amplitude of some symbols (and this is more pronounced after consecutive wrong guesses), when the ratio between the first and last samples is computed, the result is higher than 1. The reason is because the first samples value will be much larger than the last samples value, due to the increase in amplitude of the first samples. With this method, the spoofer effects are larger compared with the other two detection methods, due to the big increase in amplitude during the first samples of some symbols after consecutive bit wrong guesses.

Table 5.5 shows a brief comparison between the performance results with detection method 3. In this comparison has only been taken into account the case when 6 satellites are present in the signal and for 45 dB/Hz and 30 dB/Hz of C/No. Table 5.5 that attacks 1 and 2 are the easiest to detect, and are also detectable during more time.



		Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
				Victim C/No (dB-Hz)											
				45	40	35	30	45	40	35	30	45	40	35	30
		Samples	Time (μs)	Sign Correlation Ratio											
Attacker C/No (dB-Hz)	45	5	0.9	0.16	0.15	0.19	0.29	0.13	0.17	0.22	0.31	0.16	0.18	0.23	0.33
		10	1.8	0.12	0.14	0.14	0.18	0.13	0.16	0.16	0.24	0.15	0.17	0.19	0.27
		15	2.7	0.09	0.12	0.14	0.16	0.11	0.15	0.15	0.19	0.11	0.16	0.18	0.18
		20	3.7	0.04	0.10	0.13	0.14	0.08	0.12	0.14	0.13	0.08	0.14	0.16	0.15
		50	9.2	0.89	0.87	0.60	0.49	0.90	0.85	0.80	0.79	0.88	0.84	0.64	0.83
		100	18.3	0.99	1.04	0.78	0.78	0.97	0.99	0.88	1.01	0.96	0.94	0.85	0.95
		200	36.7	1.01	0.99	0.86	0.99	0.99	0.99	0.99	1.03	1.01	0.95	0.99	0.99
		400	73.3	1.00	1.02	0.99	0.96	1.00	1.03	0.99	1.04	1.00	0.99	1.00	0.97
		600	110	1.00	1.01	1.01	1.07	1.00	1.01	0.96	1.07	1.00	1.00	1.02	0.97
		1000	146.7	1.00	1.00	1.00	1.11	1.00	1.01	1,00	1.00	1.00	1.00	0.98	0.98
		1200	220	1.00	1.00	1.00	1.08	1.00	1.00	1.01	1.02	1.00	1.00	1.01	1.00
		1500	275	1.00	1.00	1.00	1.06	1.00	1.00	1.02	1.02	1.00	1.00	1.01	1.00
		3000	550	1.00	1.00	1.01	1.01	1.00	1.00	1.00	1.01	1.00	1.00	1.00	1.04
	40	5	0.9	0.09	0.13	0.19	0.26	0.12	0.17	0.22	0.29	0.11	0.18	0.28	0.33
		10	1.8	0.12	0.13	0.18	0.19	0.10	0.15	0.16	0.27	0.07	0.18	0.21	0.31
		15	2.7	0.10	0.06	0.13	0.17	0.05	0.13	0.15	0.23	0.05	0.11	0.17	0.27
		20	3.7	0.08	0.05	0.13	0.16	0.06	0.10	0.13	0.19	0.06	0.07	0.15	0.24
		50	9.2	0.03	0.05	0.11	0.14	0.07	0.05	0.07	0.17	0.04	0.03	0.14	0.21
		100	18.3	0.44	0.42	0.49	0.30	0.44	0.32	0.30	0.37	0.40	0.29	0.28	0.43
		200	36.7	0.87	0.74	0.82	0.61	0.87	0.71	0.66	0.62	0.83	0.77	0.64	0.70
		400	73.3	0.98	0.88	0.90	0.89	0.98	0.90	0.90	0.86	0.98	0.92	0.89	0.89
		600	110	1.00	0.97	0.97	0.94	1.00	0.95	0.96	0.94	1.00	0.95	0.94	0.98
		1000	146.7	1.00	0.99	1.02	0.99	1.00	0.99	0.97	0.98	1.00	0.98	0.94	0.99
		1200	220	1.00	0.99	1.00	1.03	1.00	1,00	0.97	0.99	1.00	1.00	0.97	1.02
		1500	275	1.00	1.00	1.01	1.02	1.00	1,00	0.99	0.99	1.00	1.00	0.96	1.01
		3000	550	1.00	1.00	1.01	1.00	1.00	1,00	1,00	1.02	1.00	1.00	1.00	0.99
	35	5	0.9	0.08	0.13	0.15	0.22	0.09	0.16	0.17	0.25	0.13	0.29	0.33	0.38
		10	1.8	0.12	0.12	0.12	0.18	0.06	0.15	0.16	0.22	0.06	0.16	0.26	0.36
		15	2.7	0.13	0.08	0.1	0.18	0.06	0.15	0.15	0.19	0.04	0.15	0.22	0.35
		20	3.7	0.09	0.07	0.09	0.16	0.04	0.11	0.12	0.18	0.02	0.14	0.17	0.29
		50	9.2	0.07	0.07	0.08	0.15	0.04	0.10	0.11	0.16	0.02	0.13	0.14	0.17
		100	18.3	0.08	0.07	0.08	0.13	0.03	0.08	0.10	0.11	0,00	0.11	0.07	0.01
		200	36.7	0.08	0.06	0.06	0.12	0.02	0.08	0.05	0.07	0.02	0.04	0.05	0.02
		400	73.3	0.79	0.67	0.52	0.45	0.83	0.73	0.63	0.48	0.82	0.66	0.60	0.58
		600	110	0.96	0.97	0.75	0.63	0.98	0.98	0.78	0.67	0.96	0.86	0.74	0.68
		1000	146.7	0.99	0.99	0.93	0.79	1.00	1.0	0.90	0.80	1.00	0.97	0.86	0.78
		1200	220	1.01	0.99	0.96	0.82	1.00	0.99	0.93	0.87	1.00	0.99	0.91	0.82
		1500	275	0.98	1.02	0.95	0.81	1.00	1.00	0.95	0.90	1.00	1.00	0.93	0.89
		3000	550	0.99	1.00	0.99	0.93	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.94
	30	5	0.9	0.07	0.15	0.24	0.33	0.07	0.18	0.27	0.35	0.07	0.19	0.29	0.32
		10	1.8	0.1	0.12	0.20	0.29	0.14	0.17	0.23	0.30	0.05	0.14	0.28	0.31
		15	2.7	0.04	0.11	0.17	0.26	0.07	0.15	0.21	0.27	0.06	0.07	0.25	0.28
		20	3.7	0.04	0.08	0.12	0.22	0.06	0.16	0.17	0.24	0.06	0.04	0.21	0.20
		50	9.2	0.03	0.08	0.07	0.18	0.04	0.11	0.12	0.18	0.05	0.05	0.18	0.20
		100	18.3	0.04	0.03	0.09	0.16	0.03	0.06	0.10	0.18	0.04	0.04	0.11	0.14
		200	36.7	0.02	0.05	0.06	0.15	0.04	0.05	0.06	0.16	0.04	0.05	0.07	0.10
		400	73.3	0.02	0.04	0.03	0.12	0.02	0.03	0.04	0.14	0.04	0.03	0.08	0.08
		600	110	0.04	0.03	0.04	0.10	0.02	0.04	0.05	0.13	0.04	0.02	0.08	0.07
		1000	146.7	0.92	0.70	0.49	0.46	0.91	0.66	0.50	0.49	0.91	0.67	0.56	0.82
		1200	220	0.99	0.86	0.60	0.72	0.98	0.81	0.64	0.91	0.97	0.83	0.66	0.86
		1500	275	1.00	0.95	0.76	0.95	1.00	0.94	0.75	0.97	1.00	0.91	0.75	0.88
		3000	550	1.00	1.00	0.96	0.98	1.00	1.00	0.96	0.99	1.00	1.00	0.96	0.95

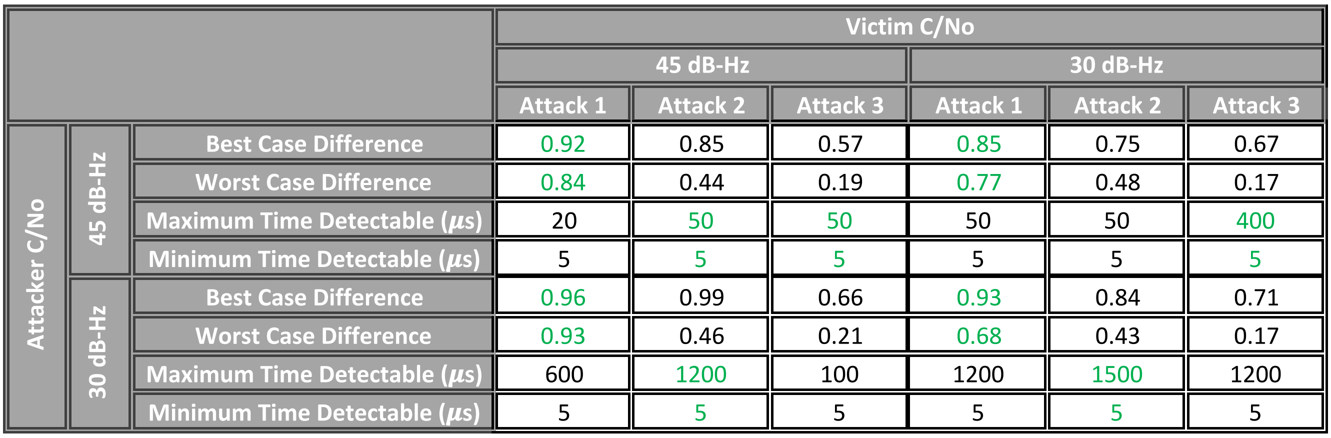
Table 5.2: Results of the Bit Sign Correlation Detection Technique against attack Chip-By-Chip Estimation strategy.

		Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
				Victim C/No (dB-Hz)											
				45	40	35	30	45	40	35	30	45	40	35	30
		Samples	Time (μs)	Correlation Ratio											
Attacker C/No (dB-Hz)	45	5	0.9	0.13	0.17	0.23	0.22	0.12	0.19	0.21	0.23	0.08	0.2	0.23	0.23
		10	1.8	0.10	0.14	0.18	0.17	0.11	0.18	0.19	0.17	0.12	0.18	0.19	0.19
		15	2.7	0.10	0.13	0.14	0.14	0.08	0.15	0.17	0.16	0.10	0.16	0.18	0.18
		20	3.7	0.08	0.11	0.09	0.15	0.07	0.14	0.11	0.15	0.09	0.15	0.14	0.15
		50	9.2	0.88	0.94	0.56	0.78	0.85	0.80	0.57	0.77	0.92	0.88	0.60	0.79
		100	18.3	0.94	0.98	0.65	0.88	0.96	0.93	0.72	0.8	0.96	0.91	0.81	0.85
		200	36.7	0.97	1.00	0.84	0.96	0.98	0.98	0.89	1.02	1,00	0.97	0.95	0.84
		400	73.3	0.98	1.03	0.97	0.99	0.98	1.01	0.94	1.03	0.99	1,00	0.99	0.91
		600	110	0.98	1.00	0.99	1.03	0.98	1.00	0.94	1.01	1.00	1.01	1.01	0.91
		1000	146.7	0.99	1.00	0.98	1.04	0.99	1.01	0.98	1.01	1.00	1.01	1.01	0.94
		1200	220	0.99	1.01	0.98	1.02	1.00	1.00	0.99	1.01	0.99	1.01	1.00	0.96
		1500	275	0.99	1.01	0.99	1.02	1.00	1.00	1.00	0.99	1.00	1.01	1.00	0.98
		3000	550	1.00	1.00	1.00	1.01	1.00	1.00	1.01	0.99	1.00	1.01	0.99	1.00
	40	5	0.9	0.11	0.21	0.21	0.18	0.13	0.18	0.19	0.21	0.12	0.18	0.28	0.26
		10	1.8	0.10	0.16	0.16	0.18	0.08	0.17	0.14	0.18	0.07	0.04	0.17	0.23
		15	2.7	0.09	0.12	0.11	0.16	0.07	0.13	0.14	0.17	0.05	0.08	0.18	0.22
		20	3.7	0.08	0.12	0.10	0.13	0.04	0.07	0.13	0.15	0.04	0.07	0.18	0.18
		50	9.2	0.01	0.07	0.12	0.11	0.05	0.05	0.06	0.12	0.02	0.03	0.14	0.15
		100	18.3	0.33	0.36	0.39	0.43	0.35	0.32	0.32	0.53	0.32	0.30	0.34	0.57
		200	36.7	0.65	0.68	0.76	0.79	0.68	0.65	0.60	0.77	0.67	0.70	0.63	0.78
		400	73.3	0.82	0.82	0.87	0.87	0.85	0.81	0.82	0.89	0.83	0.83	0.85	0.89
		600	110	0.88	0.88	0.93	0.93	0.89	0.87	0.88	0.95	0.88	0.88	0.88	0.97
		1000	146.7	0.93	0.92	0.99	0.99	0.94	0.92	0.96	0.98	0.92	0.93	0.91	0.99
		1200	220	0.94	0.93	0.98	0.98	0.95	0.93	0.98	1.01	0.94	0.94	0.93	1.02
		1500	275	0.95	0.95	0.98	1.01	0.96	0.95	0.98	1.02	0.94	0.95	0.94	1,00
		3000	550	0.97	0.96	1.00	1.00	0.98	0.97	0.99	0.99	0.98	0.97	0.98	0.99
	35	5	0.9	0.08	0.18	0.19	0.18	0.11	0.21	0.21	0.23	0.09	0.23	0.20	0.25
		10	1.8	0.07	0.12	0.16	0.17	0.08	0.15	0.18	0.20	0.03	0.13	0.16	0.24
		15	2.7	0.11	0.10	0.15	0.15	0.06	0.10	0.17	0.18	0.02	0.10	0.16	0.23
		20	3.7	0.09	0.09	0.12	0.12	0.04	0.09	0.14	0.17	0.02	0.09	0.15	0.21
		50	9.2	0.08	0.08	0.10	0.09	0.02	0.08	0.11	0.16	0.01	0.08	0.08	0.10
		100	18.3	0.09	0.07	0.11	0.07	0.02	0.08	0.08	0.09	0,00	0.07	0.08	0.03
		200	36.7	0.08	0,00	0.05	0.10	0,00	0.07	0.03	0.06	0.01	0.04	0.04	0.11
		400	73.3	0.49	0.46	0.50	0.49	0.50	0.53	0.52	0.52	0.51	0.53	0.53	0.57
		600	110	0.67	0.71	0.69	0.66	0.66	0.75	0.68	0.63	0.66	0.68	0.70	0.71
		1000	146.7	0.79	0.83	0.83	0.79	0.8	0.86	0.8	0.77	0.80	0.81	0.82	0.79
		1200	220	0.81	0.91	0.86	0.80	0.83	0.92	0.84	0.81	0.83	0.85	0.83	0.83
		1500	275	0.87	0.98	0.87	0.82	0.86	0.98	0.86	0.83	0.87	0.88	0.86	0.87
		3000	550	0.94	1.01	0.94	0.9	0.93	0.97	0.95	0.92	0.94	0.93	0.93	0.92
	30	5	0.9	0.07	0.08	0,00	0.13	0.08	0.053	0.07	0,00	0.07	0.05	0.131	0.15
		10	1.8	0.06	0.05	0.028	0.1	0.11	0.07	0.17	0,00	0.03	0.07	0.12	0.14
		15	2.7	0.04	0.01	0.03	0.09	0.09	0.09	0.14	0.03	0.05	0.03	0.06	0.08
		20	3.7	0.04	0.09	0.017	0.08	0.07	0.14	0.09	0.10	0.03	0.02	0.06	0.09
		50	9.2	0.02	0.04	0.12	0.08	0.04	0.08	0.1	0.01	0.04	0.04	0.05	0.12
		100	18.3	0.01	0.04	0.07	0.06	0.02	0.06	0.02	0.10	0.02	0.04	0.08	0.06
		200	36.7	0.01	0.02	0.05	0.07	0.02	0.04	0.02	0.02	0.02	0.03	0.05	0.07
		400	73.3	0.01	0.03	0.02	0.06	0.01	0.02	0.04	0.05	0.01	0.02	0.04	0.07
		600	110	0.01	0.02	0.02	0.05	0.01	0.02	0.03	0.07	0.01	0.01	0.05	0.06
		1000	146.7	0.41	0.39	0.39	0.67	0.40	0.40	0.40	0.67	0.40	0.40	0.43	0.79
		1200	220	0.51	0.49	0.48	0.78	0.50	0.49	0.49	0.90	0.50	0.50	0.52	0.82
		1500	275	0.61	0.59	0.59	0.89	0.60	0.59	0.59	0.92	0.59	0.60	0.60	0.84
		3000	550	0.81	0.79	0.79	0.95	0.80	0.79	0.81	0.95	0.8	0.79	0.81	0.92

Table 5.3: Results of the Bit Sign Correlation Detection Technique against Bit-Guess Estimation strategy.

		Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
				Victim C/No (dB-Hz)											
				45	40	35	30	45	40	35	30	45	40	35	30
		Samples	Time (μs)	Sign Correlation Ratio											
Attacker C/No (dB-Hz)	45	5	0.9	2.22	3.22	3.16	2.87	2.59	3.45	3.76	3.07	2.33	4.17	4.91	2.48
		10	1.8	1.79	2.44	5.28	3.69	1.96	2.88	2.53	3.08	1.84	3.91	3.78	3.04
		15	2.7	1.62	2.07	4.42	3.53	1.85	2.33	2.17	3.69	1.63	3.88	4.12	2.49
		20	3.7	1.44	2.29	3.60	2.78	1.59	2.34	2.12	3.10	1.63	4.38	4.48	2.59
		50	9.2	1.21	1.73	2.22	2.25	1.24	1.66	1.88	2.79	1.23	2.05	2.15	1.62
		100	18.3	1.07	1.29	1.76	1.6	1.09	1.28	1.76	1.49	1.08	1.67	1.65	1.39
		200	36.7	1.02	1.16	1.31	1.42	1.03	1.15	1.5	1.35	1.02	1.22	1.65	1.34
		400	73.3	1.00	1.07	1.18	1.21	1.00	1.05	1.27	1.14	1.01	1.05	1.24	1.21
		600	110	1.00	1.02	1.11	1.13	1.00	1.02	1.21	1.09	1.00	1.03	1.12	1.11
		1000	146.7	1.00	1.01	1.08	1.09	1.00	1.01	1.18	1.04	1.00	1.01	1.03	1.03
		1200	220	1.00	1.00	1.04	1.06	1.00	1.00	1.13	1.02	1.00	1.01	1.03	1.00
		1500	275	1.00	1.00	1.03	1.04	1.00	1.00	1.04	1.03	1.00	1.00	1.01	1.00
		3000	550	1.00	1.00	1.01	1.02	1.00	1.00	1.04	1.00	1.00	1.00	1.02	1.00
	40	5	0.9	2.49	3.86	4.38	3.83	3.24	3.25	3.63	3.81	3.34	4.88	4.23	3.11
		10	1.8	2.01	3.35	4.49	3.89	1.93	3.13	4.28	3.75	2.06	3.22	3.35	3.60
		15	2.7	1.64	2.71	4.16	3.06	1.62	3.43	3.98	3.11	1.74	4.33	4.26	3.15
		20	3.7	1.52	2.27	4.04	4.65	1.45	2.55	3.73	4.18	1.57	2.84	3.83	4.07
		50	9.2	1.17	1.65	2.34	2.88	1.27	1.90	2.83	3.09	1.38	1.72	2.29	4.45
		100	18.3	1.06	1.41	1.80	2.24	1.08	1.42	1.89	2.92	1.12	1.47	1.60	3.79
		200	36.7	1.02	1.17	1.39	1.59	1.02	1.18	1.66	2.09	1.09	1.17	1.46	1.91
		400	73.3	1.00	1.06	1.16	1.48	1,00	1.06	1.34	1.37	1.03	1.06	1.12	1.54
		600	110	1.00	1.02	1.09	1.27	1,00	1.03	1.15	1.26	1.03	1.02	1.12	1.34
		1000	146.7	1.00	1,00	1.04	1.12	0.99	1.01	1.09	1.12	1.00	1.01	1.06	1.26
		1200	220	1.00	1.00	1.02	1.13	0.99	1.00	1.06	1.08	1.00	1.00	1.06	1.25
		1500	275	1.00	1.00	1.01	1.06	0.99	1.00	1.04	1.06	1.00	1.00	1.03	1.16
		3000	550	1.00	1.00	1.01	1.00	0.99	1.00	1.01	1.03	1.00	1.00	1.00	1.04
	35	5	0.9	2.20	3.64	4.12	3.37	2.40	3.76	4.17	3.45	2.76	3.72	3.67	3.31
		10	1.8	1.83	2.6	4.01	3.94	1.79	2.68	4.08	3.88	2.10	3.28	3.98	3.62
		15	2.7	1.73	2.54	2.75	2.87	1.71	2.61	2.86	2.75	1.88	3.40	2.50	2.69
		20	3.7	1.54	1.93	2.44	2.35	1.63	2.01	2.48	2.43	1.62	3.01	3.02	2.58
		50	9.2	1.25	1.69	2.30	2.07	1.30	1.83	2.37	2.18	1.28	1.92	2.23	2.16
		100	18.3	1.10	1.36	2.17	2.02	1.12	1.41	2.21	2.12	1.10	1.58	1.73	2.10
		200	36.7	1.03	1.17	1.47	1.93	1.04	1.18	1.62	1.98	1.01	1.24	1.51	1.93
		400	73.3	1.00	1.09	1.22	1.62	1.00	1.12	1.33	1.65	1,00	1.08	1.16	1.60
		600	110	1.00	1.04	1.18	1.37	1.00	1.09	1.24	1.42	1,00	1.04	1.12	1.38
		1000	146.7	1.00	1.01	1.09	1.24	1.00	1.02	1.11	1.27	0.99	1.00	1.04	1.20
		1200	220	1.00	1.00	1.08	1.23	1.00	1.07	1.09	1.25	0.99	1.00	1.04	1.22
		1500	275	1.00	1.00	1.06	1.16	1.00	1.03	1.03	1.15	0.99	1.00	1.01	1.12
		3000	550	1.00	1.00	1.00	1.07	1.00	1,00	0.99	1.05	0.99	1.00	1.00	1.02
	30	5	0.9	2.27	7.21	1.59	3.42	2.35	6.71	1.80	3.55	2.91	3.04	1.83	3.42
		10	1.8	1.95	5.12	3.66	3.31	1.80	3.38	2.80	3.14	2.11	2.49	2.67	3.08
		15	2.7	1.69	3.03	4.60	2.45	1.71	2.23	3.63	2.75	1.95	2.09	2.78	2.54
		20	3.7	1.63	2.38	3.67	2.03	1.63	2.25	3.45	2.16	2.00	2.35	3.27	2.24
		50	9.2	1.28	1.67	2.33	1.97	1.31	1.57	2.39	2.06	1.44	1.56	2.65	2.11
		100	18.3	1.13	1.53	1.83	1.99	1.12	1.31	1.75	2.20	1.26	1.42	1.87	2.17
		200	36.7	1.04	1.22	1.51	1.86	1.04	1.16	1.43	1.92	1.10	1.19	1.49	1.86
		400	73.3	1.00	1.08	1.32	1.74	0.99	1.03	1.31	1.71	1.02	1.09	1.34	1.77
		600	110	1.00	1.04	1.20	1.68	0.99	1,00	1.22	1.61	1.00	1.03	1.27	1.63
		1000	146.7	0.99	1.00	1.13	1.50	0.99	0.98	1.11	1.4	0.99	1.02	1.14	1.37
		1200	220	0.99	0.99	1.07	1.42	0.99	0.98	1.04	1.37	0.99	1.01	1.09	1.21
		1500	275	0.99	1.00	1.05	1.28	0.99	0.97	1.02	1.25	0.99	1.00	1.04	1.11
		3000	550	0.99	1.00	1.00	1.15	0.99	0.98	1.03	1.11	0.99	1.00	0.99	1.01

Table 5.4: Results of the detection method 2 against FEA attack.



			Victim C/No					
			45 dB-Hz			30 dB-Hz		
			Attack 1	Attack 2	Attack 3	Attack 1	Attack 2	Attack 3
Attacker C/No	45 dB-Hz	Best Case Difference	0.92	0.85	0.57	0.85	0.75	0.67
		Worst Case Difference	0.84	0.44	0.19	0.77	0.48	0.17
		Maximum Time Detectable (μs)	20	50	50	50	50	400
		Minimum Time Detectable (μs)	5	5	5	5	5	5
	30 dB-Hz	Best Case Difference	0.96	0.99	0.66	0.93	0.84	0.71
		Worst Case Difference	0.93	0.46	0.21	0.68	0.43	0.17
		Maximum Time Detectable (μs)	600	1200	100	1200	1500	1200
		Minimum Time Detectable (μs)	5	5	5	5	5	5

Table 5.5: Comparison results with Detection Method 1. The results corresponds when 6 satellites are present in the signal.

5.2.2 Detection Technique 2: Total Correlation Ratio Detection Technique Results

In Tables 5.6, 5.7 and 5.8 the results against the three considered attack strategies are summarized when the Total Correlation Ratio detection technique is carried out. The main difference of using this detection method instead the last one is the fact that in this case is used the full correlation value instead of only the sign information. In this occasion sigma σ^2 was between 0.01 and 0.05 .

Table 5.6 shows the obtained results against the attack strategy Chip-By-Chip Estimation. Table 5.6 shows excellent results against this attack. This method shows as the attack can be detected with enough certainty in any condition of victim C/No and number of satellites. Even when the spoofer has high C/No, the victim is able to detect the spoofer. In addition, the attack can be detected after the spoofer is transmitting the correct bit. The minimum values reached with this method are practically zero. From only taking 0.9 μs of signal, the spoofer can be detected with enough certainty, since the mean obtained is about 0.1. Taking more samples of spoofing attack, this values decreases to 0.01, since more samples are available to carry out the correlation.

Table 5.7 shows the results against the attack strategy Bit-Guess Estimation. Looking at Table 5.7 we can observe as, in general, the results are quite similar as the shown in Table 5.7 in last Section. Although using the full information of the correlation value the performance is slightly better (the ratios where the spoofer can be detected are lower and closer to zero). The values are about 0.1 lower in practically all the cases. In addition, the ratio does not recovers so quickly to 1 after the attack. So the victim has a little bit more time to detect the spoofer.

Finally, in Table 5.8 the results against the FEA attack are shown. Total Correlation Ratio Detection Technique behaves excellent against FEA attacks. Superficially the results are quite similar as the shown against the other attacks. Although the ratio is slightly higher (around 0.2), but only when short observation window lengths are used. In addition, the window lengths number by which the victim can detect the spoofer has increased compared with the other two attacks. This is due to the fact that this method modifies more severely the amplitudes (above all after consecutive wrong guesses) than with the other two methods. So to return the nminal value it needs more time, since the difference in amplitude between both edges of the bit will be greater.

Table 5.9 shows a brief comparison between the performance results with detection method 3. In this comparison has only been taken into account the case when 6 satellites are present in the signal and for 45 dB/Hz and 30 dB/Hz of C/No. Table 5.9 shows that the easiest attack method to detect is the strategy 1 and 2, but not too far from the 3. On the contrary, the strategy attack 3 can be detected during more time.

		Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
				Victim C/No (dB-Hz)											
				45	40	35	30	45	40	35	30	45	40	35	30
		Samples	Time (μs)	Correlation Ratio											
Attacker C/No (dB-Hz)	45	5	0.9	0.17	0.15	0.16	0.20	0.18	0.15	0.15	0.21	0.18	0.18	0.16	0.23
		10	1.8	0.11	0.13	0.13	0.19	0.13	0.14	0.12	0.18	0.15	0.15	0.14	0.19
		15	2.7	0.08	0.08	0.11	0.18	0.10	0.10	0.12	0.16	0.11	0.12	0.14	0.18
		20	3.7	0.07	0.08	0.09	0.15	0.08	0.09	0.11	0.15	0.09	0.08	0.12	0.17
		50	9.2	0.58	0.55	0.57	0.67	0.59	0.58	0.59	0.69	0.59	0.59	0.60	0.69
		100	18.3	0.87	0.88	0.77	0.83	0.93	0.94	0.91	0.89	0.94	0.96	0.86	0.77
		200	36.7	0.98	0.96	0.89	0.94	0.97	1.00	0.94	0.96	0.98	0.99	1.00	0.98
		400	73.3	0.98	0.98	0.91	0.98	1.00	1.01	1.02	0.99	1.00	1.01	1.02	1.03
		600	110	1.00	1.00	0.92	0.99	1.00	1.00	1.01	0.98	1.01	1.00	0.99	1.07
		1000	146.7	1.00	1.00	0.94	0.94	0.99	1.01	1.01	1.02	1.00	1.00	1.00	1.07
		1200	220	1.00	1.01	0.95	0.98	1.00	1.00	1.01	1.00	1.00	0.99	1.00	1.07
		1500	275	1.00	1.02	0.96	0.95	0.99	1.00	1.00	0.99	0.99	0.99	0.98	1.04
		3000	550	1.00	1.00	0.98	0.98	1.00	1.01	1.01	0.98	1.00	0.99	0.97	1.02
	40	5	0.9	0.18	0.14	0.18	0.23	0.16	0.15	0.19	0.23	0.19	0.17	0.21	0.24
		10	1.8	0.10	0.12	0.16	0.21	0.11	0.13	0.17	0.22	0.11	0.14	0.18	0.19
		15	2.7	0.09	0.06	0.15	0.17	0.09	0.08	0.14	0.15	0.08	0.09	0.16	0.17
		20	3.7	0.09	0.06	0.14	0.14	0.06	0.08	0.14	0.14	0.05	0.08	0.14	0.15
		50	9.2	0.05	0.01	0.08	0.11	0.06	0.08	0.08	0.13	0.03	0.06	0.12	0.14
		100	18.3	0.34	0.35	0.43	0.43	0.37	0.34	0.48	0.49	0.31	0.31	0.51	0.52
		200	36.7	0.66	0.70	0.73	0.73	0.67	0.67	0.72	0.79	0.66	0.64	0.68	0.83
		400	73.3	0.83	0.85	0.86	0.88	0.85	0.85	0.85	0.91	0.83	0.82	0.86	0.94
		600	110	0.89	0.90	0.93	0.93	0.90	0.90	0.92	0.96	0.90	0.89	0.92	0.98
		1000	146.7	0.93	0.93	0.92	0.92	0.94	0.94	0.95	0.99	0.93	0.95	0.95	1.02
		1200	220	0.94	0.94	0.93	0.93	0.95	0.95	0.97	0.98	0.94	0.96	0.95	1.01
		1500	275	0.95	0.95	0.94	0.94	0.95	0.96	0.97	1.02	0.95	0.97	0.96	1.00
		3000	550	0.98	0.98	0.99	0.99	0.97	0.97	0.98	1.00	0.98	0.98	0.98	0.99
	35	5	0.9	0.16	0.12	0.18	0.23	0.18	0.14	0.19	0.25	0.16	0.15	0.21	0.26
		10	1.8	0.12	0.13	0.16	0.21	0.14	0.13	0.18	0.22	0.08	0.09	0.19	0.23
		15	2.7	0.09	0.07	0.09	0.18	0.11	0.11	0.15	0.18	0.08	0.07	0.12	0.19
		20	3.7	0.06	0.06	0.06	0.17	0.08	0.08	0.08	0.16	0.05	0.05	0.12	0.18
		50	9.2	0.03	0.05	0.07	0.13	0.04	0.06	0.06	0.14	0.05	0.03	0.04	0.15
		100	18.3	0.02	0.02	0.03	0.12	0.03	0.04	0.07	0.13	0.04	0.01	0.05	0.14
		200	36.7	0.01	0.02	0.04	0.10	0.01	0.02	0.03	0.11	0.03	0.03	0.05	0.12
		400	73.3	0.48	0.48	0.49	0.52	0.49	0.48	0.50	0.50	0.50	0.49	0.50	0.52
		600	110	0.76	0.65	0.67	0.69	0.77	0.68	0.66	0.68	0.68	0.65	0.72	0.75
		1000	146.7	0.92	0.80	0.80	0.86	0.95	0.86	0.78	0.83	0.81	0.80	0.85	0.85
		1200	220	0.98	0.88	0.89	0.98	0.99	0.90	0.88	0.97	0.93	0.93	0.88	0.98
		1500	275	0.99	0.97	0.96	0.99	0.99	0.98	0.94	0.99	0.99	0.96	0.97	0.98
		3000	550	1.00	1.02	1.02	0.98	1.01	1.00	1.02	1.02	1.03	1.03	0.98	0.99
	30	5	0.9	0.15	0.12	0.16	0.19	0.15	0.07	0.16	0.19	0.08	0.19	0.18	0.21
		10	1.8	0.08	0.12	0.14	0.18	0.13	0.08	0.15	0.18	0.04	0.07	0.16	0.20
		15	2.7	0.08	0.15	0.12	0.18	0.11	0.06	0.16	0.16	0.04	0.06	0.13	0.18
		20	3.7	0.04	0.11	0.11	0.15	0.07	0.05	0.14	0.14	0.02	0.07	0.12	0.17
		50	9.2	0.01	0.06	0.03	0.14	0.02	0.07	0.07	0.14	0.03	0.07	0.10	0.16
		100	18.3	0.01	0.06	0.03	0.13	0.02	0.02	0.03	0.12	0.02	0.03	0.08	0.13
		200	36.7	0.00	0.04	0.04	0.12	0.02	0.03	0.02	0.10	0.02	0.04	0.06	0.11
		400	73.3	0.01	0.03	0.03	0.08	0.01	0.02	0.03	0.09	0.01	0.03	0.03	0.10
		600	110	0.01	0.02	0.03	0.07	0.01	0.02	0.02	0.08	0.01	0.02	0.03	0.08
		1000	146.7	0.39	0.41	0.40	0.46	0.41	0.43	0.44	0.48	0.44	0.46	0.47	0.49
		1200	220	0.49	0.51	0.49	4.64	0.51	0.52	0.53	0.55	0.52	0.52	0.53	0.58
		1500	275	0.59	0.61	0.61	0.69	0.65	0.66	0.67	0.69	0.66	0.67	0.68	0.71
		3000	550	0.80	0.81	0.83	0.85	0.87	0.88	0.89	0.91	0.89	0.90	0.94	1.06

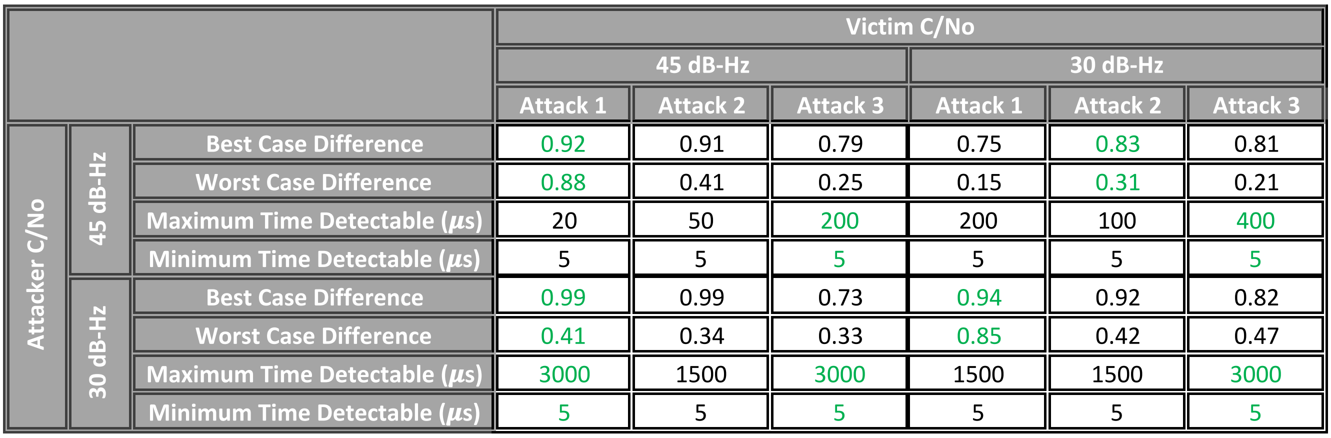
Table 5.6: Results of the Correlation Amplitude Check Detection Technique against attack Chip-By-Chip Estimation strategy.

Attacker C/No (dB-Hz)	Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
			Victim C/No (dB-Hz)											
			45	40	35	30	45	40	35	30	45	40	35	30
	Samples	Time (μs)	Correlation Ratio											
45	5	0.9	0.17	0.15	0.16	0.2	0.18	0.15	0.15	0.21	0.18	0.18	0.16	0.23
	10	1.8	0.11	0.13	0.13	0.19	0.13	0.14	0.12	0.18	0.15	0.15	0.14	0.19
	15	2.7	0.08	0.08	0.11	0.18	0.1	0.1	0.12	0.16	0.11	0.12	0.14	0.18
	20	3.7	0.07	0.08	0.09	0.15	0.08	0.09	0.11	0.15	0.09	0.08	0.12	0.17
	50	9.2	0.58	0.55	0.57	0.67	0.59	0.58	0.59	0.69	0.59	0.59	0.6	0.69
	100	18.3	0.87	0.88	0.77	0.83	0.93	0.94	0.91	0.89	0.94	0.96	0.86	0.77
	200	36.7	0.98	0.96	0.89	0.94	0.97	1,00	0.94	0.96	0.98	0.99	1,00	0.98
	400	73.3	0.98	0.98	0.91	0.98	1,00	1.01	1.02	0.99	1,00	1.01	1.02	1.03
	600	110	1,00	1,00	0.92	0.99	1,00	1,00	1.01	0.98	1.01	1,00	0.99	1.07
	1000	146.7	1,00	1,00	0.94	0.94	0.99	1.01	1.01	1.02	1,00	1,00	1,00	1.07
	1200	220	1,00	1.01	0.95	0.98	1,00	1,00	1.01	1,00	1,00	0.99	1,00	1.07
	1500	275	1,00	1.02	0.96	0.95	0.99	1,00	1,00	0.99	0.99	0.99	0.98	1.04
	3000	550	1,00	1,00	0.98	0.98	1,00	1.01	1.01	0.98	1,00	0.99	0.97	1.02
40	5	0.9	0.18	0.14	0.18	0.23	0.16	0.15	0.19	0.23	0.19	0.17	0.21	0.24
	10	1.8	0.1	0.12	0.16	0.21	0.11	0.13	0.17	0.22	0.11	0.14	0.18	0.19
	15	2.7	0.09	0.06	0.15	0.17	0.09	0.08	0.14	0.15	0.08	0.09	0.16	0.17
	20	3.7	0.09	0.06	0.14	0.14	0.06	0.08	0.14	0.14	0.05	0.08	0.14	0.15
	50	9.2	0.05	0.01	0.08	0.11	0.06	0.08	0.08	0.13	0.03	0.06	0.12	0.14
	100	18.3	0.34	0.35	0.43	0.43	0.37	0.34	0.48	0.49	0.31	0.31	0.51	0.52
	200	36.7	0.66	0.7	0.73	0.73	0.67	0.67	0.72	0.79	0.66	0.64	0.68	0.83
	400	73.3	0.83	0.85	0.86	0.88	0.85	0.85	0.85	0.91	0.83	0.82	0.86	0.94
	600	110	0.89	0.9	0.93	0.93	0.9	0.9	0.92	0.96	0.9	0.89	0.92	0.98
	1000	146.7	0.93	0.93	0.92	0.92	0.94	0.94	0.95	0.99	0.93	0.95	0.95	1.02
	1200	220	0.94	0.94	0.93	0.93	0.95	0.95	0.97	0.98	0.94	0.96	0.95	1.01
	1500	275	0.95	0.95	0.94	0.94	0.95	0.96	0.97	1.02	0.95	0.97	0.96	1,00
	3000	550	0.98	0.98	0.99	0.99	0.97	0.97	0.98	1,00	0.98	0.98	0.98	0.99
35	5	0.9	0.16	0.12	0.18	0.23	0.18	0.14	0.19	0.25	0.16	0.15	0.21	0.26
	10	1.8	0.12	0.13	0.16	0.21	0.14	0.13	0.18	0.22	0.08	0.09	0.19	0.23
	15	2.7	0.09	0.07	0.09	0.18	0.11	0.11	0.15	0.18	0.08	0.07	0.12	0.19
	20	3.7	0.06	0.06	0.06	0.17	0.08	0.08	0.08	0.16	0.05	0.05	0.12	0.18
	50	9.2	0.03	0.05	0.07	0.13	0.04	0.06	0.06	0.14	0.05	0.03	0.04	0.15
	100	18.3	0.02	0.02	0.03	0.12	0.03	0.04	0.07	0.13	0.04	0.01	0.05	0.14
	200	36.7	0.01	0.02	0.04	0.1	0.01	0.02	0.03	0.11	0.03	0.03	0.05	0.12
	400	73.3	0.48	0.48	0.49	0.52	0.49	0.48	0.5	0.5	0.5	0.49	0.5	0.52
	600	110	0.76	0.65	0.67	0.69	0.77	0.678	0.66	0.68	0.68	0.65	0.72	0.75
	1000	146.7	0.92	0.8	0.8	0.86	0.95	0.86	0.78	0.83	0.81	0.8	0.85	0.85
	1200	220	0.98	0.88	0.89	0.98	0.99	0.9	0.88	0.97	0.93	0.93	0.88	0.98
	1500	275	0.99	0.97	0.96	0.99	0.99	0.98	0.94	0.99	0.99	0.96	0.97	0.98
	3000	550	1,00	1.02	1.02	0.98	1.01	1,00	1.02	1.02	1.03	1.03	0.98	0.99
30	5	0.9	0.15	0.12	0.164	0.19	0.15	0.07	0.16	0.19	0.08	0.19	0.18	0.21
	10	1.8	0.08	0.12	0.14	0.18	0.13	0.08	0.15	0.18	0.04	0.07	0.16	0.2
	15	2.7	0.08	0.15	0.12	0.18	0.11	0.06	0.16	0.16	0.04	0.06	0.13	0.18
	20	3.7	0.04	0.11	0.11	0.15	0.07	0.05	0.14	0.14	0.02	0.07	0.12	0.17
	50	9.2	0.01	0.06	0.03	0.14	0.02	0.07	0.07	0.14	0.03	0.07	0.1	0.16
	100	18.3	0.01	0.06	0.03	0.13	0.02	0.02	0.03	0.12	0.02	0.03	0.08	0.13
	200	36.7	0,00	0.04	0.04	0.12	0.02	0.03	0.02	0.1	0.02	0.04	0.06	0.11
	400	73.3	0.01	0.03	0.03	0.08	0.01	0.02	0.03	0.09	0.01	0.03	0.03	0.1
	600	110	0.01	0.02	0.03	0.07	0.01	0.02	0.02	0.08	0.01	0.02	0.03	0.08
	1000	146.7	0.39	0.41	0.4	0.46	0.41	0.43	0.44	0.48	0.44	0.46	0.47	0.49
	1200	220	0.49	0.51	0.49	4.64	0.51	0.52	0.53	0.55	0.52	0.52	0.53	0.58
	1500	275	0.59	0.61	0.61	0.69	0.65	0.66	0.67	0.69	0.66	0.67	0.68	0.71
	3000	550	0.8	0.81	0.83	0.85	0.87	0.88	0.89	0.91	0.89	0.9	0.94	1.06

Table 5.7: Results of the Correlation Amplitude Check Detection Technique against Bit-Guess Estimation strategy.

		Victim Observation Window Length		1 Satellite				3 Satellites				6 Satellites			
				Victim C/No (dB-Hz)											
				45	40	35	30	45	40	35	30	45	40	35	30
		Samples	Time (μs)	Correlation Ratio											
Attacker C/No (dB-Hz)	45	5	0.9	4.24	4.61	3.85	2.41	4.36	4.94	4.56	2.55	4.34	4.49	4.52	4.97
		10	1.8	4.25	5.06	3.65	3.12	4.71	5.26	4.98	3.48	4.67	4.85	5.17	4.21
		15	2.7	4.06	5.23	3.96	3.27	4.58	5.42	5.07	3.76	4.19	4.8	5.07	4.51
		20	3.7	4.1	5.44	4.65	4.57	4.5	5.65	4.84	4.08	4.37	5.44	5.2	4.73
		50	9.2	2.33	2.97	4.6	4.1	2.53	2.98	4.17	3.79	2.42	3.14	3.27	2.7
		100	18.3	1.66	1.97	2.8	2.21	1.76	1.95	2.69	2.19	1.72	2.15	2.25	1.9
		200	36.7	1.31	1.48	1.78	1.67	1.37	1.43	1.74	1.63	1.33	1.56	1.77	1.47
		400	73.3	1.15	1.22	1.39	1.29	1.17	1.22	1.36	1.33	1.15	1.28	1.39	1.27
		600	110	1.09	1.14	1.28	1.17	1.12	1.14	1.32	1.19	1.1	1.17	1.24	1.16
		1000	146.7	1.05	1.08	1.19	1.09	1.06	1.08	1.22	1.15	1.05	1.1	1.12	1.09
		1200	220	1.04	1.06	1.16	1.05	1.05	1.06	1.21	1.13	1.04	1.1	1.11	1.06
		1500	275	1.04	1.04	1.12	1.03	1.04	1.05	1.15	1.1	1.04	1.07	1.09	1.05
		3000	550	1.01	1,00	1.05	1.02	1.01	1.02	1.1	1.06	1.01	1.03	1.05	1.03
	40	5	0.9	5.27	4.07	4.01	4.02	4.96	4.27	4.52	4.23	5.01	4.14	3.45	4.39
		10	1.8	4.54	5.9	6.51	2.91	4.34	5.87	6.03	3.91	5.37	5.37	4.27	4.63
		15	2.7	4.41	5.59	5.46	2.36	4.21	5.97	5.71	4.3	5.25	5.6	4.33	4.3
		20	3.7	4.2	5.26	5.58	4.05	4.01	5.98	4.76	4.99	5.19	5.69	5.66	4.99
		50	9.2	4.34	4.94	5.6	4.21	4.01	5.58	5.61	5.14	5.76	5.39	6.04	5.01
		100	18.3	3.18	3.77	4.18	4.95	3.04	3.99	6.01	6.05	3.99	3.81	4.66	6.48
		200	36.7	2.06	2.37	2.49	3.16	1.97	2.4	3.21	3.31	2.4	2.35	2.73	3.03
		400	73.3	1.52	1.68	1.72	1.97	1.47	1.68	2.09	2.09	1.68	1.66	1.81	2.1
		600	110	1.35	1.45	1.51	1.65	1.33	1.46	1.68	1.69	1.45	1.44	1.57	1.7
		1000	146.7	1.2	1.27	1.28	1.37	1.18	1.28	1.41	1.37	1.27	1.27	1.34	1.44
		1200	220	1.16	1.22	1.25	1.3	1.16	1.23	1.34	1.29	1.22	1.23	1.29	1.36
		1500	275	1.13	1.17	1.19	1.22	1.12	1.18	1.27	1.25	1.19	1.18	1.23	1.3
		3000	550	1.05	1.07	1.09	1.11	1.04	1.09	1.15	1.11	1.1	1.08	1.11	1.13
	35	5	0.9	4.48	4.28	4.99	2.78	3.94	4.93	4.46	2.87	4.11	5.05	6.8	2.49
		10	1.8	4.41	4.42	5.3	3.1	4.16	4.45	5.12	3.07	4,00	5.71	6.4	2.78
		15	2.7	4.46	4.66	5.24	4.19	4.22	4.57	5.36	3.58	3.98	5.41	5.04	2.55
		20	3.7	4.42	4.46	5.26	4.16	4.45	4.87	5.87	4.12	3.93	5.3	5.28	2.96
		50	9.2	4.48	4.46	5.85	5.66	4.21	4.26	4.78	5.8	4.05	4.86	5.19	2.68
		100	18.3	4.42	4.62	5.73	5.37	4.16	4.79	4.59	5.57	3.98	4.87	5.19	3.12
		200	36.7	4.48	4.55	5.67	6.09	4.17	5.03	5.03	5.27	3.94	4.84	5.23	3.15
		400	73.3	2.73	2.79	3.25	3.63	2.52	3.33	4.87	3.3	2.47	2.88	3.17	3.78
		600	110	2.15	2.19	2.54	2.69	2,00	2.53	5.04	2.55	1.97	2.26	2.46	3.54
		1000	146.7	1.68	1.7	1.91	1.98	1.59	1.92	3.28	1.9	1.55	1.75	1.83	3.21
		1200	220	1.56	1.58	1.77	1.83	1.49	1.78	2.95	1.74	1.45	1.62	1.68	2.16
		1500	275	1.44	1.47	1.61	1.66	1.39	1.64	2.66	1.56	1.35	1.49	1.54	1.87
		3000	550	1.2	1.23	1.29	1.35	1.18	1.37	2.06	1.24	1.17	1.23	1.25	1.42
	30	5	0.9	3.94	5.99	3.32	2.65	4.91	4.91	3.59	2.56	3.62	5.36	3.69	2.58
		10	1.8	3.83	5.22	6.02	3.12	4.39	4.39	5.65	2.87	3.66	4.42	3.87	2.87
		15	2.7	3.77	4.97	5.72	4.65	3.94	3.94	4.89	3.26	3.69	4.3	4.82	3.11
		20	3.7	3.82	4.69	5.3	5.27	3.84	3.84	5.12	4.53	3.72	4.33	4.69	4.15
		50	9.2	3.68	4.41	5.22	5.59	3.56	3.56	5.33	4.91	3.61	4.35	4.64	4.05
		100	18.3	3.72	4.41	4.86	4.72	3.54	3.54	4.87	5.5	3.65	4.39	4.83	4.67
		200	36.7	3.77	4.44	4.86	3.59	3.71	3.71	4.67	5.78	3.57	4.35	4.6	4.89
		400	73.3	3.72	4.35	4.83	3.16	3.73	3.73	4.33	6.13	3.62	4.36	4.61	4.23
		600	110	3.71	4.29	4.82	3.02	3.69	3.69	4.87	5.96	3.62	4.35	4.61	3.97
		1000	146.7	2.6	2.96	3.29	2.26	2.6	2.6	3.27	4.09	2.57	3,00	3.11	4.04
		1200	220	2.33	2.63	2.91	2.11	2.33	2.33	2.76	3.52	2.3	2.66	2.76	3.74
		1500	275	2.06	2.31	2.54	1.65	2.06	2.06	2.27	3.06	2.05	2.35	2.43	2.79
		3000	550	1.51	1.64	1.72	1.27	1.5	1.5	1.67	2.02	1.5	1.66	1.74	1.87

Table 5.8: Results of the Correlation Amplitude Check Detection Technique against FEA attack.



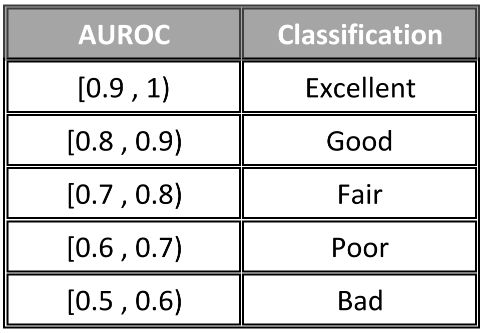
			Victim C/No					
			45 dB-Hz			30 dB-Hz		
			Attack 1	Attack 2	Attack 3	Attack 1	Attack 2	Attack 3
Attacker C/No	45 dB-Hz	Best Case Difference	0.92	0.91	0.79	0.75	0.83	0.81
		Worst Case Difference	0.88	0.41	0.25	0.15	0.31	0.21
		Maximum Time Detectable (μs)	20	50	200	200	100	400
		Minimum Time Detectable (μs)	5	5	5	5	5	5
	30 dB-Hz	Best Case Difference	0.99	0.99	0.73	0.94	0.92	0.82
		Worst Case Difference	0.41	0.34	0.33	0.85	0.42	0.47
		Maximum Time Detectable (μs)	3000	1500	3000	1500	1500	3000
		Minimum Time Detectable (μs)	5	5	5	5	5	5

Table 5.9: Comparison results with Detection Method 2. The results corresponds when 6 satellites are present in the signal.

5.3 Receiver Operation Characteristic (ROC)

In this section the Receiver Operation Characteristic (ROC) for some of the most significant cases of the Detection method 1 is depicted, although it could be also done for the other one. The ROC will be depicted for the three different attack strategies carried out. First of all, we need to specify what is the ROC, and what it represents. Figure 5.1 shows an example of ROC. In the ROC is plotted the probability of Detection (P_D) versus the probability of False Alarm (P_{FA}). Each point on the blue curve corresponds to a certain value (P_D) and (P_{FA}), for a given threshold γ. Figure 5.1 shows as the threshold γ increases (we move towards zero in the curve), (P_{FA}) and (P_D) decreases. In addition, the ROC should always be above the dashed 45 deg line. This is because the dashed line represents a detector that bases its decisions in chance, ignoring all data. The ROC should always be above the black 45deg dashed line. This dashed line corresponds to the chance detector, that bases its decision on flipping a coin and ignoring all data.

A metric to measure the test's discriminative ability (how good is the test in a given situation) from the ROC curve is the Area Under the Curve, or just AUROC. This AUROC is plotted in Figure 5.1 in transparent-blue. The AUROC is equal to the probability that a randomly chosen positive event ranks above (is deemed to have a higher probability of being positive than) a randomly chosen negative event. Or in other words, AUROC determines how good is the detector summarizing its performance in a single value, in order to be able to compare between detector easily. The perfect detector AUROC is 1, and the AUROC for the worse detector, which is the chance detector, is 0.5. The AUROC values can be classified as



AUROC	Classification
[0.9 , 1)	Excellent
[0.8 , 0.9)	Good
[0.7 , 0.8)	Fair
[0.6 , 0.7)	Poor
[0.5 , 0.6)	Bad

Table 5.10: Classification of the AUROC values depending on the detector performance.

In the next Section are plotted some ROC curves from the results shown in Section **??**. In the plotted curves has been only considered the cases when 6 satellites are present, since it is the worst case scenario considered (in terms of number of PRN codes present in the signal). In addition, only the cases when the victim C/No level is 45 dB-Hz and 35 dB-Hz has been taken into account. This is done only to show the behaviour of the detector in two typical outdoor C/No levels. Moreover, the ROC curves corresponds to the best window length for each attack.

5.3.1 ROC Comparison

In Figure 5.2 the ROC curves for the three attacks are plotted when the spoofer C/No is 45 dB-Hz. The performance of the detectors shows that in general are quite poor, above all for the Chip-By-Chip Estimation and Bit-Guess Estimation attacks, since the AUROC in these cases is about 0.5. This means that the detectors in those circumstances will behave practically as a chance detector. In this case due to the high spoofer C/No, the attacker will estimate the real symbol very quickly, and therefore the transmitted bit will be modified very little. In consequence, the victim will not be able to determine the spoofer presence with enough certainty. This bad results for these attacks were expected, since looking at the cases when the spoofer C/No is 45 dB-Hz in Tables 5.2 and 5.3 the results were not too much propitious. In contrast, Table 5.4 shows quite good results against FEA attack, with an AUROC of about 0.6. According to the classification given at the beginning of the Section, the detectors for the attacks Chip-By-Chip Estimation and Bit-Guess Estimation are considered bad detectors, since its AUROC is comprised in the range of $[0.50, 0.60)$. The detector for the FEA attack is considered a Poor detector, since the AUROC is comprised in the range $[0.60, 0.70)$.

In Figure 5.3 the ROC curves when the spoofer C/No is 40 dB-Hz are depicted. In this

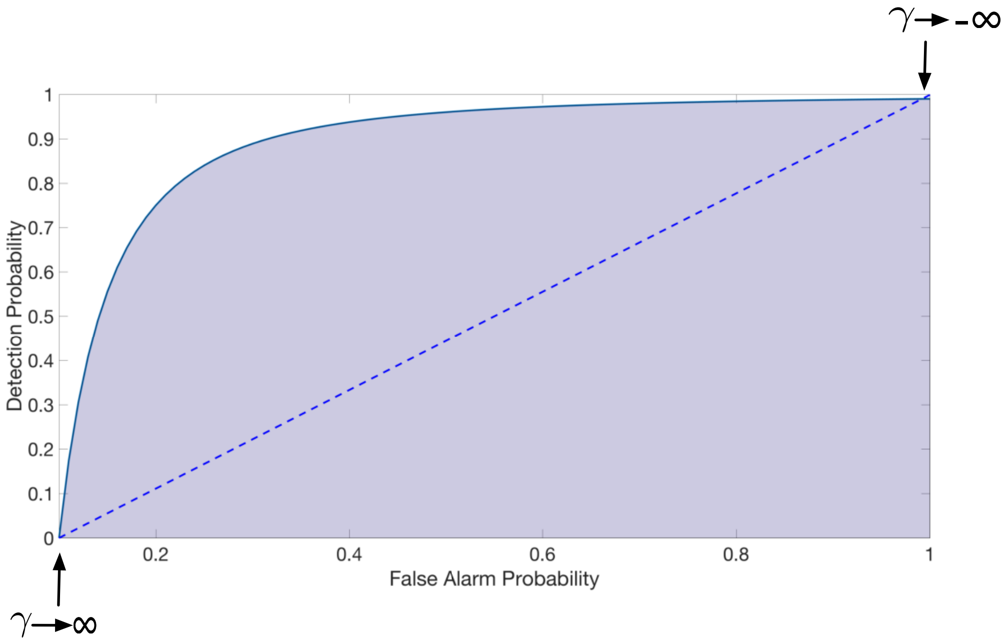


Figure 5.1: ROC example for the case of a Gaussian distribution.

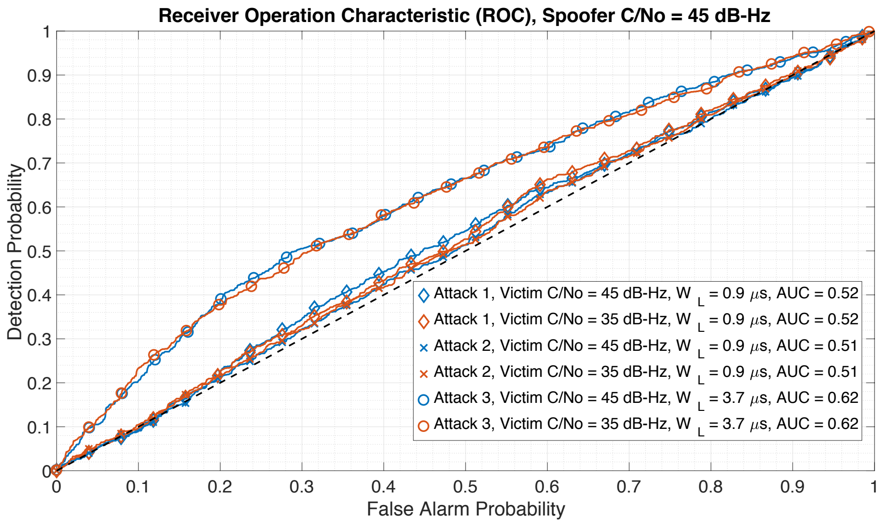


Figure 5.2: ROC for the three attacks when the spoofer C/No is 45 dB and victim C/No levels of 45 dB-Hz and 35 dB-Hz.

case, as we have seen, the spoofer needed more time (approximately three times) to estimate correctly the received bit from the satellite. In consequence, the victim has more time to detect the spoofer, and the detection results are improved. Looking at Figure 5.3 we can observe as all the behaviour of all the plotted detectors is similar. All of them have an AUROC of about 0.6-0.7. Comparing the obtained ROC results with Tables 5.4, 5.4 and 5.4 we could say that both results concur in that the detector can be considered a poor detector, according to the classification given above.

In Figure 5.4 the ROC curves when the spoofer C/No is 40 dB-Hz are depicted. In this case is shown as all the curves for all the attacks are very similar between them. The AUROC for the full amount of detectors is comprised in the range of [0.70, 0.80). According to the classification given above the detectors could be considered fair detectors. From this point, we start to obtain quite good detectors. This is mainly due to the fact that the spoofer needs a quite large amount of time (about $36.7\mu s$) to estimate the symbol coming from the satellite.

Finally, in Figure 5.5 the ROC curves when the spoofer C/No is 30 dB-Hz is depicted. Figure 5.5 shows a great improvement compared with the other cases. Above all compared with the cases of C/No 45 dB-Hz and 40 dB-Hz. In this occasion the AUROC are higher than 0.75 in any case. The best performance is obtained against the attack strategy Chip-By-Chip Estimation. The AUROC values for this case is 0.84 and 0.95, for 45 dB-Hz and 35 dB-Hz respectively. This means that the detector can be classified as an excellent detector (45 dB-Hz) or a good detector (35 dB-Hz), depending on the victim C/No, according to the classification given above. The detector against the attack strategy Bit-Guess Estimation is the worse of the three, although the

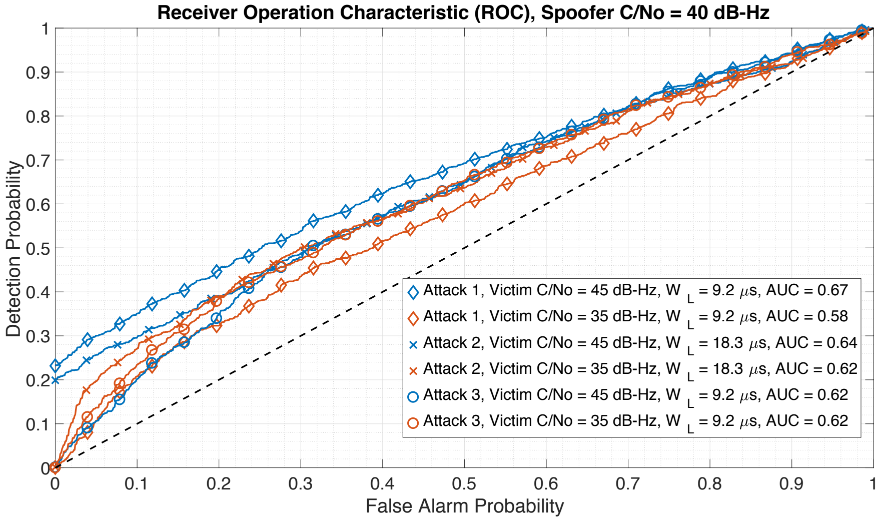


Figure 5.3: ROC for the three attacks when he spoofer C/No is 40 dB and victim C/No levels of 45 dB-Hz and 35 dB-Hz.

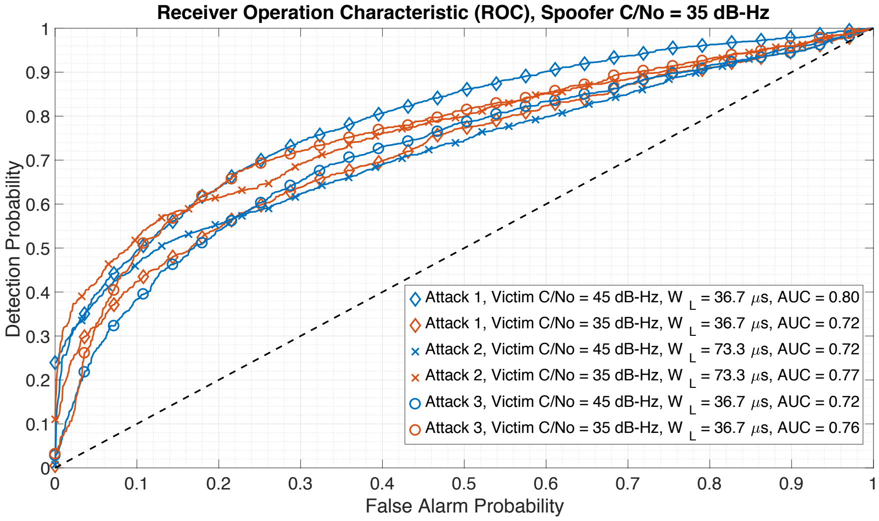


Figure 5.4: ROC for the three attacks when the spoofer C/No is 35 dB and victim C/No levels of 45 dB-Hz and 35 dB-Hz.

AUROC is between 0.6-0.7. Thus, in this case the detector behaves as a poor detector. Finally, the detector performance against the FEA attack can be classified as a good detector, since the obtained AUROC is very close to 0.8 or even beyond that value.

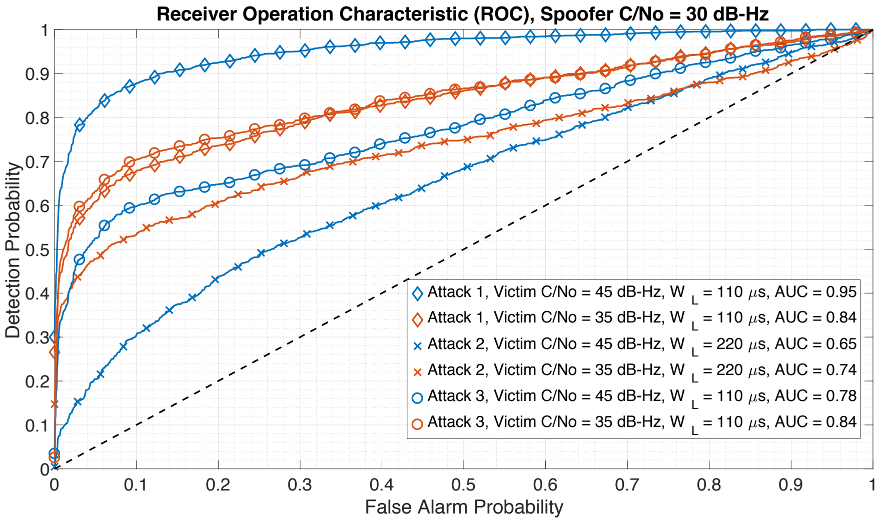


Figure 5.5: ROC for the three attacks when the spoofer C/No is 30 dB and victim C/No levels of 45 dB-Hz and 35 dB-Hz.

6 Conclusions

The main purpose of this thesis was to show that attacks against GNSS are feasible and it could have disastrous consequences, since critical systems of our society relies partially or totally on GNSS. First of all, we have provided an introduction about GNSS, in which we have described in what consists GNSS, the segments by which it is composed, its deployment architecture and the GNSS signals and receiver architecture. This outline on GNSS has been useful to understand the state-of-the-art attacks described in Chapter 3. In this Chapter, some attacks against GNSS proposed in the literature has been described. Then, the strategies used to perform the attacks in this thesis has been fully described. They were split in two approaches. The first one, consisted in the estimation of the real bit transmitted by the satellite, and the rebroadcast of this estimation. By means of this approach, the received signal by the victim had some instabilities at the beginning of some bits or the sign of the beginning and ending of each symbol were different, produced by the estimation process of the unpredictable bits. The second one, the FEA attack, consisted in predicting somehow the bits of the Navigation Data, or obtaining them from other source since some of the information provided by the Navigation Message is public. Some bits are unpredictable, so the spoofer needed to guess them. Some of the guesses were wrong, and the spoofer increased the amplitude of the first samples after each wrong guess in order to maintain the same bit energy as if the signal were the authentic.

After describing the attacks, the different proposed detection techniques were described. They basically consisted in computing the ratio between the first and last part of the bits, but following different approaches (taking into account the sign, energy, etc.). After showing them, they were applied against real recorded signals in different conditions of C/No. Some signals where authentic, and some other were modified to simulate the spoofer attack. Then the results against both type of signals were compared in order to decide if the victim could determine the spoofer presence.

From the results shown in Chapter 5 can be drawn the following conclusions:

1. All the proposed attack strategies can be detected by some method. The performance of the proposed detection methods is strongly dependant on the spoofer and victim C/No

level, as well as the observation window length carried out by the victim.

2. The lower the C/No at the spoofer, the more time it needs to estimate the bits transmitted by the satellite. Therefore, the victim will be able to detect the attacker with a wider observation window length due to the wider tell-tale. Thus the victim will have more freedom degrees to apply during the detection process.

3. When the victim C/No worsens, the victim has more difficulties to detect the spoofer. The noise in the signal conceals the remaining effects produced by the modifications carried out by the attacker.

4. The number of satellites present in the signal is not determining in the detection performance. The cross-correlation effect produced by the presence of more PRN sequences ends up with an increment of about 0.1-0.2.

5. The best observation window length that the victim can choose is directly related to the number of samples that are modified by the spoofer. Therefore, the optimal window length is strongly dependant on the spoofer C/No. Depending on the attack nature, this optimal window length can be equal to the number of modified samples or two times this value. For example, for the attack strategies Chip-By-Chip Estimation and FEA, the optimal length is equal to the number of samples the spoofer modifies. When the victim takes only the number of samples modified by the spoofer, the difference between the first and last samples is maximum (the samples are balanced out one each other, or is taken the full samples with increased amplitude), and therefore the ratio is minimum (or maximum in the case of the FEA attack). On the contrary, the optimal length for the Bit-Guess Estimation is two times the samples that are modified, since the minimum ratio occurs when the guess and the true symbol cancels completely (after switching the polarity of the bit when the guess is wrong).

6. The proposed detection methods behaves better against some of the attacks than against the others. The best detection performance is obtained against FEA attack, which is the attack that modifies the most the signal, increasing amplitude of the first samples of the bit the most. On its behalf, the detection performance against the Chip-By-Chip and Bit-Guess Estimation strategies was quite similar. Although the attack Bit-Guess Estimation shows that the spoofer was better concealed, and thus the detection methods were more effective against attack 1, above all at low victim C/No.

   In terms of best absolute performance of the proposed methods, we could say that in general terms the best detection method is obtained with the Total Correlation Ratio Detection Technique, specially at low spoofer C/No. At high spoofer C/No the differences are reduced, and the performance for all the detection techniques is quite similar. When the spoofer C/No is high enough, in general the performance is more dependant on the victim C/No than in the detection method carried out.

Bibliography

[Ako12] Dennis Akos, “Who is afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc).”, Vol. 59, 12 2012.

[AR15] Dirk Kowaleski Alexander Rügamer, “Jamming and spoofing of gnss signals – an underestimated risk?!”, May 2015.

[Bha17] Jahshan Bhatti, Todd E. Humphreys, “Hostile control of ships via false gps signals: Demonstration and detection”, *Navigation*, Vol. 64, nº 1, pags. 51–66, 2017, navi.183.

[Cap17] Gianluca Caparra, Silvia Ceccato, Nicola Laurenti, Justan Cramer, Chuck J Walter, “Feasibility and limitations of self-spoofing attacks on gnss signals with message authentication”, 09 2017.

[Cur17] James T. Curran, Cillian O’Driscoll, “Message authentication as an anti-spoofing mechanism”, 06 2017.

[DB11] Chief Foreign Correspondent David Blair, Alex Spillius, “Iran shows off captured us drone”, December 2011.

[DW12] K D. Wesson, M Rothlisberger, T.E. Humphreys, “Practical cryptographic civil gps signal authentication”, Vol. 59, 09 2012.

[EH08] T E. Humphreys, B M. Ledvina, Mark Psiaki, B W. O.Hanlon, Jr P. M. Kintner, “Assessing the spoofing threat: Development of a portable gps civilian spoofer”, pags. 2314–2325, 01 2008.

[ER17] Daniel Egea-Roca, *Change Detection Techniques for GNSS Signal-Level Integrity*, PhD Thesis, Department of Telecommunication Systems Engineering, Autonomous University Barcelona, 2017.

[FH16] I. Fernández-Hernández, G. Seco-Granados, “Galileo nma signal unpredictability and anti-replay protection”, *2016 International Conference on Localization and GNSS (ICL-GNSS)*, pags. 1–5, June 2016.

[FP03] C. Fernadez-Prades, J. A. Fernandez-Rubio, G. Seco, “Joint maximum likelihood estimation of time delays and doppler shifts”, *Seventh International Symposium on Signal Processing and Its Applications, 2003. Proceedings.*, Vol. 2, pags. 523–526 vol.2, July 2003.

[Gof17] Stan Goff, “Reports of mass gps spoofing attack in the black sea strengthen calls for pnt backup”, July 2017.

[Her15] Ignacio Fernandez Hernandez, *Snapshot And Authentication Techniques For Satellite Navigation*, PhD Thesis, Faculty of Engineering and Science, Aalborg University, may 2015.

[Hum09] Todd E. Humphreys, Brent M. Ledvina, Markt L. Psiaki, Brady W. O'Hanlon, Paul M. Kintner, "Assessing the spoofing threat", *GPS World*, Vol. 20, pags. 28–38, January 2009.

[JJ12] Ali Jafarnia-Jahromi, Ali Broumandan, J Nielsen, GÃ©rard Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques", Vol. 2012, 07 2012.

[JJ13] Ali Jafarnia-Jahromi, *GNSS Signal Authenticity Verification in the Presence of Structural Interference*, PhD Thesis, Department of Geomatics Engineering, University of Calgary, 2013.

[Jua11] J. C. Juang, "Gnss spoofing analysis by vias", 2011.

[Kap06] Elliott D. Kaplan, *Understanding GPS: principles and applications; 2nd ed.*, Artech House, Boston, MA, 2nd ed., 2006.

[Ker14] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, Todd E. Humphreys, "Unmanned aircraft capture and control via gps spoofing", *Journal of Field Robotics*, Vol. 31, nº 4, pags. 617–636, 2014.

[Kuu07] H. Kuusniemi, A. Wieser, G. Lachapelle, J. Takala, "User-level reliability monitoring in urban personal satellite-navigation", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 43, nº 4, pags. 1305–1318, October 2007.

[Lev11] P. Levin, D.S. De Lorenzo, P.K. Enge, S.C. Lo, "Authenticating a signal based on an unknown component thereof", jun. 28 2011, uS Patent 7,969,354.

[Loer] S. Lo, D. De Lorenzo, P. Enge, D. Akos, P. Bradley, "Signal Authentication: A Secure Civil GNSS for Today", *2009*, pags. 30–39, September.

[LS16] S. Locubiche-Serra, G. Seco-Granados, J. A. López-Salcedo, "Doubly-adaptive autoregressive kalman filter for gnss carrier tracking under scintillation conditions", *2016 International Conference on Localization and GNSS (ICL-GNSS)*, pags. 1–6, June 2016.

[McD07] C.E. McDowell, "Gps spoofer and repeater mitigation system using digital spatial nulling", July 2007, uS Patent 7,250,903.

[Mon09] Paul Y. Montgomery, Todd E. Humphreys, Brent M. Ledvina, Vol. 1, pags. 124–130, 2009.

[O'H10] Brady W. O'Hanlon, Mark L. Psiaki, Todd E. Humphreys, Jahshan A. Bhatti, *Real-time spoofing detection in a narrow-band civil GPS receiver*, Vol. 3, pags. 2211–2220, 2010.

[OSQ15] OSQZSS, "Software-defined gps signal simulator", `https://github.com/osqzss/gps-sdr-sim`, 2015.

[Pap08] P. Papadimitratos, A. Jovanovic, “Gnss-based positioning: Attacks and countermeasures”, *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pags. 1–7, Nov 2008.

[Per02] Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song, “The tesla broadcast authentication protocol”, 2002.

[PM06] Per Enge Pratap Misra, *Global Positioning System: Signals, Measurements and Performance*, Ganga-Jamuna Press, 2$^{\underline{\text{nd}}}$ ed., 2006.

[Poz10] O. Pozzobon, L. Canzian, M. Danieletto, A. D. Chiara, “Anti-spoofing and open gnss signal authentication with signal authentication sequences”, *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pags. 1–6, Dec 2010.

[Psi14] Mark L. Psiaki, Brady W. O’Hanlon, Steven P. Powell, Jahshan A. Bhatti, Todd E. Humphreys, Andrew Schofield, “Gnss lies, gnss truth: Spoofing detection with two-antenna differential carrier phase”, 11 2014.

[Psi16] M. L. Psiaki, T. E. Humphreys, “Gnss spoofing and detection”, *Proceedings of the IEEE*, Vol. 104, n$^{\underline{\text{o}}}$ 6, pags. 1258–1270, June 2016.

[Sch16] Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, MichałRen, “A survey and analysis of the gnss spoofing threat and countermeasures”, *ACM Comput. Surv.*, Vol. 48, n$^{\underline{\text{o}}}$ 4, pags. 64:1–64:31, may 2016.

[Seb16] Clare Sebastian, “Getting lost near the kremlin? russia could be ’gps spoofing”’, December 2016.

[SG12] G. Seco-Granados, J. López-Salcedo, D. Jiménez-Baños, G. López-Risueño, “Challenges in indoor global navigation satellite systems: Unveiling its core features in signal processing”, *IEEE Signal Processing Magazine*, Vol. 29, n$^{\underline{\text{o}}}$ 2, pags. 108–131, March 2012.

[Sta12] GPS World Staff, “Massive gps jamming attack by north korea”, May 2012.

[Wen17] Hengqing Wen, Peter Yih-Ru, John Huang, Andy Dyer, John Archinal, Fagan , “Countermeasures for gps signal spoofing”, 09 2017.