Università degli Studi di Padova

Department of Information Engineering

Master Thesis in Telecommunication Engineering

Security Evaluation of GNSS Signal Quality Monitoring Techniques against Optimal Spoofing Attacks

Supervisor
Nicola Laurenti
Università degli Studi di Padova

Co-supervisor
Gianluca Caparra
Università degli Studi di Padova

Master Candidate
Leonardo Chiarello

Academic Year 2017/2018
9 July 2018

"In theory, there is no difference between theory and practice, but in practice there is."

Johannes L. A. van de Snepscheut and Yogi Berra

Abstract

Leonardo Chiarello

Security Evaluation of GNSS Signal Quality Monitoring Techniques against Optimal Spoofing Attacks

GNSS-dependent positioning, navigation, and timing synchronization procedures have a significant impact on everyday life. Therefore, such a widely used system increasingly becomes an attractive target for illicit exploitation by terrorists and hackers for various motives. As such, spoofing and anti-spoofing algorithms have become an important research topic within the GNSS discipline. This Thesis provides a review of recent research in the field of GNSS spoofing/anti-spoofing, designs a method to generate an energy optimal spoofing signal and evaluates the performance of the anti-spoofing signal quality monitoring techniques against it.

Contents

List of Figures **vii**

List of Tables **ix**

List of Abbreviations **xi**

1 Introduction **1**

2 An Introduction to GNSS **3**
2.1 GNSS Systems . . . 3
2.2 GNSS Segments . . . 4
2.3 GNSS Signals . . . 5
2.3.1 GPS Signals . . . 7
2.3.2 Galileo Signals . . . 9
2.4 GNSS Receivers . . . 10
2.4.1 Antennas . . . 11
2.4.2 Front End . . . 11
2.4.3 Baseband signal processing . . . 12
2.4.4 Application Processing . . . 20

3 The Spoofing Threat **23**
3.1 General Model of a Spoofing Attack . . . 23
3.2 Spoofing Generation Techniques . . . 24
3.3 Spoofing Based on Receiver State . . . 25
3.4 Types of Spoofing Attacks . . . 26

4 Signal Processing Techniques for Anti-Spoofing **31**
4.1 Spoofing Detection . . . 32
4.1.1 Methods Based on the Received Signal Strength (RSS) . . . 32
4.1.2 Spoofing Discrimination Using Spatial Processing . . . 35
4.1.3 Time of Arrival (TOA) Discrimination . . . 39
4.1.4 Correlation Peak Monitoring . . . 40
4.1.5 Signal Parameters Monitoring . . . 42
4.2 Spoofing Mitigation . . . 44
4.2.1 Vestigial Signal Detection . . . 44
4.2.2 Multiantenna Beamforming and Null Steering . . . 45
4.2.3 Spoofing Estimating Delay Lock Loop (SEDLL) . . . 47
4.2.4 Spoofing Detection, Classification and Cancellation (SDCC) . . . 48

5 Optimal Spoofing Attacks against Signal Quality Monitoring Techniques **51**
5.1 Spoofing Scenario . . . 51
5.2 A Trivial Attack . . . 52
5.3 Signal Quality Monitoring Techniques . . . 52
5.3.1 Metrics . . . 52

5.3.2 Detection thresholds 54
5.4 Nulling Attack 55
5.5 Optimal Attack 55
5.5.1 Constraints 56
5.5.2 Optimization Problem 61

6 Security Evaluation of the Signal Quality Monitoring Techniques 65
6.1 Comparison between different authentic code delays 68
6.2 Comparison between different metric precisions 71
6.3 Comparison between nulling and optimal attack with unknown authentic phase 72
6.4 Simulation of a lift-off-aligned attack 73

7 Conclusions and Future Work 75

A Relation between C/N_0 and pre-correlation noise power 77

B Statistics of the correlator output 79

C Relation between C/N_0 and post-correlation noise power 83

Bibliography 85

List of Figures

2.1 GNSS architecture. From [15]. 5
2.2 Composition of the navigation satellite signal. From [17]. 6
2.3 GPS, Glonass, Galileo and Beidou navigational frequency bands. From [15]. 7
2.4 Legacy GPS signal structure. From [15]. 8
2.5 Power spectral density of a BOC(1,1) and BPSK-modulated signals. From [18]. 10
2.6 Generic receiver architecture. From [18]. 11
2.7 Example of GNSS receiver's front end structure. From [15]. 12
2.8 Block diagram of internal functions in a generic baseband processing block. From [16]. 13
2.9 Normalized ACF of two differently modulated signals. 15
2.10 Example of GPS C/A correlation function during signal acquisition. From [16]. 17
2.11 Block diagram of a GNSS signal tracking engine. From [16]. 18
2.12 Early-minus-late DLL discriminator. From [16]. 19
2.13 Positioning through intersecting spheres. From [16]. 20
2.14 Pseudorange measurement contents. From [15]. 21

3.1 The spoofing threat continuum: simplistic, intermediate, and sophisticated spoofing attacks. From [19]. 24
3.2 Repeater spoofer block diagram. From [10]. 25
3.3 Lift-off-delay spoofing attack (left) and corresponding tracking error te (right) with spoofing commenced at T2. From [21]. 26
3.4 Meaconing attack: Introducing a delayed replica with varying amplitude. From [21]. 27
3.5 Non line-of-sight spoofing: Spoofing of low elevation (blocked to the user) SVs. From [21]. 28

4.1 Vulnerability region comparison of C/N_0 versus absolute power monitoring techniques. From [10]. 33
4.2 Variations of spoofing and authentic received C/N_0 versus receiver distance from spoofer transmitting antenna. From [10]. 34
4.3 Single-differenced carrier phase time histories (top plot) and spoofing detection statistic time history (bottom plot) for a spoofing attack. From [27]. 37
4.4 Spatial sampling for a moving handheld GPS receiver. From [10]. . . . 37
4.5 Correlation amplitude for spoofing and authentic PRN signals. From [10]. 38
4.6 Distribution of prompt correlator output power for authentic signals and authentic-spoofing interaction for different spoofing powers. From [10]. 42

4.7 Authentic and spoofed SNR variations as a function of average spoofing power. From [10]. 46
4.8 Block diagram of the SEDLL receiver architecture. From [34]. 47
4.9 SEDLL Spoofing cancellation. From [34]. 48
4.10 Block diagram of the SDCC receiver architecture. From [10]. 49

5.1 Normalized correlation function of authentic, spoofing and total signals for two differently modulated signals as a function of $\Delta\tau$. Early, late and prompt in-phase correlator outputs of the total correlator function are also shown. 53
5.2 Normalized correlation function of authentic, spoofing and total signals for two differently modulated signals as a function of $\Delta\tau$. Early, late and prompt in-phase correlator outputs of the total correlator function are also shown. 56

6.1 Normalized ACF of the two signals that are used in the simulations. . 65
6.2 Authentic, spoofing and total correlation function during a snapshot of the optimal attack with default parameters (BPSK(1,1) signal). 66
6.3 ROC for different authentic code delays (BPSK(1) signal). 69
6.4 ROC for different authentic code delays (BOC(1,1) signal). 70
6.5 ROC for different metric precisions (BPSK(1) signal). 71
6.6 ROC with unknown authentic phase (BPSK(1) signal) (continued). . . 72
6.7 ROC with unknown authentic phase (BPSK(1) signal) (continued). . . 73
6.8 Evolution of the amplitude of the prompt correlator and the authentic code delay for the lift-off-aligned attack. 74
6.9 Simulation of a lift-off-aligned attack (BPSK(1) signal) (continued). . . 74

List of Tables

2.1 Current GPS navigation signals. From [15]. 8
2.2 Galileo navigation signals. The PRN codes relative to PRS signals are encrypted. The two signals located in the E5a and E5b bands respectively are modulated onto a single E5 carrier frequency of 1191.795 MHz using the AltBOC technique: AltBOC(15,10). From [15]. 9

4.1 Summary of spoofing detection techniques. 43
4.1 Summary of spoofing detection techniques (continued). 44
4.2 Summary of spoofing mitigation techniques. 50

5.1 Signals involved in the attack in their time and frequency domain version. 56

6.1 Default parameters. 67
6.2 Spoofing and total energy for different authentic code delays (BPSK(1) signal). 69
6.3 Spoofing and total energy for different authentic code delays (BOC(1,1) signal). 70
6.4 Spoofing and total energy for different metric precisions (BPSK(1) signal). 71
6.5 Spoofing and total energy with unknown authentic phase (BPSK(1) signal). 72

List of Abbreviations

ACF	**A**uto**C**orrelation **F**unction
ADC	**A**nalog-to-**D**igital **C**onverter
AERM	**A**symmetric **E**arly **R**atio **M**etric
AGC	**A**utomatic **G**ain **C**ontrol
ALL	**A**mplitude-**L**ocked **L**oop
ALRM	**A**symmetric **L**ate **R**atio **M**etric
BDS	**B**ei**D**ou navigation satellite **S**ystem
BOC	**B**inary **O**ffset **C**arrier
BPSK	**B**inary **P**hase **S**hift **K**eying
C/A	**C**oarse/**A**cquisition
CADLL	**C**oupled **A**mplitude **D**elay **L**ocked **L**oop
CAF	**C**ross **A**mbiguity **F**unction
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
CS	**C**ommercial **S**ervice
DDM	**D**ouble **D**elta **M**etric
DLL	**D**elay-**L**ocked **L**oop
DM	**D**elta **M**etric
ELPM	**E**arly-**L**ate **P**hase **M**etric
FLL	**F**requency-**L**ocked **L**oop
FOC	**F**ull **O**perational **C**apability
GLRT	**G**eneralized **L**ikelihood **R**atio **T**est
GNSS	**G**lobal **N**avigation **S**atellite **S**ystem
GPS	**G**lobal **P**ositioning **S**ystem
IF	**I**ntermediate **F**requency
IMU	**I**nertial **M**easurement **U**nit
ITU	**I**nternational **T**elecommunication **U**nion
LOS	**L**ine-**O**f-**S**ight
MDM	**M**agnitude **D**ifference **M**etric
MEDLL	**M**ultipath **E**stimating **D**elay **L**ock **L**oop
NAV	**NA**vigation **M**essage
OS	**O**pen **S**ervice
PDF	**P**robability **D**ensity **F**unction
PHD	**P**isarenki **H**armonic **D**ecomposition
PLL	**P**hase-**L**ocked **L**oop
PPS	**P**recise **P**ositioning **S**ervice
PRN	**P**seudo**R**andom **N**oise
PRS	**P**ublic **R**egolated **S**ervice
PVT	**P**osition-**V**elocity-**T**ime
RF	**R**adio **F**requency
RHCP	**R**ight-**H**and **C**ircularly **P**olarized
RM	**R**atio **M**etric
ROC	**R**eceiver **O**perating **C**haracteristic
SAR	**S**earch and **R**escue **S**ervice

SCER	**S**ecurity **C**ode **E**stimation and **R**eplay
SDCC	**S**poofing **D**etection, **C**lassification and **C**ancellation
SEDLL	**S**poofing **E**stimating **D**elay **L**ock **L**oop
SIS	**S**ignal **I**n **S**pace
SoL	**S**afety-**o**f-**L**ife
SPP	**S**tandard **P**oint **P**ositioning
SPS	**S**tandard **P**ositioning **S**ervice
SQM	**S**ignal **Q**uality **M**onitoring
SV	**S**pace **V**ehicle
TOA	**T**ime **O**f **A**rrival
TSP	**T**otal **S**poofing **P**ower
U.S.	**U**nited **S**tates

To my parents, Mauro and
Tiziana, and my sister, Linda

Chapter 1

Introduction

As technological advances are introduced in society and their use spreads among the people, more and more applications are found for each technology. Global navigation satellite system (GNSS) technology is a clear example of this phenomenon. Ever since the global positioning system (GPS) became operational, its applications and use have increased dramatically. Nowadays, almost every person has a device with them, capable of guiding them through the ever-changing cities by means of GNSS signals. Additionally, these devices are supported by infrastructures that are synchronized thanks to these GNSS signals. Many other examples can be found to understand how ubiquitous GNSSs are in everyday activities.

Technology evolves and spreads, and the concerns for security in all electronic and telecommunication systems increase as well. This concern applies to many different sectors of today's society, one of them being GNSS. As can be seen, modern society strongly relies on GNSS, for a constantly increasing number of applications and services. However, the issues related to the security of such systems are sometimes underestimated. This is the case of some services relying on GNSS civil signals. In fact, the menace of intentional radio-frequency interference, such as jamming or spoofing attacks, is gaining momentum, and discussions are being held, trying to find ways to protect GNSS civil users from these attacks.

Nowadays, the effects of these intentional interferences, which are able to compromise the correct functioning of the GNSS receivers are well known [1]–[5], and the need for improving the security of the receiver has been demonstrated [6], [7], especially in case of applications whose malfunctioning would put people's safety at risk.

Among the different interference attacks that can affect GNSSs, one of the most dangerous is the spoofing attack. It consists of the transmission of GNSS-like signals, aligned with the satellite signals, with the goal of taking control of the position-velocity-time (PVT) solution that the receiver computes. In this way, the attacker is able to fake the target position without being noticed and may cause severe damage to the applications relying on the GNSS signal.

Several spoofing countermeasure techniques have been proposed in the open literature and they can be generally divided into two main categories, namely spoofing detection and spoofing mitigation [8], [9]. Spoofing detection algorithms concentrate on detecting the presence of spoofing attack while spoofing mitigation techniques aim to neutralize the spoofing threat and help the target GNSS receiver to recover its positioning capability. Spoofing countermeasures can take place at any of the operational layers of a GNSS receiver, namely at the signal processing level, data bit level and/or position solution and navigation level [10].

Spoofing countermeasure methods look for specific features of spoofing signals that make them different from the authentic ones. Some of the previously proposed countermeasure techniques can be enumerated as received signal strength (RSS)

monitoring, received signal time of arrival (TOA) monitoring, spatial coherency analysis of received GNSS signals, signal quality monitoring (SQM), cryptographic authentication, receiver autonomous integrity monitoring (RAIM) and consistency check among different sensors and constellations [11]–[14].

In this context, the contribute of this Thesis is to provide a performance evaluation of the SMQ techniques against a proposed attack, that is optimal in the sense of energy used by the attacker. The Thesis is structured as follows:

- Chapter 2 provides a brief description of the existing GNSS systems, followed by a brief description of their general architecture; then, a delineation of the structure of the GNSS signals emitted by a satellite is presented, succeed by a characterization of the the building blocks of a typical GNSS receiver, that is antennas, front end, baseband processing and application processing.
- Chapter 3 presents the general model of a spoofing attack, the spoofing generation techniques and receiver state vulnerability to spoofing are investigated; finally different cases of spoofing attacks are illustrated.
- Chapter 4 reviews different detection and mitigation spoofing countermeasures, restricting the whole set of techniques to those that operate in the signal processing level of the receiver.
- Chapter 5 describes the signal quality monitoring techniques and illustrates the functioning of the nulling attack and of the proposed optimal spoofing attack.
- Chapter 6 outlines the simulation scenario, presents figures and comments the results obtained.
- Finally, Chapter 7 draws some conclusions and suggests possible future research topics that will continue the work of this Thesis.

Chapter 2

An Introduction to GNSS

As the years pass by, the GNSSs are becoming an invisible technology, used by a big portion of the society, but one that is not fully understood by the typical user. As a consequence, the innovative uses and the possible threats to GNSSs are also unknown. The United States (U.S.) GPS has been around for more than 20 years now, and people have adopted the use of navigation systems in everyday life, to the point where paper maps are becoming obsolete and everyone owns a GNSS receiver in some form. Knowledge of the basic operation of GNSS, and understanding of its limitations and risk, should be an important topic for the general user.

The goal of this Chapter is to present a condensed and brief summary on the GNSS functional basics and to introduce the knowledge needed to follow the discussions presented throughout this report. This Chapter is based mainly on the analysis done in [15], [16].

2.1 GNSS Systems

In this section we introduce the major GNSS systems available at the time of writing and their status.

GPS The GPS is the U.S. GNSS which provides free positioning and timing services worldwide. GPS receivers compute their position in the GPS Reference System using satellite technology and based on triangulation principles. Originally developed for the U.S. military, the incident with the Korean Air Lines Flight 007 led the US Government to decide to make GPS use free for civilian purposes very early in the experimental phase of GPS. The launch of the first Block I Navstar GPS satellite meant the beginning of the deployment of the GPS system on 22 February 1978, followed by the declaration of the Initial Operating Capability in December 1993 with 24 operational satellites in orbit, and the Full Operational Capability in June 1995. GPS is maintained by the United States government and is freely accessible by anyone with a GPS receiver. The Department of Defense is responsible for operating the system, but it also receives national-level attention and guidance through the National Executive Committee for space-based positioning, navigation, and timing (PNT).
Two services are available in the current GPS system:

- The standard positioning service (SPS) is a positioning and timing service available to all GPS users.
- The precise positioning service (PPS) is highly accurate positioning, velocity and timing service restricted by cryptographic techniques to military and authorized users.

Galileo The Galileo program is Europe's initiative for a state-of-the-art global satellite navigation system, providing a highly accurate, guaranteed global positioning service under civilian control. While providing autonomous navigation and positioning services, Galileo will be interoperable with other GNSS systems such as GPS and GLONASS. In full operational capability (FOC) phase, the system will consist of 30 satellites, to be deployed in a staggered approach, and the associated ground infrastructure.
The services that are planned to be provided by Galileo are the following:

- The open service (OS) provides position and timing information, free of user charge, that competes in performance with other GNSS systems.
- The commercial service (CS) improves accuracy and higher data throughput with a user fee.
- The public regulated service (PRS) provides navigation and timing for authorized users, with high continuity and accuracy.
- The search and rescue service (SAR) broadcasts globally alerts and distress signals received by the satellite and communicates back an acknowledgment signal.
- The safety-of-life (SoL) Service consists of an augmentation signal to the OS intended for most transport safety critical applications.

GLONASS The Russian GNSS, called GLONASS, has been operational since 1993 and achieved optimal status in 1995 with 24 satellites. Following completion, the system fell into disrepair with the collapse of the Russian economy and the reduction in funding for space industry. Since year 2000, the Russian government has been working for the restoration of the system, updating their satellites and designing modern signals to be broadcast. In October 2011, the full orbital constellation of 24 satellites was restored, enabling full global coverage and providing Standard Positioning Service and Precise Positioning Service similar to GPS.

BeiDou The BeiDou navigation satellite system (BDS) is China's second-generation satellite navigation system that will be capable of providing positioning, navigation, and timing services to users on a continuous worldwide basis. Although the evolution of its regional navigation system towards a global solution started in 1997, the formal approval by the Government of the development and deployment of BDS System was done in 2006 and it is expected to provide global navigation services by 2020.
The BeiDou supports both global worldwide services and regional services. The global services are the Open Service and the Authorized Service, which are similar to, respectively, SPS and PPS of GPS. The regional services can be further sub-divided in two other services: the Wide Area Differential Service consists of an augmentation signal to reach one meter positioning accuracy and the Short Message Service consists in allowing the user and the station to exchange short messages.

2.2 GNSS Segments

This Section provides a brief overview of the main components of a GNSS system.

As illustrated in Fig. 2.1, a GNSS basically consists of three main segments: the space segment, which comprises the satellites; the control segment (also referred to as

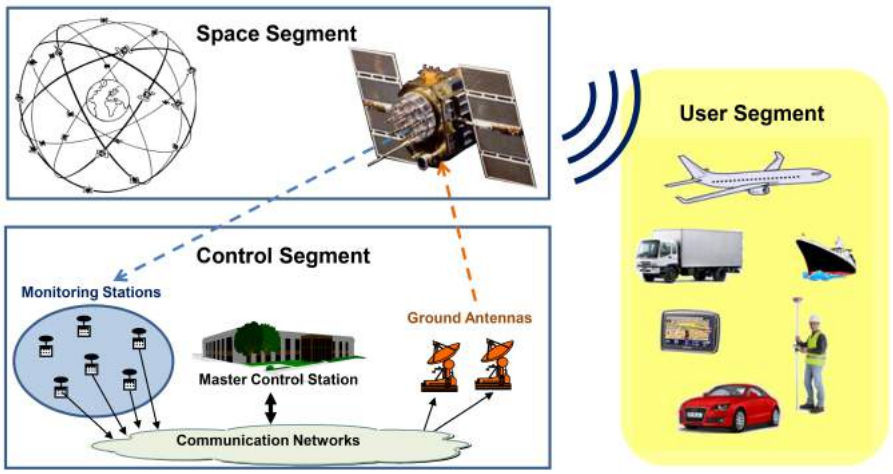


FIGURE 2.1: GNSS architecture. From [15].

the ground segment), which is responsible for the proper operation of the system; and the user segment, which includes the GNSS receivers providing positioning, velocity and precise timing to users.

Space Segment The main functions of the space segment are to generate and transmit code and carrier phase signals, and to store and broadcast the navigation message uploaded by the control segment. These transmissions are controlled by highly stable atomic clocks onboard the satellites.
The GNSS space segments are formed by satellite constellations with enough satellites to ensure that users will have at least four satellites in view simultaneously from any point on Earth's surface at any time.

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

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

User Segment The user segment is composed of GNSS receivers. Their main function is to receive GNSS signals, determine pseudoranges (and other observables) and solve the navigation equations in order to obtain the coordinates and provide a very accurate time.
The basic elements of a generic GNSS receiver are: an antenna with preamplification, a radio frequency section, a microprocessor, an intermediate-precision oscillator, a feeding source, some memory for data storage and an interface with the user. The calculated position is referred to the antenna phase centre.

2.3 GNSS Signals

In this Section we present the basic structure of the GNSS signals and describe briefly their different components and characteristics.

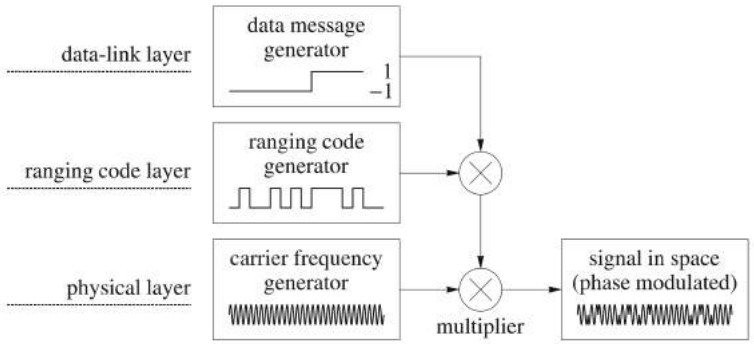


FIGURE 2.2: Composition of the navigation satellite signal. From [17].

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

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

Therefore, a generic unmodulated GNSS signal emitted by a satellite, denoted as signal in space (SIS), can be written as:

$$s(t) = \sqrt{2P}C(t)D(t)\cos\left(2\pi f_{\mathrm{RF}}t + \phi_0\right), \tag{2.1}$$

where P is the average power of the sinusoidal signal and ϕ_0 is the initial phase. In Fig. 2.2 is represented an example of carrier, code and data signals together with the resulting SIS.

Frequency allocation The allocation of frequency bands is a complex process because multiple services and users can fall within the same range. That is, the same frequencies can be allocated for different purposes in different countries. The international telecommunication union (ITU) is a United Nations agency coordinating the shared global use of the radio spectrum. It involves, for instance, television, radio, cell (mobile) phone, radar satellite broadcasting, etc., and even microwave ovens. The ITU divides the electromagnetic spectrum into frequency bands, with different radio services assigned to particular bands.
Figure 2.3 shows the frequency bands for the radionavigation satellite service (RNSS), that is a radiodetermination-satellite service used for the purpose of radionavigation, and for the aeronautical radionavigation service (ARNS), which is a radionavigation service intended for the benefit and for the SoL applications.

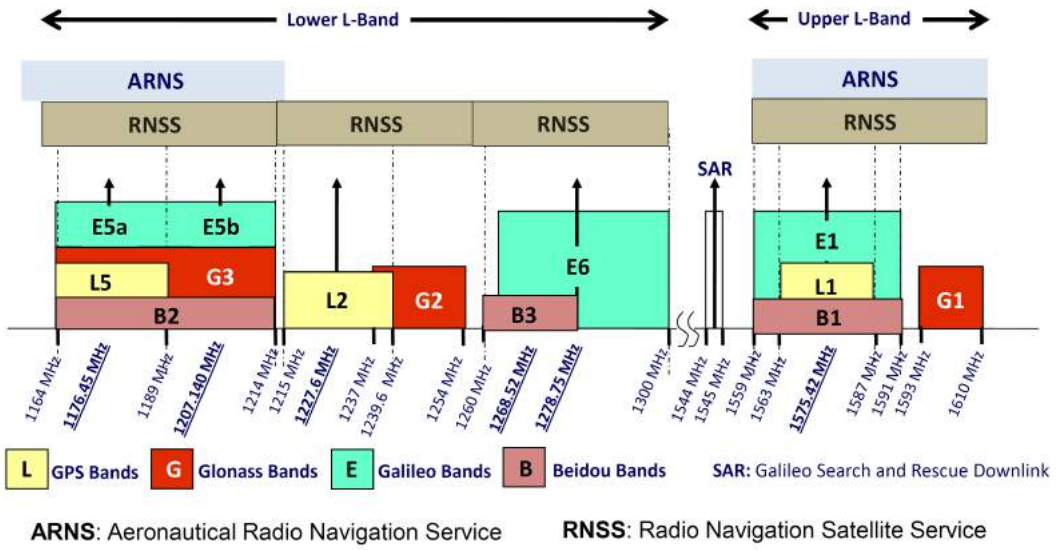


FIGURE 2.3: GPS, Glonass, Galileo and Beidou navigational frequency bands. From [15].

2.3.1 GPS Signals

Legacy GPS signals are transmitted on two radio frequencies in the L band, referred to as Link 1 (L1) and Link 2 (L2). They are right-hand circularly polarized (RHCP) and their center frequencies are derived from a fundamental frequency $f_0 = 10.23\,\text{MHz}$, generated by onboard atomic clocks: $f_{\text{L1}} = 154 \times 10.23\,\text{MHz} = 1575.420\,\text{MHz}$ and $f_{\text{L2}} = 120 \times 10.23\,\text{MHz} = 1227.600\,\text{MHz}$.
The GPS uses the code division multiple access (CDMA) technique to send different signals on the same radio frequency, and the modulation method used is binary phase shift keying (BPSK).
The following types of PRN codes are modulated over the two carriers:

- Coarse/Acquisition (C/A) code, also known as civilian code $C(t)$: this sequence contains 1023 bits and is repeated every millisecond (i.e., a chip rate of $R_c = 1.023\,\text{Mbps}$). Then, the duration of each C/A code chip is $T_c = 1\,\mu\text{s}$, which means a chip width or wavelength of 293.1 m. This code is modulated only on L1. The C/A code defines the SPS.

- Precision code, $P(t)$: This is reserved for military use and authorized civilian users. The sequence is repeated every 266 days (38 weeks) and a weekly portion of this code is assigned to every satellite. Its chip rate is 10 Mbps, which leads to a wavelength of 29.31 m. This code defines the PPS.
  In order to protect military receivers against an adversary transmitting a faulty copy of the GPS signal to mislead the receiver, and to deny access of non authorized users to the precise ranging code P, the latter is encrypted by combining it with a secret W code (called security code), resulting in the Y code, which is modulated over the two carriers L1 and L2.

The resulting SIS emitted by a satellite takes the following form (see Fig. 2.4):

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

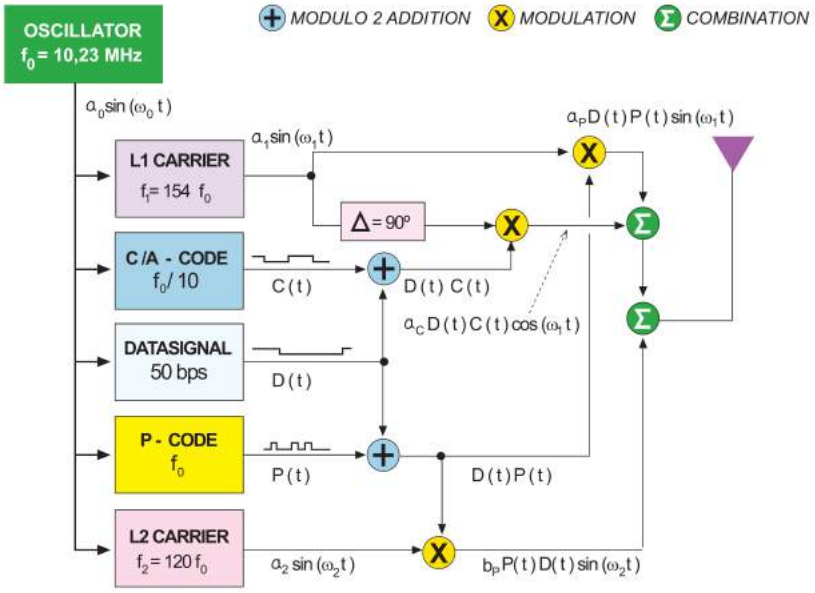


FIGURE 2.4: Legacy GPS signal structure. From [15].

where

$$s_{L1}(t) = \sqrt{2P_{P,1}}W(t)P(t)D(t)\sin\left(2\pi f_{L1}t + \phi_{L1}\right) + \sqrt{2P_C}C(t)D(t)\cos\left(2\pi f_{L1}t + \phi_{L1}\right), \tag{2.3}$$

$$s_{L2}(t) = \sqrt{2P_{P,2}}W(t)P(t)D(t)\sin\left(2\pi f_{L2}t + \phi_{L2}\right). \tag{2.4}$$

Finally, Table 2.1 contains a summary of the current GPS signals, frequencies and applied modulations. The ranging code rate and data rate are also given in the table.

Navigation message Every satellite receives from the ground antennas the navigation data, which are sent back to users through the navigation message. The navigation message contains all the necessary information to allow users to perform the positioning service. This includes the ephemeris parameters, needed to compute the satellite coordinates with sufficient accuracy, the time parameters and clock corrections, needed to compute satellite clock offsets and time conversions, the service parameters with satellite health information, the ionospheric parameters model, needed for single-frequency receivers, and the almanacs, allowing computation of the position of "all satellites in the constellation", with a reduced accuracy, which is needed for acquisition of the signal by the receiver. The ephemeris and clock parameters are usually updated every two hours, while the almanac is updated at least every six days.

TABLE 2.1: Current GPS navigation signals. From [15].

Link	Carrier freq. (MHz)	PRN code	Modulation type	Code rate (Mcps)	Data rate (bps)	Service
L1	1575.420	C/A	BPSK(1)	1.023	50	Civil
		P	BPSK(10)	10.23	50	Military
L2	1227.600	P	BPSK(10)	10.23	50	Military

TABLE 2.2: Galileo navigation signals. The PRN codes relative to PRS signals are encrypted. The two signals located in the E5a and E5b bands respectively are modulated onto a single E5 carrier frequency of 1191.795 MHz using the AltBOC technique: AltBOC(15,10). From [15].

Link	Carrier freq. (MHz)	Signal and channel	Modulation type	Code rate (Mcps)	Data rate (bps)	Services
E1	1575.420	E1-A data	$BOC_{cos}(15,2.5)$	2.5575	N/A	PRS
		E1-B data	MBOC(6,1,1/11)	1.023	125	OS, CS, SoL
		E1-C pilot			–	
E6	1278.750	E6-A data	$BOC_{cos}(10,5)$	2.5575	N/A	PRS
		E6-B data	BPSK(5)		500	CS
		E6-C pilot			–	
E5a	1176.450	E5a-I data	BPSK(10)	10.23	25	OS
		E5a-Q pilot			–	
E5b	1207.140	E5b-I data	BPSK(10)	10.23	125	OS, CS, SoL
		E5b-Q pilot			–	

As, anticipated, the current "legacy" navigation message (NAV) is modulated on both carriers at 50 bps. The whole message contains 25 pages (or "frames") of 30 s each, forming the master frame that takes 12.5 min to be transmitted. Every frame is subdivided into five subframes of 6 s each; in turn, every subframe consists of 10 words, with 30 bits per word. A full description of the GPS message structure can be found in [15].

GPS Signal Modernization The goal of modernization for the civil service is to improve accuracy, availability, coverage, integrity and robustness. In order to do so, modernization has introduced new civil signals (L2C, L5 and L1C) and frequencies (L5) in order to provide the user with increased redundancy, possibilities for ionospheric corrections and higher accuracy.

2.3.2 Galileo Signals

In FOC phase, each Galileo satellite will transmit 10 navigation signals in the frequency bands E1, E6, E5a and E5b, each right-hand circularly polarized. These signals can contain data and pilot channels. Both channels provide ranging codes, but the data channels also include navigation data. Pilot channels are data-less signals, so no bit transition occurs, thus helping the tracking of weak signals.
As in GPS, all satellites share the same frequencies, and the signals are differentiated by the CDMA technique, while the modulation methods used are BPSK and binary offset carrier (BOC) (and a couple of its variants), depending on the signal component.

A summary of Galileo signals, frequencies and applied modulations is presented in Table 2.2. The ranging code rate and data rate are also given in the table.

Navigation message The Galileo satellites will broadcast five types of data in four navigation messages: the freely accessible navigation message (F/NAV), similar to the NAV of GPS, the integrity navigation message (I/NAV), the commercial navigation message (C/NAV) and the governmental navigation message (G/NAV).

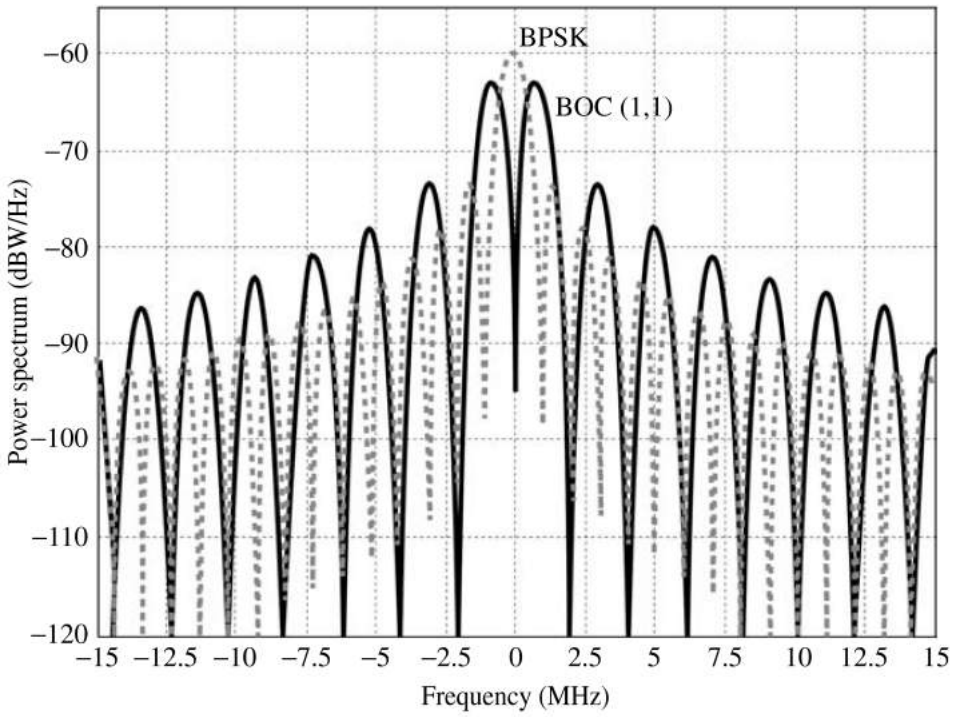


FIGURE 2.5: Power spectral density of a BOC(1,1) and BPSK-modulated signals. From [18].

The complete navigation message is transmitted on each data channel as a sequence of frames. A frame comprises a certain number of subframes, and a subframe comprises several pages. A full description of the Galileo message structure can be found in [15].

BOC modulation The BOC modulation consists in multiplying the PRN code of chip rate $R_c = m \times 1.023\,\text{Mcps}$ with a rectangular sub-carrier of frequency $f_s = n \times 1.023\,\text{MHz}$. The BOC signal is referred to as BOC(f_s,R_c) or, for simplicity, BOC(n,m).
The main idea behind BOC modulation is to reduce the interference with BPSK-modulated signals, which has a sinc function shaped spectrum. Indeed, BPSK-modulated signals have most of their spectral energy concentrated around the carrier frequency, while BOC-modulated signals have low energy around the carrier frequency and two main spectral lobes further away from the carrier and, more precisely, centered at frequencies $f_{\text{RF}} \pm nR_c$. As an example, Fig. 2.5 shows the PSD of a BPSK signal against the PSD of a BOC(1,1) signal.
The BOC modulation has several variants and, as can be seen in Table 2.2, those selected for Galileo are BOC_{sin}, BOC_{cos}, MBOC and AltBOC.

2.4 GNSS Receivers

In this Section a brief explanation of the functionality of a GNSS receiver is provided and the general GNSS receiver architecture is described.

GNSS receivers are responsible for processing the L-band SIS coming from the GNSS satellites in order to determine the user position, velocity, and precise time. Most GNSS receivers have a similar block diagram, although some architecture

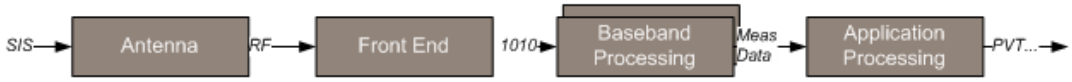


FIGURE 2.6: Generic receiver architecture. From [18].

variations might be present to accommodate different solutions. The basic building blocks of a generic GNSS receiver are as shown in Fig. 2.6.

2.4.1 Antennas

GNSS antennas are RHCP and aim at capturing GNSS signals in the L-band, with the associated amplification and filtering. It is the entry point from the space segment to the user segment, as it receives the L-band signals to pre-process and feed as an analog electrical signal to the front end.
When designing a GNSS antenna, the main objective is to maximize the antenna gain towards emitting satellites above a given elevation angle, while rejecting multipath signals (usually at lower elevation angles) and interference. The design of the antenna has to cope with the environmental conditions of the target application, while respecting mobility, power and size constraints. Usually GNSS antennas present hemispherical radiation patterns that can reject multipath coming from low elevation angles.
As far as interference is concerned, antenna arrays can be used to modify the radiation pattern so as to reject signals coming from the direction of the interferer. In addition, beam steering techniques are often employed to "follow" the signal from a given satellite with maximum gain.

From Eq. (2.1), the received signal for a visible satellites at the end of a receiver antenna can be modeled as

$$r_{\mathrm{RF}}(t) = a\sqrt{2P}D(t - t_{\mathrm{p}})C(t - \tau)\cos\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D}})(t - t_{\mathrm{p}}) + \phi_0\right] + n_{\mathrm{RF}}(t) \tag{2.5}$$

with

$$f_{\mathrm{D}} = -\frac{f_{\mathrm{RF}}}{c}\frac{\mathrm{d}t_{\mathrm{p}}}{\mathrm{d}t}\,, \tag{2.6}$$

where a is the path attenuation, t_{p} is the propagation time, τ is the propagation time modulo the code period, denoted as code delay, f_{D} is the carrier Doppler frequency shift (Hz) and $n_{\mathrm{RF}}(t)$ is the additive noise component at RF. In order to simplify the notation, Eq. (2.5) can be rewritten as

$$r_{\mathrm{RF}}(t) = AD(t - t_{\mathrm{p}})C(t - \tau)\cos\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D}})t + \phi\right] + n_{\mathrm{RF}}(t)\,, \tag{2.7}$$

where A is the signal amplitude taking into account the signal power as well as the attenuation factor and $\phi = \phi_0 - 2\pi(f_{\mathrm{IF}} + f_{\mathrm{D}})t_{\mathrm{p}}$ is the carrier phase offset in addition to the Doppler shift.

2.4.2 Front End

The GNSS signal captured through the receiver's antenna is fed to the front end section. The front end is then responsible for "preparing" the received signals for signal processing tasks, and many different implementations can achieve the desired results. As always, some requirement and trade-off analysis is needed when designing a front-end for GNSS receivers, depending on the application at hand. Figure 2.7 illustrates a typical front end structure in GNSS receivers.

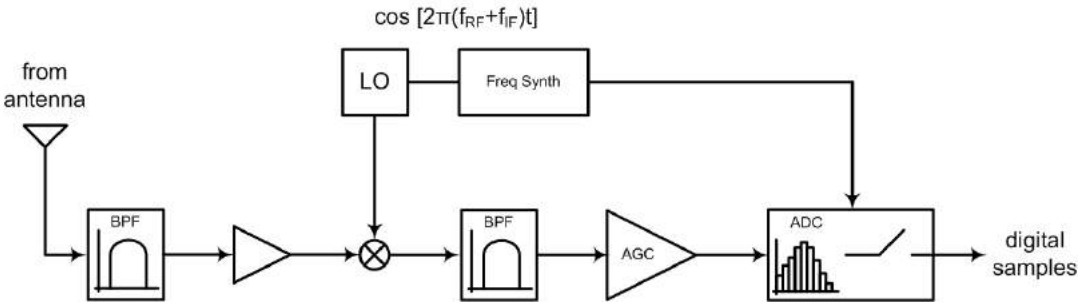


FIGURE 2.7: Example of GNSS receiver's front end structure. From [15].

The frequency synthesizer provides the receiver with time and frequency reference for all the front end components. Such components, at front end architecture level, gather typical interconnected steps to process and convert a RF signal to a baseband digital signal:

- Filtering and amplification: these stages are necessary to ensure low noise and out-of-band rejection in the received signals, as well as amplification stages to compensate for transmission losses.
- Down-conversion: the front end is responsible for down-converting the input signal from RF to intermediate frequency (IF). This is achieved through signal mixing operations which consist in mixing two different frequency signals in order to shift the same information at two different frequencies, where one is the sum of the two frequencies mixed, and the other is their difference. The basis of the mixing process is the local oscillator (LO), which must be carefully chosen to avoid harmonics and image frequencies near IF.
- Quantization: the incoming signals are digitized through analog to digital converters (ADC), ensuring that quantization errors and dynamic ranges are appropriate to accommodate the signal's characteristics.
- Automatic Gain Control: the automatic gain control (AGC) stage is closely related to the downconversion and quantization steps, and is responsible for adjusting the gain of the front end section in order to take benefit from the full dynamic range.

From Eq. (2.5), the signal at the end of the front end for a single satellite can be modeled as

$$\begin{aligned} r_{\mathrm{IF}}(k) = AD(kT_{\mathrm{s}} - t_{\mathrm{p}})C(kT_{\mathrm{s}} - \tau)\cos\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D}})kT_{\mathrm{s}} + \phi\right] \\ + n_{\mathrm{IF}}(t) \qquad \text{for } k = 0, 1, 2, \dots, \end{aligned} \tag{2.8}$$

where T_{s} is the sampling time interval (s) such that $t = kT_{\mathrm{s}}$ and n_{IF} is the corresponding noise at IF.

2.4.3 Baseband signal processing

The baseband processing block is responsible for processing the down-converted and digitized GNSS signal in order to provide observables: code pseudoranges and carrier phase measurements, as well as navigation data.
In most GNSS receivers' architectures, the baseband processing relies on independent channels that track each satellite signal autonomously. Then, the information from

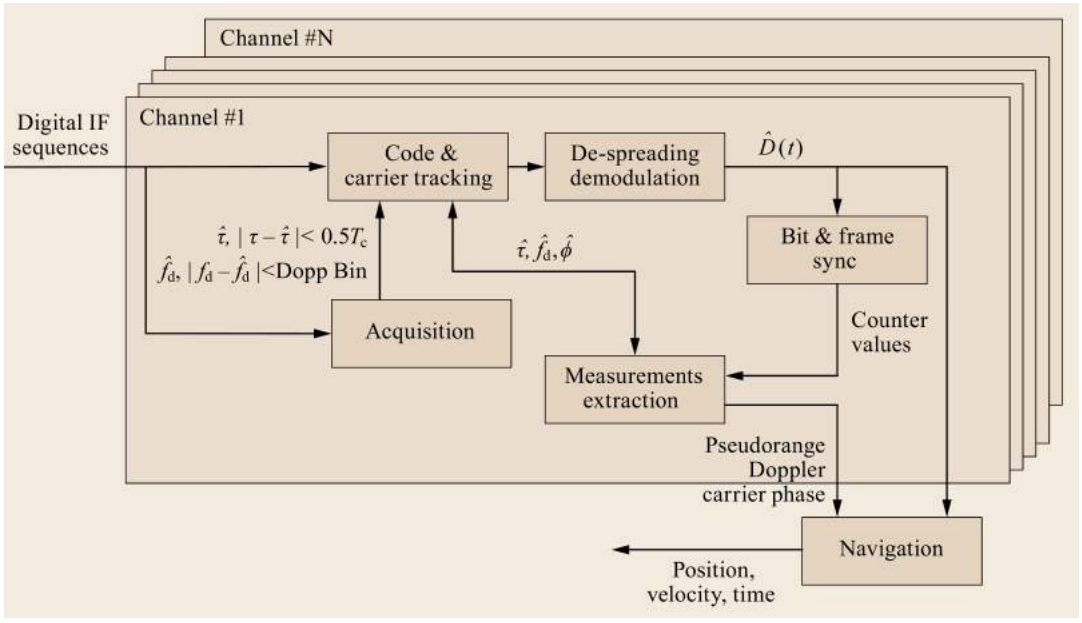


FIGURE 2.8: Block diagram of internal functions in a generic baseband processing block. From [16].

each channel is integrated to derive a navigation solution. Figure 2.8 shows the main components of the baseband processing block.

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

$$\begin{aligned} r(k;\tau,\phi,f_{\mathrm{D}},A) = AD(kT_{\mathrm{s}}-\tau)C(kT_{\mathrm{s}}-\tau)\mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}}+f_{\mathrm{D}})kT_{\mathrm{s}}+\phi\right]} \\ + n(kT_{\mathrm{s}}) \qquad \text{for } k = 0,1,2,\ldots, \end{aligned} \tag{2.9}$$

where

$$n(kT_{\mathrm{s}}) \sim \mathcal{CN}\left(0,\sigma_n^2\right), \tag{2.10}$$

is the complex additive Gaussian noise with zero mean and variance σ_n^2 (see Appendix A for the relation between σ_n^2 and C/N_0). Moreover, T_{s} is the sampling time interval, f_{IF} is the IF at which the signal is down-converted by the front end, D is the navigation data symbol sequence and C is the spreading code sequence with a chip duration of T_c. Finally, A is the signal amplitude, τ is the code delay, f_{D} is the carrier Doppler frequency shift and ϕ is the carrier-phase delay. For the sake of simplicity, the dependency of the various functions on τ, ϕ, f_{D} and A will be dropped.
Assuming the navigation data bit does not change in the integration time interval, the locally generated replica signal component of a visible GNSS satellite at the IF, without the use of amplitude and navigation data bit, can be modeled as

$$\hat{r}_{\mathrm{IF}}(k) = C(kT_{\mathrm{s}}-\hat{\tau})\mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}}+\hat{f}_{\mathrm{D}})kT_{\mathrm{s}}+\hat{\phi}\right]}. \tag{2.11}$$

The correlation operation is given by

$$\text{corr}\left[r(k), \hat{r}(k)\right] = \frac{1}{M}\sum_{k=1}^{M} r(k)\hat{r}^*(k)\,, \tag{2.12}$$

where $\text{corr}(x, y)$ is the correlation function of x and y and M is the number of samples within the coherent integration time $T_{\text{coh}} = MT_{\text{s}}$, which is usually shorter or equal to the navigation data bit period.
From the computations in [16], the correlator output, also called cross ambiguity function (CAF), can be written as

$$S = ADR(\Delta\tau)\,\text{sinc}\left(\Delta f_{\text{D}} T_{\text{coh}}\right)\text{e}^{j\left(\Delta\phi + \pi\Delta f_{\text{D}} T_{\text{coh}}\right)} + \eta \tag{2.13}$$

where

$$\eta \sim \mathcal{CN}\left(0, \sigma_\eta^2\right)\,, \tag{2.14}$$

is the noise after the correlation operation, $\Delta\tau = \tau - \hat{\tau}$ is the code delay error, $\Delta\phi = \phi - \hat{\phi}$ is the carrier phase error, $\Delta f_{\text{D}} = f_{\text{D}} - \hat{f}_{\text{D}}$ is the Doppler error and $R(\Delta\tau)$ is the normalized autocorrelation function (ACF) of $C(kT_{\text{s}})$ at lag $\Delta\tau$. In Eq. (2.13) the sinc function is defined as $\text{sinc}(x) = \sin(\pi x)/(\pi x)$. The in-phase and quadrature components of the CAF are given by

$$I = ADR(\Delta\tau)\,\text{sinc}(\Delta f_{\text{D}} T_{\text{coh}})\cos\left(\Delta\phi + \pi\Delta f_{\text{D}} T_{\text{coh}}\right) + \eta_I\,, \tag{2.15}$$

$$Q = ADR(\Delta\tau)\,\text{sinc}(\Delta f_{\text{D}} T_{\text{coh}})\sin\left(\Delta\phi + \pi\Delta f_{\text{D}} T_{\text{coh}}\right) + \eta_Q\,, \tag{2.16}$$

where η_I and η_Q represent the noise in I and Q respectively.
Finally, it is useful to specify the notation

$$S_{\pm\alpha} = ADR(\Delta\tau \pm \alpha)\,\text{sinc}\left(\Delta f_{\text{D}} T_{\text{coh}}\right)\text{e}^{j\Delta\phi} + \eta = I_{\pm\alpha} + jQ_{\pm\alpha}\,, \tag{2.17}$$

to indicate the output of a particular correlator whose delay is $\pm\alpha$ chips from the prompt one, that is

$$\hat{r}_{\mp\alpha}(k) = C(kT_{\text{s}} - \hat{\tau} \mp \alpha)\text{e}^{j\left[2\pi(f_{\text{IF}} + \hat{f}_{\text{D}})kT_{\text{s}} + \hat{\phi}\right]}\,. \tag{2.18}$$

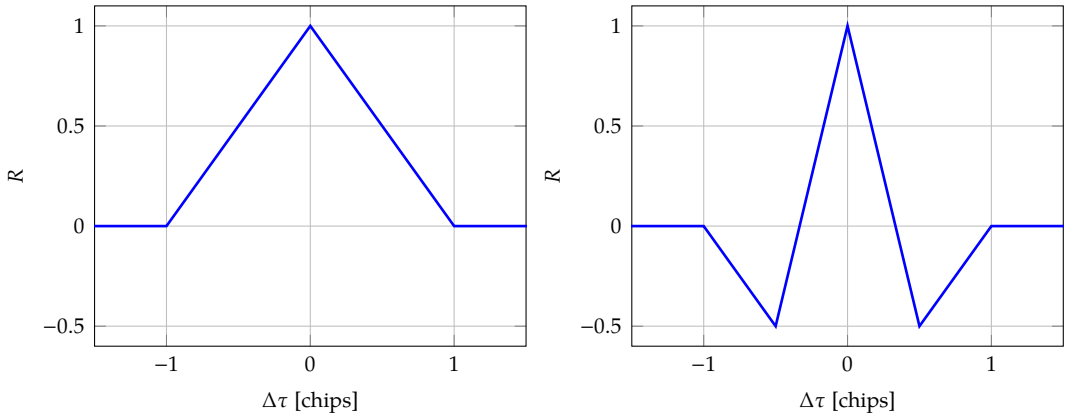
Using this notation, we can define the prompt correlator as $S_{\text{P}} = S_0$. Moreover, correlators with $-\alpha$ are called early correlators, while those with $+\alpha$ are called late correlators; if an early and a late correlator have the same α, their distance in chips is called early-late spacing $d = 2\alpha$.

In order to clarify the concept of ACF, a pair of examples (in particular, for the two code signals that will be used for testing the signal quality monitoring [SQM] metrics) are reported:

- **BPSK(1) signal**. The ACF of a BPSK(1) signal, like the GPS C/A code signal, takes the approximative form

$$R(\Delta\tau) = \begin{cases} 1 - \frac{|\Delta\tau|}{T_c} & \text{for } |\Delta\tau| \le T_c\,, \\ 0 & \text{for } |\Delta\tau| > T_c\,, \end{cases} \tag{2.19}$$

  that is represented in Fig. 2.9a.



(A) BPSK(1) signal. (B) BOC(1,1) signal.

FIGURE 2.9: Normalized ACF of two differently modulated signals.

- **BOC(1,1) signal**. The ACF of a BOC(1,1) signal, whose alternative versions are be adopted in some Galileo code signals, takes the approximative form

$$R(\Delta\tau) = \begin{cases} 1 - \frac{3|\Delta\tau|}{T_c} & \text{for } |\Delta\tau| \leq T_c/2\,, \\ -1 + \frac{|\Delta\tau|}{T_c} & \text{for } T_c/2 < |\Delta\tau| \leq T_c\,, \\ 0 & \text{for } |\Delta\tau| > T_c\,, \end{cases} \tag{2.20}$$

  that is represented in Fig. 2.9b.

Acquisition The goal of the acquisition stage is to identify which satellites are in view and to obtain the code delay τ and the Doppler frequency shift f_D, for each satellite signal present, so the tracking stage can refine these estimates and obtain an accurate solution. The signal search can intuitively be seen as a numerical evaluation of the signal's correlation function in the two-dimensional Doppler and code phase space. If the peak magnitude of this function exceeds a certain threshold, then the signal is declared to be present and the position of the peak are the coarse estimates. From a theoretical point of view, this picture can be translated in a generalized maximum likelihood ratio test (GLRT).

In the theory of signal detection, signal acquisition has to decide which of the following hypotheses is true:

H_0: Considered satellite signal is not present

H_1: Considered satellite signal is present.

The acquisition engine evaluates the total power

$$|S|^2 = A^2 R(\Delta\tau)^2 \operatorname{sinc}(\Delta f_D T) + \text{noise} = I^2 + Q^2 \tag{2.21}$$

for a certain range of Doppler and code-phase values, searches the peak within this area and compares the value of the peak against a threshold γ. If the peak exceeds the threshold, the hypothesis H_1 is declared to be true, otherwise H_0. To increase the sensitivity one can increase the coherent integration time T. Under the assumption of a signal being present, the total power S assumes the shape of a peak like the one shown in Fig. 2.10. A further sensitivity increase is achieved by a noncoherent

integration; that is to compute the correlation function several (= ν) times and to average them:

$$S_{\text{nc}} = \sum_{n=1}^{\nu} |S_n|^2 \,, \tag{2.22}$$

where n denotes subsequent coherent integrations each over an interval of T. The total integration time is $T_{\text{tot}} = T\nu$.
Mathematically speaking, the function S_{nc} is the sum of 2ν squared zero-mean Gaussian random variables (each coherent integration has a contribution from the real I and the imaginary Q part) under the assumption H_0, and S_{nc} follows a central chi-squared distribution with right-tail probability $Q_{\chi^2;\alpha}$, where $\alpha = 2\nu$ are the degrees of freedom. Therefore, the false alarm probability, that is the chance that the receiver incorrectly detects a signal even if it is not present, is given by

$$P_{\text{fa}} = P(S_{\text{nc}} > \gamma | H_0) = Q_{\chi^2;2\nu} \,. \tag{2.23}$$

Under H_1, the probability distribution of S_{nc} is a noncentral chi-squared distribution with right-tail probability $Q_{\chi^2;\alpha;z}$ and the noncentrality parameter $z = 2\nu TC/N_0$ relates to the carrier-to-noise ratio C/N_0 and the number of noncoherent integrations ν

$$P_{\text{d}} = P(S_{\text{nc}} > \gamma | H_1) = Q_{\chi^2;2\nu;2\nu TC/N_0} \,. \tag{2.24}$$

The term $P(S_{\text{nc}} > \gamma | H_1)$ is the detection probability, that is the ability of the receiver to detect signals that are actually present. The threshold γ can be found by setting one of two probabilities of Eqs. (2.23) and (2.24) to the desired value.
Finally, the coarse estimation of code delay and Doppler frequency shift, for a given satellite/PRN code, is given by

$$\hat{\tau}^*, \hat{f}_{\text{D}}^* = \arg\max_{\hat{\tau}, \hat{f}_{\text{D}}} S_{\text{nc}} \,, \tag{2.25}$$

where the search space $\hat{\tau}, \hat{f}_{\text{D}}$ is usually discrete, as a sort of grid, that is $\hat{\tau} \in \{0, \tau_{\text{grid}}, 2\tau_{\text{grid}}, \ldots, T_c\}$ and $\hat{f}_{\text{D}} \in \{-f_{\text{d,max}}, -f_{\text{d,max}} + f_{\text{d,grid}}, \ldots, f_{\text{d,max}} - f_{\text{d,grid}}, f_{\text{d,max}}\}$, where τ_{grid} is the code resolution in chips, $f_{\text{d,max}}$ is the maximum reasonable Doppler frequency shift and $f_{\text{d,grid}}$ is the frequency resolution in Hertz.

Tracking After the coarse estimate of initial code delay and carrier Doppler by the acquisition block, the signal tracking is performed to obtain fine estimates of signal parameters of interest. The core of the tracking stage are the tracking loops, which are designated to adjust the input of the local replica signal generators to match the received signals. There exists three tracking loops architectures: phase-locked-loop (PLL) for carrier-phase tracking, frequency-locked-loop (FLL) for carrier Doppler frequency shift tracking, and delay-locked-loop (DLL) for code delay tracking. Figure 2.11 shows a high-level block diagram of a single-channel signal tracking engine in typical digital GNSS receivers.

The operation of the signal tracking engine is as follows. The carriers in the digital IF signal sequences are wiped off by the replica carrier signals to produce the I and Q signal components. The replica carrier signals are synthesized by the carrier generator using the carrier phase estimate generated by the PLL or the FLL.
The I and Q signal components are then correlated (i.e., mixed and integrated and dumped) with the replica codes at early, prompt, and late branches (for the most simple case of standard tracking of a BPSK signal). They are, similar to the previous

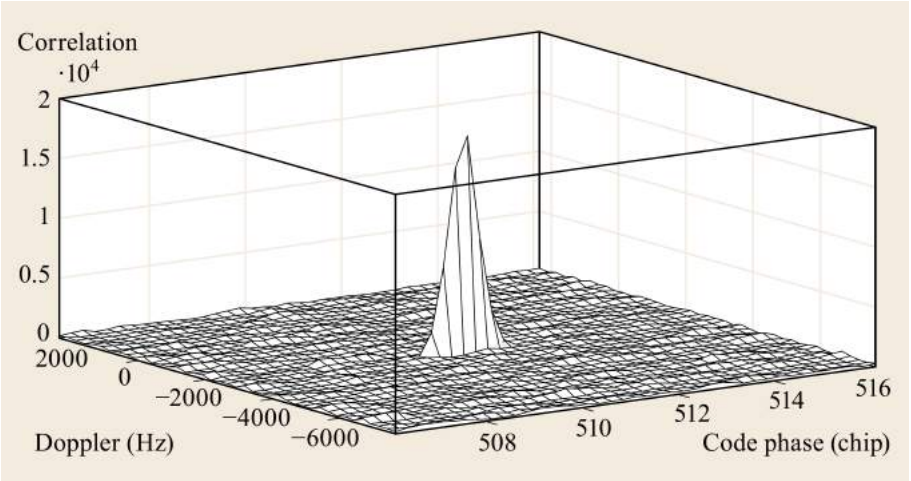


FIGURE 2.10: Example of GPS C/A correlation function during signal acquisition. From [16].

case, synthesized by the code generator with a 3 bit shift register using the code delay estimate generated by the DLL. Normally, the correlator output at prompt branches (I_P, Q_P) is used in the carrier tracking whereas the correlator output at early and late branches (I_E, Q_E and I_L, Q_L) are used in the code tracking.
After the correlation process there are the discriminators, which have the task to extract the signal parameter error information from the correlator outputs I and Q at the early, prompt, and late branches. The type of discriminator algorithm determines the type of tracking loop (i.e., PLL, FLL or DLL):

- **PLL and FLL Discriminators.** The carrier loop discriminator determines characteristics of the carrier tracking loop as a carrier-phase tracking loop or a carrier Doppler tracking loop. The carrier-phase tracking loops are more accurate but more sensitive to dynamic stress than the carrier Doppler tracking loop.
  For the carrier-phase tracking loop, there are mainly two types: a pure PLL and a Costas PLL. The pure PLL is sensitive to the presence of bit/symbol modulation on the signal. The Costas PLL is insensitive to that if the integration time of the correlator to produce the baseband I_P and Q_P does not straddle the data bit/symbol transitions. Under the assumption of no noise in Eqs. (2.15) and (2.16), the carrier-phase error can be obtained by

$$\frac{Q_P}{I_P} = \frac{\sin(\Delta\phi)}{\cos(\Delta\phi)} = \tan(\Delta\phi) \approx \Delta\phi \quad \text{for } \Delta\phi \approx 0 \qquad \Rightarrow \qquad \Delta\phi = \tan^{-1}\left(\frac{Q_P}{I_P}\right). \tag{2.26}$$

  For pure PLLs, the arctangent in Eq. (2.26) is substituted by a four-quadrant arctangent in order to remain linear over the full input error range of ±180°, whereas arctangent for Costas PLLs remains linear over half of the input error range (±90°).
  For the carrier Doppler tracking loop, the Doppler error can be obtained by

$$\Delta f_D = \frac{\tan^{-1}\left(\frac{I_{P,k}Q_{P,k+1} - I_{P,k+1}Q_{P,k}}{I_{P,k}I_{P,k+1} + Q_{P,k}Q_{P,k+1}}\right)}{T}, \tag{2.27}$$

  where k is used to index baseband samples and T is the coherent integration

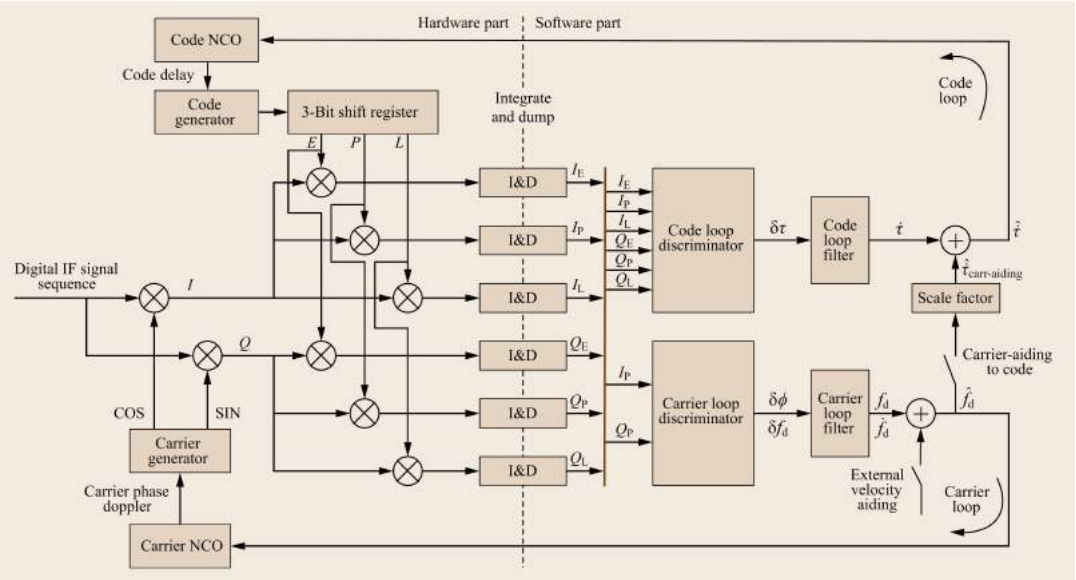


FIGURE 2.11: Block diagram of a GNSS signal tracking engine. From [16].

time. Intrinsically, the FLL tracks the carrier frequency and not the carrier phase so that the FLL discriminator is insensitive to ±180° phase reversals but its integration time must not straddle the navigation data bit/symbol transitions. Beside the discriminators described before, there are several variants of PLL and FLL discriminator algorithms that produce slightly different characteristics in terms of optimality depending on signal-to-noise ratio, integration time and computational complexity.

- **DLL Discriminators.** The DLL discriminator uses the early and late branches rather than the prompt branch of the carrier loop. Figure 2.12 shows how the early, prompt, and late correlators change as the offset of the locally generated code replicas are advanced with respect to the incoming satellite's code signal. If the replica code is aligned, then the early and late branches are equal in amplitude and no error is generated by the discriminator. If not, the early and late samples are not equal by an amount proportional to the code offset. From this idea can be derived the early-minus-late envelope discriminator:

$$\Delta\tau = \frac{1}{2}\frac{E-L}{E+L}, \tag{2.28}$$

where $E = \sqrt{I_{\mathrm{E}}^2 + Q_{\mathrm{E}}^2}$ and $L = \sqrt{I_{\mathrm{L}}^2 + Q_{\mathrm{L}}^2}$. Note that there are several variants of DLL discriminator algorithms that produce slightly different characteristics in terms of required coherent-noncoherent integrations, accuracy, availability depending on the carrier-lock condition, correlator spacing and computational complexity.
The DLL tracking becomes more fragile when considering BOC-modulated ranging codes and their ambiguous discriminator function. There are different concepts to avoid false tracking. One of them is to track only one sidelobe of the BOC frequency spectrum, consequently neglecting half of the energy in the signal. A method which takes full advantage of the BOC energy spectral spreading is the bump and jump technique, relying on two more correlators, a

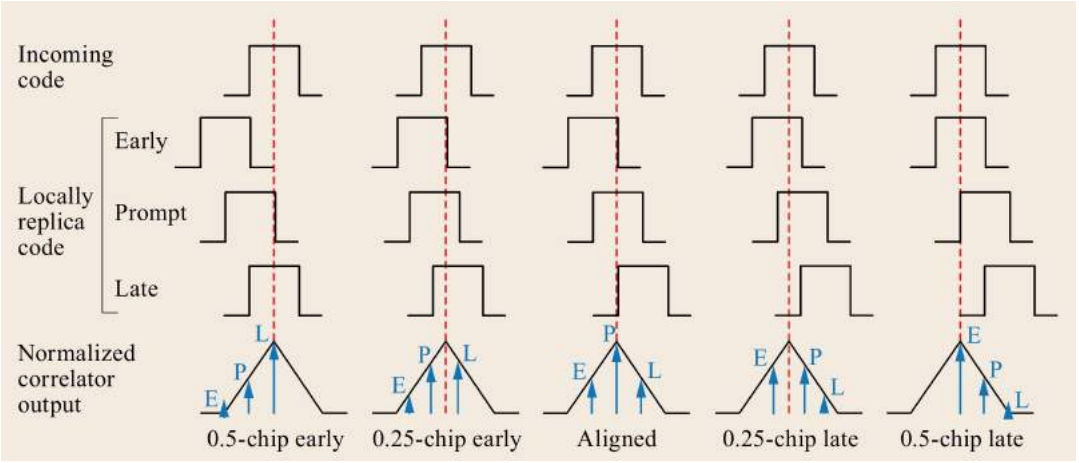


FIGURE 2.12: Early-minus-late DLL discriminator. From [16].

very early and a very late correlator.

The discriminator outputs contain much noise that should be efficiently filtered out by the loop filter. The output of the loop filter is the rate of change information of the signal parameter of interest (i.e., $\dot{\tau}$, $\dot{\phi}$, $\dot{f}_{\mathrm{D}}$) which is then integrated in the numerically controlled oscillator (NCO) to predict the signal parameter estimate (i.e., $\hat{\tau}$, $\hat{\phi}$, $\hat{f}_{\mathrm{D}}$) for the next step. This signal parameter estimate is used in the local signal generator to produce the estimated local replica signals for the correlation.

Time Synchronization and Data Demodulation While the tracking loops extract code and carrier information to synchronize the locally generated PRN code with the incoming signal, the synchronization, both at bit/symbol and frame level, and data demodulation stage aims at extracting the navigation message to be used by the applications processing block, when generating a navigation solution. The inputs are the measurements from the tracking loops (code and carrier information), as well as the sign of the prompt correlator outputs. In fact, when a signal is being correctly tracked, the sign of the prompt correlator output is positive when the transmitted navigation symbol is 1 and negative when the symbol is -1, by definition of correlation.

GNSS Measurements At this point, the receiver is tracking the incoming signal and has extracted the navigation message, and therefore can compute the observables, namely pseudorange and Doppler frequency. Although Doppler frequency is quite straight forward, and can be directly taken from the FLL or the instantaneous phase measured at the PLL, the pseudorange still needs to be computed from the code delay values provided by the DLL.

Considering a reference time scale T, the pseudorange to a given satellite can be computed as:

$$R = c(t_{\mathrm{r}}(T_2) - t^{\mathrm{s}}(T_1)) \tag{2.29}$$

where: c is the speed of light in a vacuum; $t_{\mathrm{r}}(T_2)$ is the time of signal reception, measured on the time scale given by the receiver clock T_2; and $t^{\mathrm{s}}(T_1)$ is the time of signal transmission, measured on the time scale given by the satellite clock T_1. In particular $t^{\mathrm{s}}(T_1)$ is extrapolated from sum of the time of the time stamp recorded by the satellite at the beginning of each subframe, the number of navigation data bits transmitted since the beginning of the subframe, the number of code periods since

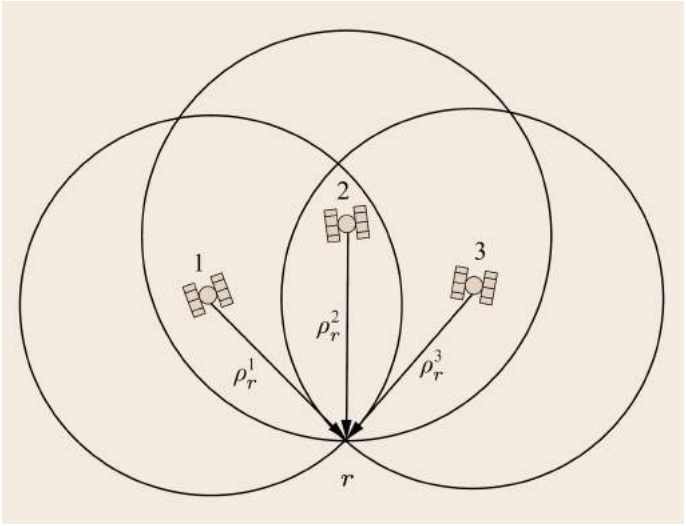


FIGURE 2.13: Positioning through intersecting spheres. From [16].

the beginning of the current navigation data bit, the number of chips elapsed in the current code cycle and, finally, the code delay provided by the DLL.

2.4.4 Application Processing

The applications processing block extracts observables and navigation data from each channel of the baseband processing block, and combines this information to satisfy the requirements of a given application.
The most common raw information provided by a GNSS receiver is the PVT information, but other information may still be used such as time and frequency transfer, static and kinematic surveying, ionospheric parameters monitoring, differential GNSS reference stations, GNSS signal integrity monitoring, etc.

PVT solution In order to calculate the user's PVT solution there exist two methods: single-frequency code-based positioning for standard point positioning (SPP) and dual-frequency code and carrier-based for precise point positioning (PPP). Here it is summarized the first one.

The aim is to determine the receiver coordinates $\mathbf{r} = (x; y; z)$ (using earth centered, earth fixed (ECEF) coordinates) and clock offset δt from pseudorange measurements R of at least four satellites in view. Indeed, the positioning principle is based on solving a trilateration problem where each satellite (with known coordinates) is the center of a sphere with radius the measured pseudorange and the user position is the point we want to find as intersection of the four (or more) spheres (see Fig. 2.13).
The pseudorange to a given satellite in Eq. (2.29) can be modeled as

$$R = \rho + c(dt_{\mathrm{r}} - dt^{\mathrm{s}}) + I + T + K_{\mathrm{r}} + K^{\mathrm{s}} + \epsilon_{\mathrm{mp}} + \epsilon_{\mathrm{n}}\,. \tag{2.30}$$

Here ρ denotes the geometric distance between the receive antenna at the reception epoch and the transmit antenna at the transmission epoch. Moreover, dt^{s} and dt_{r} are the satellite and receiver clock offsets with respect to the common system timescale, I and T represent ionospheric and tropospheric path delays, K_{r} and K^{s} denote the receiver and satellite instrumental delays, and the remaining terms describe various forms of measurement errors. These include multipath errors (ϵ_{mp}) and receiver noise (ϵ_{n}). A visual representation of the pseudorange measurement contents is given in

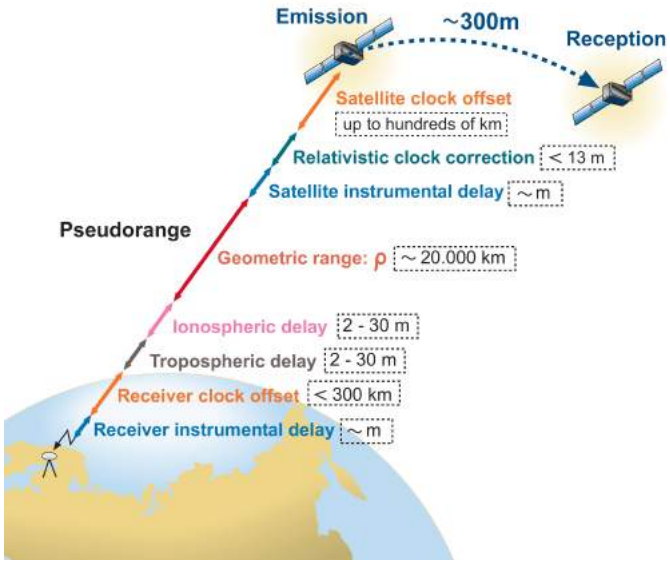


FIGURE 2.14: Pseudorange measurement contents. From [15].

Fig. 2.14.
From the code pseudorange measurements R^j for $n \geq 4$ satellites, the following measurement equation system can be written, neglecting the multipath and receiver noise terms:

$$R^j - D^j \approx \sqrt{(x^j - x)^2 + (y^j - y)^2 + (z^j - z)^2} + c\delta t_r\,, \qquad j = 1, \ldots, n \tag{2.31}$$

where the left-hand side contains the measurements R^j and all modeled terms $D^j = -c\delta t^{s,j} + ION^j + TRO^j + K_r + K^s$. The right-hand side contains the four unknown parameters: the receiver coordinates $(x; y; z)$ and the receiver clock offset δt.
Equations 2.31 defines a nonlinear system, which can be solved by linearizing the geometric range ρ in the a neighborhood of a point (x_0, y_0, z_0) corresponding to the approximate position of a receiver. Following the procedure in [15], we obtain a linearized version of the system 2.31:

$$R^j - \rho_0^j - D^j = \frac{x_0 - x^j}{\rho_0^j}\Delta x + \frac{y_0 - y^j}{\rho_0^j}\Delta y + \frac{z_0 - z^j}{\rho_0^j}\Delta z + c\delta t\,, \qquad j = 1, \ldots, n \tag{2.32}$$

where $\rho_0^j = \sqrt{(x^j - x_0)^2 + (y^j - y_0)^2 + (z^j - z_0)^2}$, $\Delta x = x - x_0$, $\Delta y = y - y_0$ and $\Delta z = z - z_0$. In general, this is an over-determined system, which can be solved using the least squares adjustment. After solving it, the estimate of the receiver is $(x, y, z) = (x_0 + \Delta x, y_0 + \Delta y, z_0 + \Delta z)$. Equations 2.31 can be linearized again about these new estimates od the receiver's position, and the solution can be iterated until the change between two consecutive iterations is below a given threshold. Typically the starting point is set to the Earth's center, that is $(x_0, y_0, z_0) = (0, 0, 0)$.

Chapter 3

The Spoofing Threat

Spoofing signals were considered a threat for military GNSS signals from the start; however, due to the recent rapid increase in the application of civilian GNSS dependant systems, motivation has increased to spoof these signals for illegal or concealed transportation, fishing and hunting in prohibited areas, misleading receiver timing being used by power distribution grids and cellular networks and interrupting stock exchange transactions. Spoofing signals try to induce falsified timing and position solution to their target receivers and they are designed to mimic different features the authentic GNSS signals in order to prevent detection. The ubiquity of GNSS has generated the motivation for spoofing attacks and generating this type of interference has become more feasible and less costly thanks to the fact that the structure of most civilian GNSS signals is known to the public and due to advances in software defined radio (SDR) technology.

In this Chapter the general model of a spoofing attack is first described, then a classification of the spoofing generation techniques is done followed by a receiver state based analysis of spoofing and finally an overview the different types of spoofing attacks and techniques is illustrated.

3.1 General Model of a Spoofing Attack

From Eq. (2.7), an authentic typical received GNSS signal takes the form

$$r_{\mathrm{a}}(t) = \sum_{i=1}^{N_{\mathrm{a}}} A_{\mathrm{a},i} D_{\mathrm{a},i}(t - t_{\mathrm{p,a},i}) C_{\mathrm{a},i}(t - \tau_{\mathrm{a},i}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D,a},i})t + \phi_{\mathrm{a},i}\right]} + n_{\mathrm{a}}(t)\,, \tag{3.1}$$

where the subscript 'a' stands for "authentic" and N_{a} is the number of the visible satellites at the end of a receiver antenna and the other variables are as defined after Eqs. (2.5) and (2.7).
In a spoofing attack, an attacker, called spoofer, wants to lead a tracking receiver to a false PVT solution through a false GNSS signal, called spoofing signal. At the end of a receiver antenna the malicious signal can be written in the form

$$r_{\mathrm{s}}(t) = \sum_{i=1}^{N_{\mathrm{s}}} A_{\mathrm{s},i} D_{\mathrm{s},i}(t - t_{\mathrm{p,s},i}) C_{\mathrm{s},i}(t - \tau_{\mathrm{s},i}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D,s},i})t + \phi_{\mathrm{s},i}\right]} + n_{\mathrm{s}}(t)\,, \tag{3.2}$$

where the subscript 's' stands for "spoofer". Specifically, N_{s} in the number of spoofed satellites, D_{s} is the spoofed navigation data symbol sequence, C_{s} is the spoofed spreading code sequence with a chip duration of T_c and n_{s} is the noise. Moreover, A_{s}, τ_{s}, $f_{\mathrm{D,s}}$ and ϕ_{s} are, respectively, the spoofed amplitudes, code delays, Doppler shifts and carrier phases. From now on, the dependency of the various functions on

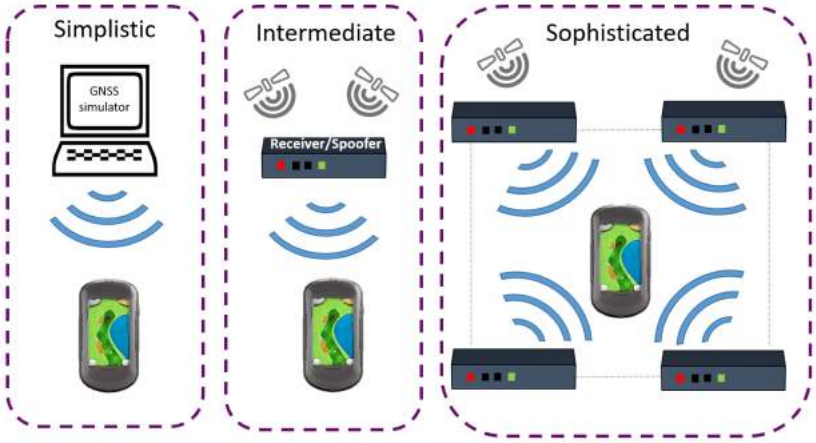


FIGURE 3.1: The spoofing threat continuum: simplistic, intermediate, and sophisticated spoofing attacks. From [19].

$\tau_s, \phi_s, f_{D,s}$ and A_s will be dropped.
In this way, the total received signal at the victim receiver is

$$r(t) = r_a(t) + r_s(t)\,, \tag{3.3}$$

where the noise term is included in the authentic and spoofing components.

3.2 Spoofing Generation Techniques

Spoofing generation techniques consists of the synthesis and transmission of fake GNSS signals which are received by the victim in the form of Eq. (3.3). These techniques can be categorized as follows (see Fig. 3.1) [10]:

- *GNSS signal simulators*: this category of spoofing attack consists of a GNSS signal simulator connected to an RF transmitter. The signals generated by this kind of spoofers are not essentially synchronized to real GNSS signals. In other words, the spoofing correlation peaks are not essentially aligned with the authentic ones. Therefore, this type of spoofing signals looks like noise for a GNSS receiver operating in the tracking mode (even if the spoofer power is higher than the authentic signals). However, this type of spoofers can adversely affect the acquisition process of conventional GNSS receivers and degrade their performance especially if the spoofing signal power is higher than that of the authentic signals. A GPS signal simulator is the simplest GPS spoofer and it can be detected by different anti-spoofing techniques such as amplitude monitoring, consistency check among different measurements and consistency check with Inertial Measurement Units (IMUs).

- *Receiver-based spoofer*: a more complicated type of spoofer consists of a GNSS receiver concatenated with a spoofing transmitter. This system first synchronizes itself with the current GNSS signals and extracts the position, time and satellite ephemeris and then generates the spoofing signal knowing the position of its target receiver's antenna. This spoofer can even mislead the tracking GNSS receivers by generating synchronized fake signals.
  This type of spoofers is relatively hard to detect since they are synchronized with real GNSS satellites. The main challenge toward realization of this kind

of spoofer is projecting the spoofing signals to the intended victim receiver with the correct signal delay and strength. Figure 3.2 shows a repeater-spoofer structure.

- *Sophisticated receiver-based spoofer*: this category is the most complex and effective type of the spoofing generation methods. Herein, the spoofer is assumed to know centimetre level position of the target receiver's antenna phase centre to perfectly synchronize the spoofing signal code and carrier phase to those of authentic signals at the receiver. This type of spoofer can take advantage of several transmit antennas in order to defeat angle of arrival (AOA) based anti-spoofing techniques.

3.3 Spoofing Based on Receiver State

Satellite navigation receivers are susceptible to spoofing attacks rather differently during the acquisition and the tracking phase. Spoofers will aim at taking advantage of this dependency [20]:

- Spoofing starts before acquisition and the receiver has no a priori knowledge. This situation occurs after the receiver is switched on (cold start). It provides a maximum of options to the spoofer who wants the receiver to capture his signal first. The receiver cannot distinguish the spoofer's signal from an authentic GNSS signal, unless the signal is somehow authenticated. Even if some information is available to the receiver (e.g. almanac, user position, time estimation, etc.), the clock may have drifted substantially and the position might be completely different at power-up than it was at power-down.
- Spoofing starts before acquisition but the receiver has a priori knowledge. This occurs if the receiver has lost one or all satellites for a short while (reacquisition), or acquires satellites that have newly raised above the horizon. In this situation, the spoofer has to be aware that the receiver combines knowledge about its state, the environment, and their evolution to detect spoofer activity. Changes that a receiver might analyze against models include position, clock-offsets, and atmospheric delays.
- Spoofing during tracking. This is the most demanding situation for the spoofer, since the signals now have to change in a manner compatible with the detailed physical movement of the receiver, as well as with the changes in its environment.

The above description provides a characterization with respect to the relative timing of spoofing and acquisition.

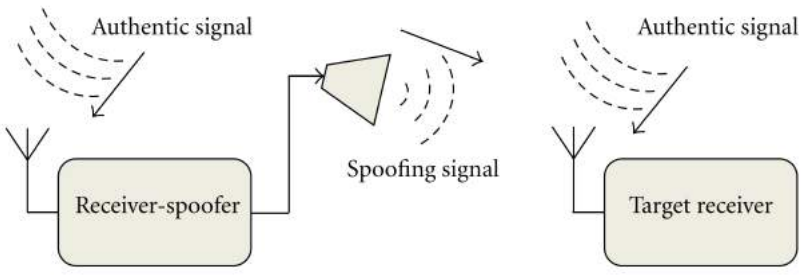


FIGURE 3.2: Repeater spoofer block diagram. From [10].

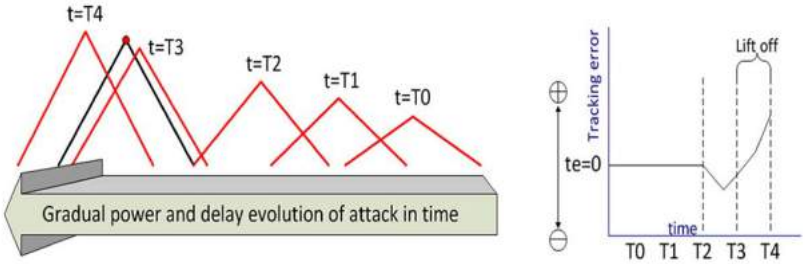


FIGURE 3.3: Lift-off-delay spoofing attack (left) and corresponding tracking error te (right) with spoofing commenced at T2. From [21].

3.4 Types of Spoofing Attacks

Spoofing aims to deceive the GNSS receiver estimate of position and timing information. The navigation processing of a GNSS receiver makes use of the modulated ranging code $C(t)$ and the navigation data information $D(t)$ conveyed in the GNSS signal. This gives the chance to the spoofer to realize two attack types [10]:

- *Signal processing level attacks*: the structure of civilian GNSS signals, including the modulation type, PRN signals, transmit frequency, signal bandwidth, Doppler range, signal strength and many other features are publicly known. Therefore, knowing the general structure and operational basics of a civilian GPS receiver, a spoofer module can generate counterfeit signals that are similar to the authentic GNSS signals so as to effectively mislead its target receiver by tuning the parameters A_s, τ_s, $f_{D,s}$, ϕ_s of Eq. (3.2).

- *Data bit level attacks*: the framing structure of the GNSS signals is publicly known. The navigation frame consists of different parts such as almanac and satellite ephemeris. This information does not change rapidly during short time intervals; for example, the satellite ephemeris information can be acquired in less than 1 minute but it remains unchanged for 12.5 minutes. Therefore, the spoofer can take advantage of this stability in order to create the GNSS data frame.

An attacker can also leverage on a combination of the two types of attack in order to lead the receiver to the desired PVT solution.
Many different variants of spoofing attacks can exists, depending on the receiver state, the environment, etc. The following list encapsulates the most significant ones [21], [22]:

- *Lift-off-delay*: the spoofer approaches the authentic signal with a relative delay $\Delta\tau_s$ (and possibly Doppler), adjusting the spoofing signal's amplitude A_s. Specifically, the spoofer starts with a certain relative delay and low amplitude, then it gradually reduces $\Delta\tau_s$ and simultaneously increases A_s. When $\Delta\tau_s \approx 0$ the amplitude A_s is similar to the authentic one; at this point the spoofing power starts exceding the received signal power and the relative delay is increased again to move the tracking point farther away from the true signal parameters (i.e., lift-off). An illustration of this attack is reported in Fig. 3.3.

- *Lift-off-aligned*: this attack is similar to the previous one, but with the spoofer aligned to the line-of-sight (LOS) satellite signal (i.e., $\Delta\tau_s \approx 0$) until $A_s \approx A$, when the lift-off starts. It avoids being detected at a point distant to the prompt

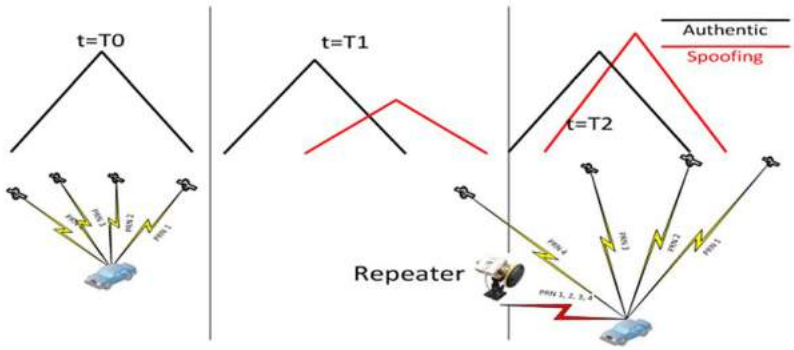


FIGURE 3.4: Meaconing attack: Introducing a delayed replica with varying amplitude. From [21].

correlator, but it can create more abrupt changes to the tracking parameters if the spoofing signal appears suddenly. The receiver is more vulnerable to this attack during signal acquisition or, when accomplished with self-spoofing devices, during tracking.

- *Meaconing and selective delay*: meaconing records the true GNSS signals with a single reception antenna and replays the signals through a transmitter with enough gain to overwhelm the true signal at the victim antenna and with a delay $\Delta\tau_s$ = constant > 0. The victim receiver's false position fix will be that of the spoofer's reception antenna. A meaconer has the potential to spoof any GNSS signal, even an encrypted military signal. An representation of a meaconing attack is shown in Fig. 3.4.
  Selective delay attack is a more sophisticated meaconing attack in which the spoofer uses multiple receiver antennas and phased-array signal processing in order to record-and-replay each satellite signal on an individual channel. Alternatively, using a single reception antenna, the attacker can separate the signals by tracking the different PRNs, thus introducing an additional delay due to the integration time in correlators. Such systems could independently steer the relative delays for each satellite to produce any conceivable false position.
  In case $A_s < A$, one speaks of "multipath attack" as the spoofing signal looks like a nearby reflected signal. A multipath attack degrades the ranging accuracy while leaving the tracking point close to the authentic signal.

- *Jam and spoof*: the spoofer forces the receiver into the acquisition mode via excessive jamming that cause loss-of-lock on the authentic GNSS signals, while transmitting spoofing signals. The the jammer is switched off with the intention that the receiver acquires the spoofing signals.

- *Nonline of sight spoofing*: in suburban and urban environments a receiver will, in general, neither be able to track all satellites above the recommended mask angle, nor will it be aware of the surrounding obstructions, creating the opportunity for a spoofer to spoof the blocked LOS signals as shown in Fig. 3.5. Thus the spoofer can transmit signals only for potentially blocked satellites, making it difficult for the receiver to identify the presence of a spoofing signal.

- *Trajectory spoofing*: except in the case of meaconing, the spoofing signals can be generated independently of each other or can refer to a common position. In the latter case one speaks of a trajectory spoofing attack, where a spoofer with

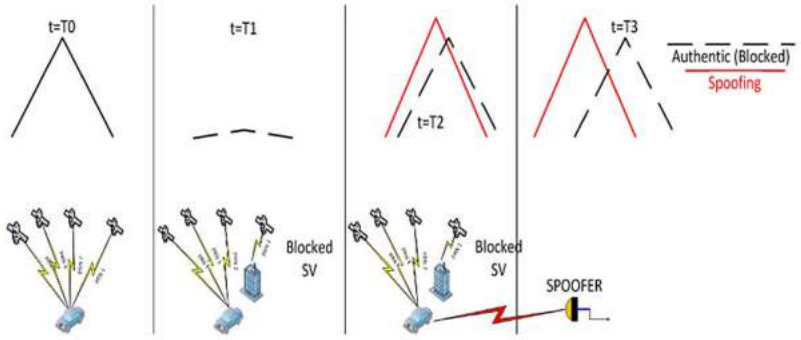


FIGURE 3.5: Non line-of-sight spoofing: Spoofing of low elevation (blocked to the user) SVs. From [21].

the use of a GNSS signal simulator attempts to capture the tracking points of all channels of a receiver along its intended trajectory, forcing the user to follow the spoofed trajectory. In this case all spoofing signals will then be generated coherently with respect to a specific trajectory, that would make satellite range consistency techniques fail.

- *Nulling*: the spoofer transmits two signals for each spoofed signal. One is the spoofed version that acts in concert with all other spoofed signals in order to induce a false position/timing fix. The other is the negative of the true signal. Nulling erases all traces of the true signal from the total received signal of Eq. (3.3).

- *Multiantenna spoofing*: an advanced spoofer acting against a multiantenna victim receiver might use multiple independent spoofer transmission antennas and match each one to a corresponding receiver antenna. The relative geometry of each spoofer/victim antenna pair would need to be known. Also, the spoofer would need to be sufficiently close to the victim and have sufficiently narrow individual antenna gain patterns so that each victim antenna received only the signal from the intended spoofer antenna. Therefore this type of spoofing would likely be practical only with a cooperative victim.
  An expensive type of multiantenna spoofer might transmit only one spoofed signal from each antenna. Such a spoofer might deceive spoofing defenses that were based on signal direction of arrival. It might need to distribute its antennas about the victim so that the spoofed signal arrival directions would seem physically reasonable to the victim's detection system.

Except for meaconing and selective delay, the attacks described above make the assumption that the transmitted spreading code and the transmitted data bit stream are known. However, if the signal is somehow authenticated, then $C(t)$ and $D(t)$ are not fully predictable and the spoofer, to mount its attack, must synthesize approximate replicas of them "on the fly" based on noisy received version of them. This can be done using some prediction based attacks:

- *Security code estimation and replay (SCER)* [23]: this attack is based on estimating the security code or the encrypted data bits by observing the received SIS. As soon as the spoofer gets a reliable estimate, he immediately injects it in the signal replica generator primed with up-to-date spreading code and carrier replicas.

- *Forward estimation attack (FMA)* [24]: while SCER attack focuses on the received signal in a chip by chip or symbol by symbol fashion as if they were independent, in this case it is exploited the redundancy introduced by the forward-error orrection (FEC) used in some GNSS signals to predict the value of the later symbols in a codeword, based on the observations of the earlier symbols.
- *State modeling attack (SMA)* [24]: although the adversary might predict sufficiently many navigation symbols such that the target receiver is oblivious to the attack, not all symbols can be predicted. The target receiver may leverage this fact in an attempt to protect itself from the adversary, by implementing a correlation-based signal verification. This verification technique performs a correlation between the received symbols and the genuine security related symbols available at the receiver. If the received signal is authentic, then the correlation should follow a Gaussian distribution with a certain mean. Given that the test cannot distinguish energy accumulated in one symbol or another, the spoofer tunes the amplitude of each spoofed symbol based on the a posteriori knowledge of the correlation value calculated with the previously disclosed symbols.

In general, not all spoofing attacks will be applicable to all user cases. For example, a lift-off-delay attack would not be feasible for high dynamics users, or a multipath-like attack would probably not be effective for nonline of sight or dense multipath channel conditions. This fact has to be taken into account to assess the performance of the anti-spoofing techniques that are the focus of the next Sections.

Chapter 4

Signal Processing Techniques for Anti-Spoofing

In recent years, several research groups and companies have focused on GNSS interference countermeasures and several articles have been published in this regard. The special case of spoofing countermeasures has recently attracted considerable research interest as spoofing is such a potential menace. However, civilian commercial GNSS receivers remain generally defenceless against this type of interference. The main focus of the research in the field of GNSS spoofing countermeasure is to answer the following questions: "How can a GNSS receiver make sure that it is providing a valid position solution?" and "How can this receiver recover its positioning capability once it is exposed to counterfeit GNSS signals?".
Spoofing countermeasure techniques can be classified into two main categories:

- *Spoofing detection*: spoofing detection algorithms concentrate on discriminating the spoofing signals but they do not necessarily perform countermeasures against the spoofing attack.
- *Spoofing mitigation*: spoofing mitigation techniques mainly concentrate on neutralizing the detected spoofing signals and help the victim receiver to retrieve its positioning and navigation abilities.

Another possible classification is to view the anti-spoofing techniques from a multilayer perspective:

- *Signal processing level techniques*: these techniques are applicable within the antenna, front end and baseband signal processing blocks of a typical GNSS receiver and are based on signal processing algorithms.
- *Data bit level techniques*: data bit level techniques are performed after the data demodulation block and can be subdivided in cryptographic and non cryptographic. The non cryprographic techniques rely on analysis of the navigation message, such as clock and ephemeris consistency check between different satellites, while the cryptographic ones are based on encryption in order to create unpredictable parts of the transmitted signal; however, most of latter require some modifications in the GNSS signal structure.
- *Position solution and navigation level techniques*: finally, these techniques are implemented in the application processing level and are mainly based on a consistency check of solution with other navigation and position technologies, such as IMU and wifi/cellular positioning.

Spoofing threat might be detected/mitigated at any of the above-mentioned levels. Moreover, cross-layer techniques can be developed to incorporate measurements from different operational levels.

This Chapter concentrates on spoofing detection and mitigation techniques at the signal processing level and it is mainly based on the classification of anti-spoofing methods done in [10], [21], [22].

4.1 Spoofing Detection

4.1.1 Methods Based on the Received Signal Strength (RSS)

RSS based spoofing countermeasure techniques rely on the assumption that the power level of spoofing signals is higher than authentic GNSS signals in order to be able to misdirect their target GNSS receiver(s).

AGC Monitoring A spoofing countermeasure method based on monitoring the receiver's AGC gain level is based on the fact that the presence of spoofing signals increases the power content of the received signal set and this changes the AGC level, possibly moving it to an abnormal value. Based on the analyses provided by [25], AGC monitoring is a powerful measure for detecting the presence of spoofing signals especially if their power level is considerably higher than that of the authentic ones.

C/N_0 Monitoring Most GPS receivers employ C/N_0 measurements as a parameter that characterizes the received signal quality. In open sky conditions, only satellite movement and ionosphere variations can cause gradual smooth changes in the received signal power. However, when a higher power spoofer misleads a GPS receiver, the received C/N_0 may experience a sudden change that can indicate the presence of the spoofing signal. The anti-spoofing receiver can continuously monitor the C/N_0 and look for any unusual variation that can be a sign of spoofing attack. It is easy for a GPS receiver to store a time history of the signal received from each satellite.

The C/N_0 measurement for each GPS signal is proportional to the ratio between the despread signal power at the correlator output to the noise power plus other signal interferences. The postprocessing SNR, which is linked to the C/N_0 value, can be shown as

$$\mathrm{SNR} = \frac{P}{|I_\mathrm{a}|^2 + |I_\mathrm{s}|^2 + (\sigma^2/M)}, \tag{4.1}$$

where $P = A^2/2$ is the authentic signal power, I_a and I_s are interference terms caused by cross-correlation effect of other authentic and spoofing signals, σ^2 is the variance of the received noise n and M is the number of samples within the coherent integration time. GNSS signals are designed such that $|I_\mathrm{a}|^2$ is negligible compared to the filtered Gaussian noise variance. However, $|I_\mathrm{s}|^2$ increases as the total spoofing power (TSP) increases. TSP is the sum of signal powers for different spoofing PRNs. Therefore, an asynchronous spoofing source that is transmitting several PRNs with considerable power can effectively reduce the C/N_0 of the authentic signals.
However, during signal acquisition, a spoofer with an high TPS generates correlation peaks higher than the authentic ones over an elevated noise floor due to the cross-correlation term I_s. Therefore, if a spoofing signal is despread, its corresponding C/N_0 measurement would be in the normal authentic C/N_0 range. As a consequence, the receiver might be tracking the higher power spoofing correlation peaks while its C/N_0 measurement does not show any abnormalities.

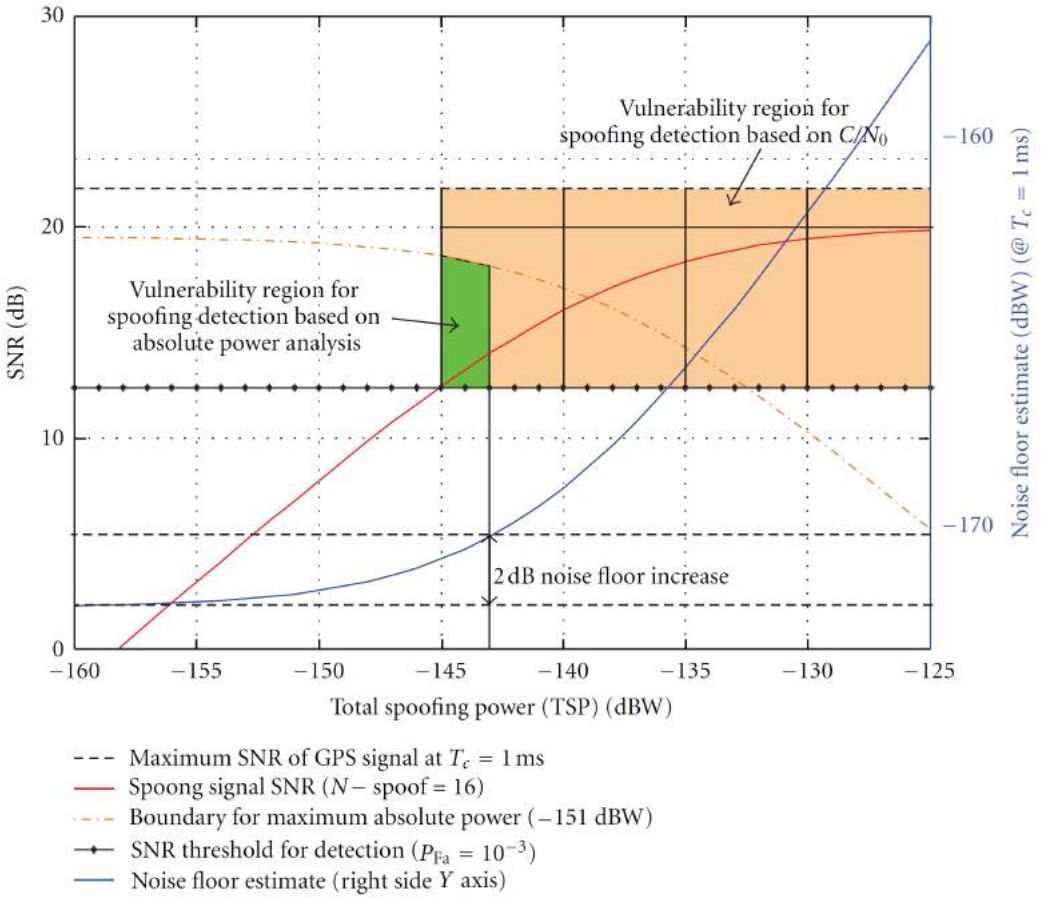


FIGURE 4.1: Vulnerability region comparison of C/N_0 versus absolute power monitoring techniques. From [10].

Absolute Power Monitoring As the path loss between the spoofer and target receiver is highly variable, it is difficult for a spoofer to estimate the transmit power required to impose sufficient signal strength at the target receiver while not excessively exceeding the typical power level of the authentic GPS signals. The maximum received power of the GNSS signals at earth terminals is around −153 dBW at the L1 frequency. Therefore, reception of a spoofing signal whose absolute power is considerably higher than the expected authentic GNSS signal power is a simple direct means of detecting a spoofing attack.

Figure 4.1 provides a comparison between the spoofing vulnerability regions for a C/N_0 monitoring receiver and an absolute power monitoring receiver during signal acquisition. It has been assumed that the absolute power monitoring receiver is able to discriminate the elevated noise floor as well as higher power PRN signals within a 2 dB accuracy range. In other words, this receiver discriminates those PRNs whose absolute power is 2 dB or higher than the maximum possible received power of GPS L1 C/A signal. Furthermore, this receiver is capable of detecting a 2 dB increase in noise floor from its desired value. On the other hand, the C/N_0 monitoring receiver is only able to discriminate the signals whose SNR is higher than the maximum possible SNR of the GPS L1 C/A signal.

Hence, the vulnerability region of the absolute power monitoring receiver is much smaller than the vulnerability region of the C/N_0 monitoring receiver. Furthermore, if the receiver is able to detect the absolute receiver power more accurately, it can

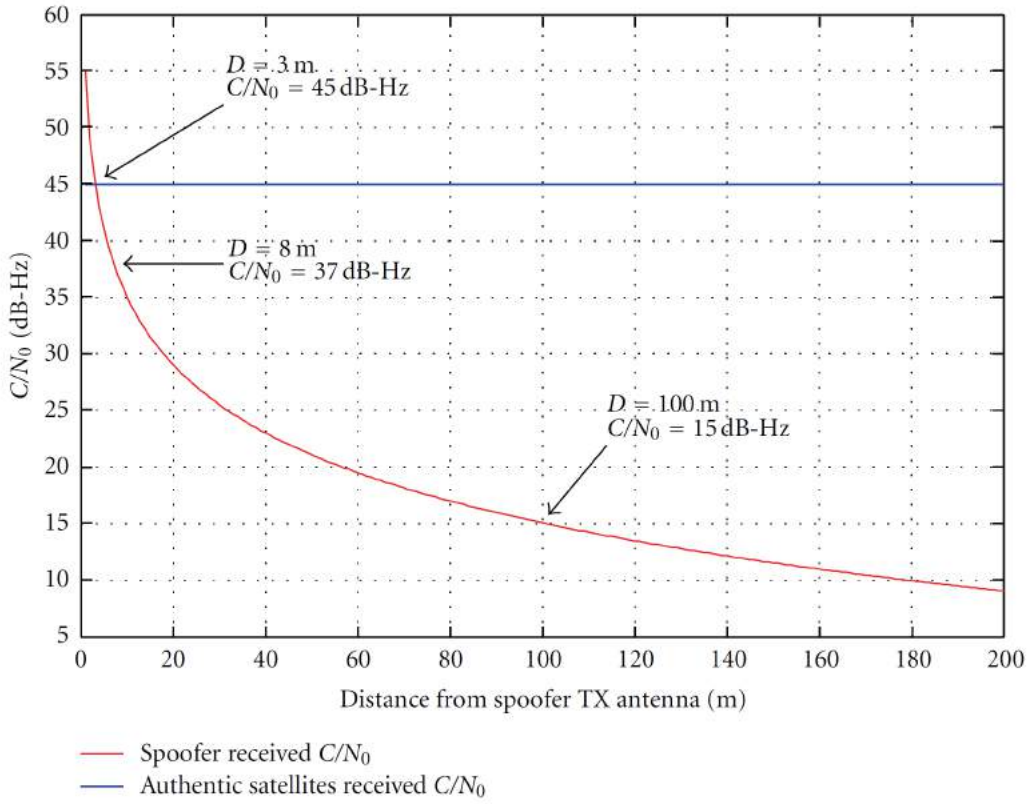


FIGURE 4.2: Variations of spoofing and authentic received C/N_0 versus receiver distance from spoofer transmitting antenna. From [10].

considerably reduce the size of its vulnerability window in the presence of a spoofing attack.

Implementation of this power monitoring technique requires the receiver ability to measure the absolute amplitude of the received signal within a certain accuracy level. Hence, the hardware complexity slightly increases. In addition, the relatively high dynamic range of the GPS signal strength imposes another limitation to the performance of the amplitude discrimination techniques.

Received Power Variations versus Receiver Movement Based on the free space square law of propagation, the received power of a free space propagating signal is proportional to the inverse of the squared propagation distance. GNSS satellites are around 20 000 kilometers away from the earth surface; therefore, if the receiver moves on the earth surface in low multipath open sky environments, no considerable change in the received power from authentic satellites should be observed other than the deterministic losses occurring at lower elevations. However, the spoofing signal is usually transmitted from a single directional antenna located much closer to the receiver compared to the GPS satellites. Therefore, the movement of the receiver relative to the spoofer antenna can considerably change the C/N_0 received from spoofing signals. Figure 4.2 illustrates the variations of spoofing and authentic received C/N_0 values versus the receiver distance from a spoofer antenna. It is observed that when the spoofer is very close to its target receiver, even a slight movement between spoofer and the target receiver can considerably affect the received spoofing signal C/N_0. It should be considered that all the spoofing signals are usually transmitted from the same antenna and therefore all experience the same propagation

medium. As such, variations of all spoofing signals will be the same regardless of the receiver movement and multipath effects. Here it is assumed that the spoofer does not differentially modulate the C/N_0 of the different PRN signals.

This method is a low-complexity spoofing discrimination technique that does not impose extensive hardware/software modifications to the GPS receiver. However, since the receiver does not necessarily know 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/N_0 of the spoofer generated signals. For example, when both spoofing transmitter and GPS receiver are located in the same vehicle, the movement of vehicle does not cause variation in measure of spoofing signals C/N_0. Another disadvantage of this technique is that it cannot be employed for the case of static GPS receivers. Therefore, the effectiveness of this spoofing discrimination technique is limited to a few spoofing scenarios.

Structural Power Analysis (SPA) The structure of spoofing signals is very similar to that of authentic GNSS signals. The presence of additional spoofing PRNs increases the power content of structural signals in the GNSS frequency band. This excessive amount of power can be detected prior to the despreading process using the authenticity verification method proposed by [26], that is based on comparing a detection test statistic (the variance of a filtered version of the received signal) to a threshold in order to differentiate between the presence and absence of spoofing signals. This technique can successfully detect the presence of spoofing signals when these are powerful enough to interrupt the normal operation of user equipment, even if the receiver is equipped with an AGC that applies an unknown gain to the received signal set. The computational complexity of this method is relatively low; therefore, it can be used as an integrated signal authenticity verification block in civilian GPS receivers or it can be materialized as a portable stand-alone GPS signal quality assurance system.

Relative Frequency Band Power Monitoring There is a predefined power level difference between GNSS signals in different frequency bands and many GNSS receivers are able to monitor signals in different bands separately. However, a low-complexity spoofer may only generate a single-band signal. Therefore, a large difference between two different band power levels or the absence of a particular band in a signal can reveal the presence of a spoofing signal. This method can successfully detect the single-band spoofers. However, most of the civil GPS receivers do not have the ability to monitor different frequency bands and this discrimination technique imposes additional hardware complexity to the GPS receiver.

4.1.2 Spoofing Discrimination Using Spatial Processing

Due to logistical limitations, spoofing transmitters usually transmit several counterfeit signals from the same antenna while the authentic signals are transmitted from different satellites with different directions. Therefore, a spatial processing technique can be employed to estimate the spatial signature of received signals and discriminate those signals that are spatially correlated.

Multiantenna Spoofing Discrimination There are several proposals that make use of a multiantenna receiver:

- In [9] a spoofing detection technique is proposed which observes the phase difference between two fixed antennas for around one hour. Knowing the bearing 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 to discriminate the spoofing threat. The main drawback of the algorithm is that it takes a long time (about 1 hour) to discriminate the spoofing signals. In addition, this technique requires a calibrated antenna array with known array orientation in order to operate properly.

- Another method that is based on the carrier-phase difference between two receiver antennas is proposed in [27]. The signal-in-space properties used to detect spoofing are the relationships of the signal arrival directions to the vector that points from one antenna to the other. In the un-spoofed case, there are a multiplicity of relationships between the interantenna vector and the arrival directions of the multiple signals, which results in a quantifiable multiplicity of carrier-phase single-differences between the antennas. In the spoofed case, there is a single direction of arrival, assuming a single spoofer transmission antenna, and the carrier phase single-differences are identical for all channels, up to an integer cycle ambiguity.
  A spoofing detection statistic is developed that equals the difference between the optimized values of the negative-log-likelihood cost functions for two data fitting problems. One problem fits the single-differenced beat carrier phases of multiple received signals to a spoofed model in which the fractional parts of these differences are identical - in the absence of receiver noise - because the spoofed signals all arrive from the same direction. The other problem fits the single-differenced carrier phases to a non-spoofed model. The simple difference of the two optimized cost functions equals a large positive number if there is no spoofing, but it equals a negative number if the signals are being spoofed.
  Figure 4.3 demonstrates the performance of this spoofing detection algorithm. The upper panel shows the beat carrier phase difference time histories between the two antennas and the bottom panel the corresponding spoofing detection statistic time history before ($t < 400\,\mathrm{s}$) and after a spoofing attack ($t > 400\,\mathrm{s}$), revealing the successful detection.
  However, other tests revealed some challenges for this spoofing detection strategy. They occur primarily during the initial attack phase, before the spoofer has dragged the victim receiver to a wrong position or timing fix. If the spoofer power is not very much larger than that of the true signals, then beating occurs between the spoofed and true signals during this initial period. This beating can cause difficulties for the receiver tracking loops, making single-differenced carrier phase unavailable.

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, there are many practical limitations to realizing such a sophisticated spoofing scenario.

Synthetic Spoofing Array Discrimination Anti-spoofing methods that use a synthetic spoofing array are mainly based on pairwise correlation and carrier phase bias:

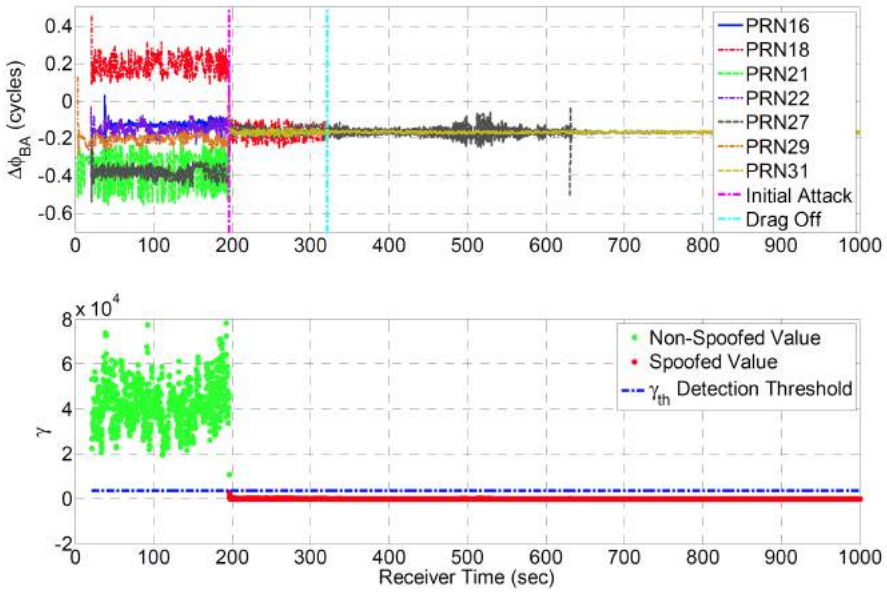


FIGURE 4.3: Single-differenced carrier phase time histories (top plot) and spoofing detection statistic time history (bottom plot) for a spoofing attack. From [27].

- In [28] a spoofing detection technique that employs a synthetic antenna array has been proposed. In this scenario a single-antenna handheld GPS receiver is moved along a random trajectory and forms a synthetic antenna array structure. This scenario is shown in Fig. 4.4. The received signals amplitude and phase corresponding to different PRN signals are continually compared to each other using a correlation coefficient metric (ρ_{ij}). Therefore, after acquiring different PRN signals in the received signal set (both authentic and spoofing signals), spoofing signals are discriminated using the following normalized correlation coefficient:

$$\rho_{i,j} = \left| \frac{\mathrm{E}\left[(\mathbf{y})_i^{\mathsf{H}}(\mathbf{y})_j\right]}{\sqrt{\mathrm{E}\left[(\mathbf{y})_i^{\mathsf{H}}(\mathbf{y})_j\right]}\sqrt{\mathrm{E}\left[(\mathbf{y})_j^{\mathsf{H}}(\mathbf{y})_j\right]}} \right| , \tag{4.2}$$

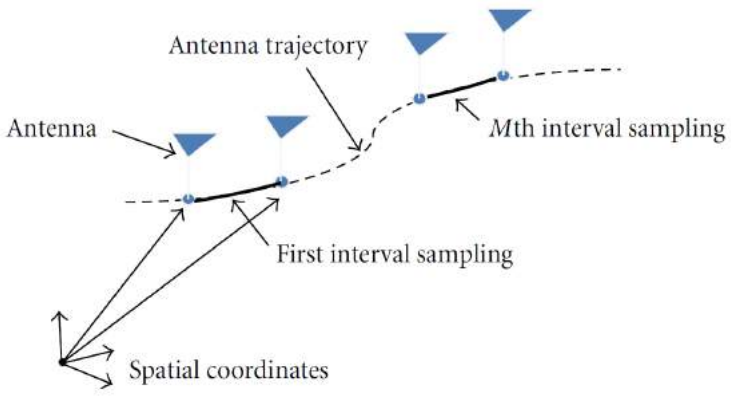


FIGURE 4.4: Spatial sampling for a moving handheld GPS receiver. From [10].

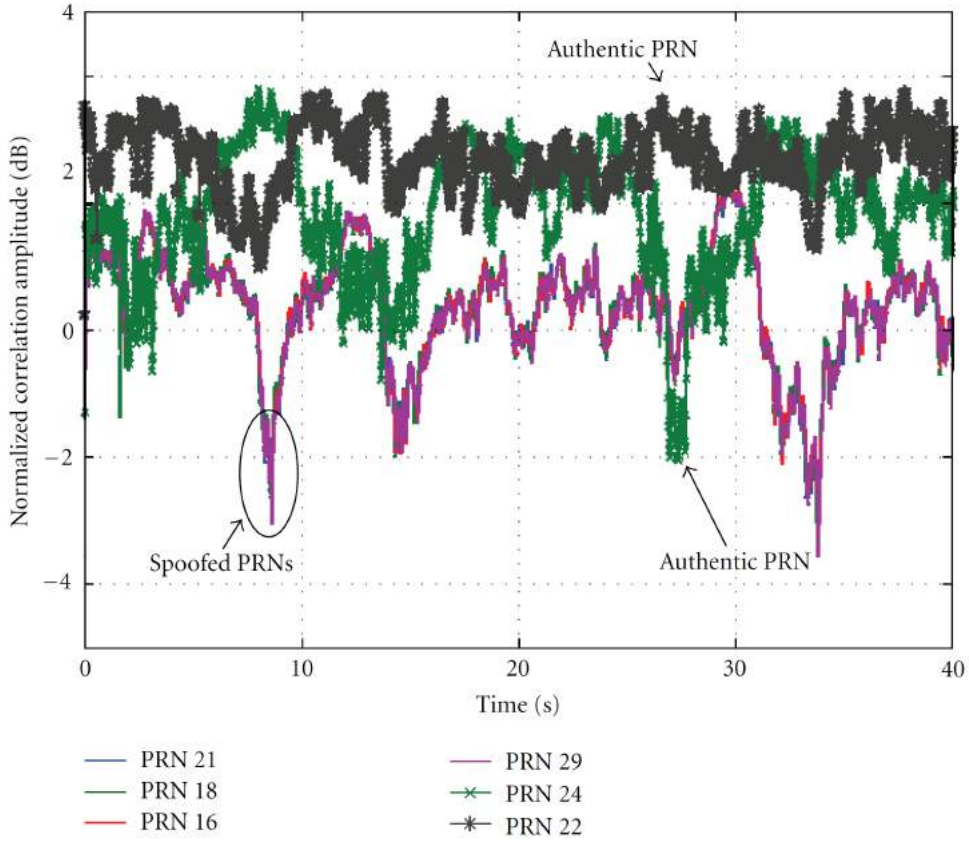


FIGURE 4.5: Correlation amplitude for spoofing and authentic PRN signals. From [10].

where E[·] represents the statistical expectation and the superscript H denotes the conjugate transpose. $(\mathbf{y})_i$ and $(\mathbf{y})_j$ represent the i-th and j-th columns of matrix $\mathbf{y}$, which is defined as follows:

$$\mathbf{y} = \begin{bmatrix} [\mathbf{y}^{\mathrm{a}}[1], \mathbf{y}^{\mathrm{s}}[1]] \\ [\mathbf{y}^{\mathrm{a}}[2], \mathbf{y}^{\mathrm{s}}[2]] \\ \vdots \\ [\mathbf{y}^{\mathrm{a}}[J], \mathbf{y}^{\mathrm{s}}[J]] \end{bmatrix}_{J \times L}, \tag{4.3}$$

$$\mathbf{y}^{\mathrm{a}}[k] = \left[y_1^{\mathrm{a}}(kMT_{\mathrm{s}}), \ldots, y_N^{\mathrm{a}}(kMT_{\mathrm{s}}) \right],$$

$$\mathbf{y}^{\mathrm{s}}[k] = \left[y_1^{\mathrm{s}}(kMT_{\mathrm{s}}), \ldots, y_{N_{\mathrm{s}}}^{\mathrm{s}}(kMT_{\mathrm{s}}) \right].$$

In Eq. (4.3), it is assumed that correlator outputs are monitored during J time instances and $\mathbf{y}$ is an $J \times L$ matrix where L is the number of acquired PRN signals ($L \leq N + N_{\mathrm{s}}$). $\mathbf{y}^{\mathrm{a}}[k]$ is the set of correlator outputs for all acquired authentic signals at time instant kMT_{s}, whereas $\mathbf{y}^{\mathrm{s}}[k]$ consists of all acquired spoofing peaks for that time instant. J is the number of equivalent spatial samples and M is the number of samples within the coherent integration time.

Figure 4.5 illustrates the normalized signal amplitude for acquired spoofing and authentic signals. During the data collection, the antenna was randomly moved. It is observed that the amplitude variations for spoofing signals are highly correlated (i.e., the plots representing the amplitudes of PRN-16, PRN-18, PRN-21, and PRN-29 are totally overlaid) while this correlation does not exist for

the authentic signals (i.e., the amplitudes of PRN-22 and PRN-24 do not overlay). This technique works effectively even in multipath environments because all the spoofing signals experience the same fading path. Furthermore, since this method does not employ several receive antennas, its hardware complexity is much lower as compared to the technique proposed in [9]. However, in the case that spoofer differentially modulates the amplitude and/or phase of different PRN signals, some modifications should be applied to this method in order to successfully discriminate the counterfeit signals.

- In [29] a method is proposed that uses a short segment of beat carrier-phase time histories that are collected while the receiver's single antenna is undergoing a known, high frequency motion profile, typically one pre-programmed into an antenna articulation system. The antenna also can be moving in an unknown way at lower frequencies, as might be the case if it were mounted on a ground vehicle, a ship, an airplane, or a spacecraft. The spoofing detection algorithm correlates high-pass-filtered versions of the known motion component with high-pass-filtered versions of the carrier phase variations. True signals produce a specific correlation pattern, and spoofed signals produce a recognizably different correlation pattern if the spoofer transmits its false signals from a single antenna. The most pronounced difference is that non-spoofed signals display variations between the beat carrier phase responses of multiple signals, but all signals' responses are identical in the spoofed case. These differing correlation characteristics are used to develop a hypothesis test in order to detect a spoofing attack or the lack thereof.

4.1.3 Time of Arrival (TOA) Discrimination

PRN Code and Data Bit Latency In the case that the receiver-based spoofer does not have any prior information regarding the navigation data bits, it should first decode the received GPS signals and then generate a processed replica as the spoofing signal. Hence, an unavoidable delay exists between the spoofing data bit boundaries with respect to the authentic ones. Therefore, if the data bit transition happens at time instants with a spacing other than the data bit period, then a spoofing attack might be present.
This technique encounters some limitations because the GNSS data frame structure is already known and it consists of different parts with different update frequencies. The update frequency of most parts of the GNSS frame is very low. Therefore, the majority of the GNSS data bits can be predicted by the spoofer if it has already acquired the GNSS information before starting to transmit the fake spoofing signals.

Different Band Signals Relative Delay GNSS satellites transmit signals on different frequency bands. The signals received on different frequencies have a relative delay/attenuation that is caused by the different frequency response of the ionosphere. Therefore, if a multiple frequency GNSS receiver correlates the different band signals, it should observe only one correlation peak. The GNSS receiver knows the approximate delay correlation relative delay of correlation peaks, therefore the spoofer should be able to generate signals on different frequencies with the correct delay in order to defeat this countermeasure.

4.1.4 Correlation Peak Monitoring

Signal Quality Monitoring (SQM) SQM techniques have been previously employed to monitor the GPS correlation peak quality in multipath fading environments. The interaction between spoofing and authentic signals can affect the correlator output in a way similar to that of multipath components. Therefore, reference [14] has extended the previously proposed SQM techniques to detect spoofing attacks on tracking receivers working in LOS conditions. Different metrics have been proposed in order to detect any abnormal asymmetry and/or flatness of correlation peaks that is imposed by the interaction between authentic and spoofing signals. Two of the most common test metrics are the delta test, with metric

$$\Delta = \frac{I_{\mathrm{E}} - I_{\mathrm{L}}}{I_{\mathrm{P}}}\,, \tag{4.4}$$

and the ratio test, with metric

$$R = \frac{I_{\mathrm{E}} + I_{\mathrm{L}}}{\xi I_{\mathrm{P}}}\,, \tag{4.5}$$

where ξ is a constant factor, that represents the slope of the correlation function. The metrics are then used to build a test statistic to decide whether spoofing is present or not. For example, in the case the delta test is used, it is easy to see that the mean value of Δ will tend to zero in a clean data set, and in case of asymmetries, Δ will be a positive or a negative number, based on the delay and phase of the spoofing signal. It is assumed that the receiver has initially locked onto the authentic correlation peaks and a spoofing source tries to deceive the receiver toward tracking its fake correlation peaks.

The SQM antispoofing techniques are powerful methods toward detecting the spoofing attack especially in the LOS propagation environments. However, in the presence of multipath propagation, the SQM method might not be able to discriminate between spoofing signals and multipath reflections.

Coupled Amplitude Delay Locked Loop (CADLL) The CADLL was initially designed as a pure multipath estimation and mitigation architecture. However, its ability to accurately estimate the features of multipath rays and their evolution in time, allowed [30] to revisit it to detect spoofing signals. The CADLL is composed of several parallel tracking units, each tracking a component signal. Inside each tracking unit, a normal DLL with wide or narrow spacing is used to track the code phase and two amplitude-locked loops (ALL) are used to track the amplitudes of I and Q components of the signal.

The working procedure of CADLL is made of different steps. It first uses a conventional tracking loop to lock onto the incoming signal getting a rough estimation about the code phase of LOS signal and then it activates two units in order to try to track a multipath signal. If the inserted unit fails to track any signal, it means there is no multipath in the incoming signal. It continues inserting a new unit into this feedback loop to look for a new multipath component. A monitor block is governing the process of searching a new multipath component by checking the tracking results of the new unit. If it is considered that there is no new multipath component, the trial unit will be shut down by the monitor block. In fact the parameters of each unit are normally monitored to decide for enabling additional unit or shutting down a unit that is not actually tracking a signal. The process will not stop until there is no new multipath found or the number of enabled units reaches the maximum number which is pre-defined according to available resources.

The spoofing detection technique basically requires a modification of the monitoring unit of the CADLL. The basic idea is to compare the features of the monitored components with the expected behavior of a replica due to a reflection. Such a comparison is essentially based on two principles:

- Multipath delay cannot be smaller than LOS delay.
- Multipath amplitude is correlated with the delay, i.e. the distance of the obstacle generating the reflection.

Only two units are required for spoofing detection purposes. However, more units may allow dealing with environments where both spoofing signals and multipath are present.

Distribution Analysis of the Correlator Output In LOS conditions, the correlator output power for a tracking receiver approximately follows a Chi-squared (χ^2) distribution. For the case of a spoofing attack on a tracking receiver, the spoofing signal correlation peak should be located as close as possible to that of the authentic signal; therefore, the correlator output power is affected by the spoofing signals. If the interaction between authentic and spoofing signals causes the correlator output to considerably deviate from the expected distribution for authentic signals, a spoofing attack will be flagged. This feature can be used for detecting the presence of spoofing signals. For example, for the case of consistent Doppler spoofing attack on a tracking receiver, the interaction between spoofing and authentic signals causes rapid fluctuations in the amplitude of the correlator output and these fluctuations can be detected by the proposed countermeasure technique. Figure 4.6 shows the correlator output distributions for different relative powers for authentic and spoofing signals. It is observed that the correlator output distributions are completely different in the presence and absence of spoofing attacks.

This technique can successfully discriminate spoofing signals in the LOS propagation environments. However, in presence of multipath propagation, the χ^2 distribution is not a valid assumption for the distribution of correlator output amplitude. Therefore, this method is of limited applicability in nonline of sight propagation environments.

Correlator's Spectral Analysis The proposal in [31] is based on the idea that GNSS signal replicas are a very specific type of interference. Unlike common RF interferences, spoofing may not be evident until the receiver has corrected its carrier and code at the correlation process. Therefore, by analysing the output correlation values of the receiver one could find the traces of the interferences. At this point, the resulting signal in an interference-free environment is a constant value affected by noise while in the presence of multiple signals with the same spreading code, it is a sum of complex sinusoids at the residual frequencies. The remaining frequency errors in the second case are occasioned by the presence of the interference that affects the correct demodulation of the authentic signal. It is possible to detect the presence of the interference formulating a decision problem with the two states of the output correlation using the GLRT which allows to decide the most likely event. However, it requires the estimation of the residual frequencies which are difficult to estimate using classical non-parametric techniques like the periodogram when the data record is short. For this reason the authors propose the use of a super-resolution frequency estimation method based on the Pisarenko harmonic decomposition (PHD) due to its

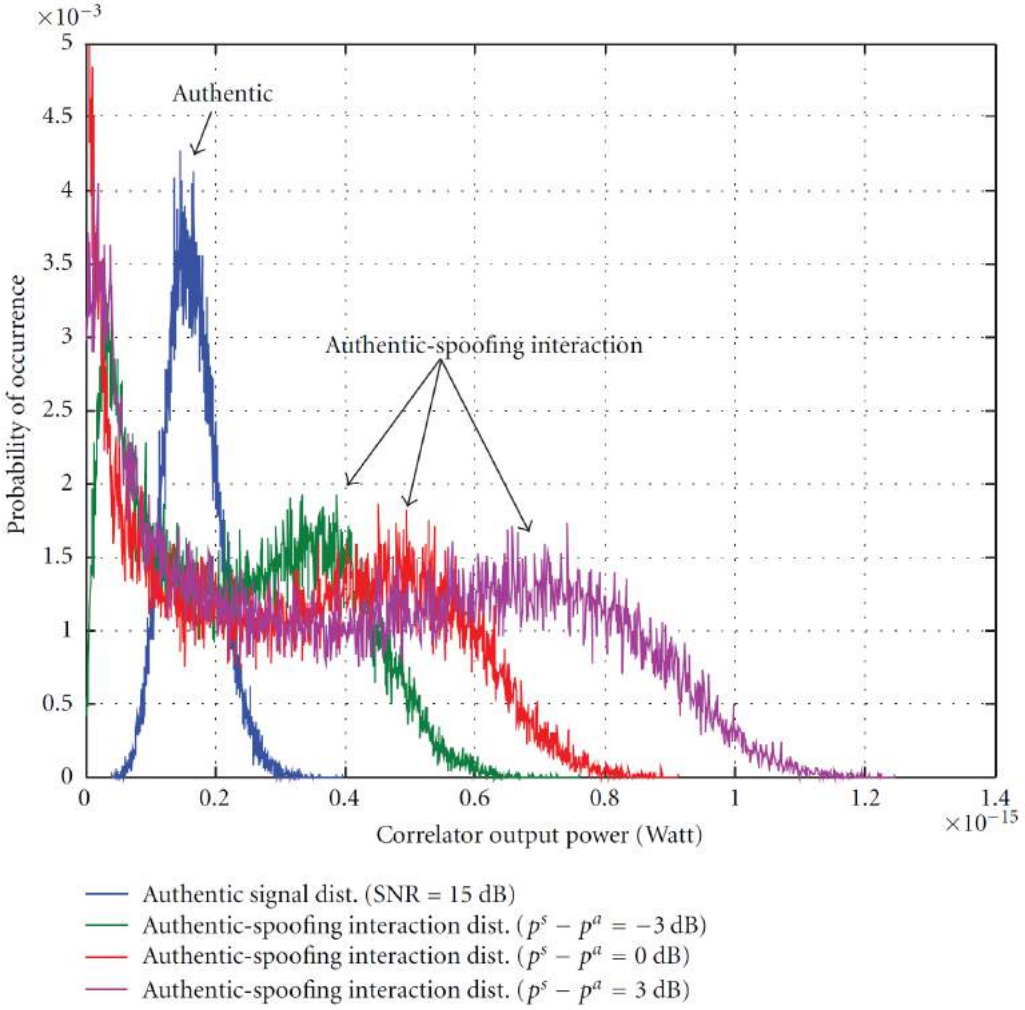


FIGURE 4.6: Distribution of prompt correlator output power for authentic signals and authentic-spoofing interaction for different spoofing powers. From [10].

simplicity compared to other algorithms. Thanks to the estimates obtained with PHD it is possible to carry out the GLRT and detect the presence of the interference.

4.1.5 Signal Parameters Monitoring

Doppler Shift Check GNSS receivers have position solution and satellite position. The relative speed of the receiver with respect to each GPS satellite can thus be derived. It is impossible to get all the Doppler shifts for all satellites correct by mimicking satellite movement by the spoof source using a single transmitter because the Doppler shift is changing carrier frequency. Although CDMA signals with different PRN code can be summed before being modulated on a carrier, the spoof signal has to be modulated to a different carrier to avoid the Doppler test. A spoofer might thus have to use one transmitter for each spoofed space vehicle (SV). The Doppler shift should also compare with the rate at which the phase range measurement changes, i.e.

$$f_D = \lambda \dot{\phi} \,, \tag{4.6}$$

where $\dot{\phi}$ is the phase rate and $\lambda = 1/f_{RF}$.

Code and Phase Rates Consistency Check In the case of authentic signals, the Doppler frequency and the code delay rate are consistent because they are both affected by the relative movement between GPS satellite and receiver. This consistency requires that

$$f_D = -f_{RF}\dot{\tau}\,, \tag{4.7}$$

where $\dot{\tau}$ is the code delay rate. A low-quality spoofer might not keep this consistency between Doppler frequency and code delay rate. As such, a spoofing aware receiver can successfully detect this type of spoofers if the loop filter output of PLL and DLL are not consistent. The PLL and DLL loop filter outputs are estimates of the phase and delay rates, respectively.

Table 4.1 provides a summarized comparison among the previously discussed spoofing detection algorithms.

TABLE 4.1: Summary of spoofing detection techniques.

Anti-spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
AGC monitoring	Higher power	Low	Medium	AGC monitoring	Medium
C/N_0 monitoring	Higher C/N_0	Low	Medium	C/N_0 monitoring	Medium
Absolute power monitoring	Higher amplitude	Low	Medium	Absolute power monitoring	High
Structural power analysis	Higher power	Low	Medium	Specific pre-despreading processing unit	High
Power variation versus receiver movement	Higher power variations due to proximity	Low	Low	Antenna movement/C/N_0 monitoring	Low
Relative band power monitoring	Single band spoofing	Medium	Low	Different bands reception capability	Low
Direction of arrival comparison	Spoofing signals coming from the same direction	High	High	Multiple receiver antennas	High
Pairwise correlation in synthetic array	Spoofing signals coming from the same direction	Low	High	Measuring correlation coefficient	High

Table 4.1: Summary of spoofing detection techniques (continued).

Anti-spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
TOA discrimination	Inevitable delay of spoofing signal	Medium	Medium	TOA Analysis	Low
Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low
CADLL	Similarity to multipath	Medium	Medium	Parallel tracking units (one DDL and two ALL per unit)	High
Distribution analysis of the correlator output	Perturbed amplitude distribution due to spoofing-authentic interaction	Low	Medium	Distribution analysis of correlator outputs	Medium
Correlator's spectral analysis	Different residual frequency from authentic signal	Low	Medium	Super-resolution frequency estimates	High
Doppler shift check	Mismatch between Doppler shift and carrier frequency	Low	Low	—	Low
Code and phase rate consistency check	Mismatch between artificial code and phase rate	Low	Low	—	Low

4.2 Spoofing Mitigation

4.2.1 Vestigial Signal Detection

Suppressing the authentic signal is very hard for GNSS spoofers because it requires precise knowledge of the victim antenna phase centre position relative to spoofer antenna phase centre. In most cases, after successful lift-off, a vestige of the authentic signal that can be used for spoofing detection and mitigation remains. In [8] the

authors have proposed a vestigial detection technique in which the receiver employs the following software-defined technique. First, the receiver copies the incoming digitized front end data into a buffer memory. Second, the receiver selects one of the GPS signals being tracked and removes the locally regenerated version of this signal from the buffered signal. Third, the receiver performs acquisition for the same PRN signal on the buffered data. This technique is very similar to the successive interference cancellation (SIC) used for removing strong signals in order to combat the near/far problem in Direct Sequence Code Division Multiple-Access (DS-CDMA) networks.

The implementation of the vestigial signal detection 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 and limited bit resolution, the authentic vestige might not still be detectable since it might have been fallen under the sensitivity level of the GNSS receiver quantizer.

4.2.2 Multiantenna Beamforming and Null Steering

A multiantenna receiver can employ array processing techniques in order to shape its beam. As such, after detecting the direction of spoofing signal, this receiver can steer a null toward the spoofer source and suppress its harmful effect. Therefore, spoofing signals can be mitigated if the received signal is multiplied by a complex weighting vector ($\boldsymbol{f}$) such that

$$\boldsymbol{f}^{\mathsf{H}}\boldsymbol{b} = 0\,, \qquad \text{constraint: } \|\boldsymbol{f}\| = 1\,, \tag{4.8}$$

where $\boldsymbol{b}$ is the steering vector incorporating all spatial characteristics of the antenna array for spoofing signals, assuming the spoofer uses a single transmitting antenna.

- In [32] an antenna array structure is used to detect and mitigate spoofing signals based on their spatial correlation. The correlator output phase measurements for different PRN signals are mutually compared to discriminate the ones received from the same spatial sector, that are then spatially nulled through beamforming. This technique can successfully detect and mitigate spoofing signals originated from a single transmit antenna and it does not need any array calibration or information regarding array orientation. In addition, the multipath propagation does not degrade the performance of this method since all the spoofing signals experience the same propagation channel characteristics. However, this technique increases the hardware complexity of the GNSS receiver as it necessitates the use of several antenna branches. Furthermore, applying this method increases the computational complexity of GNSS receiver since the receiver needs to acquire and track both spoofing and authentic signals in order to be able to discriminate spoofing PRNs.

- In [33] a very low computational complexity double antenna spoofing mitigation method is proposed that is able to spatially filter out the spoofing signals. This method cross-correlates the received signals from different antennas and extracts the spatial signature of spoofing signals based on their spatial power dominancy. All these operations are performed on the raw samples before despreading the authentic and spoofing signals. Assuming that spoofer module transmits several PRN signals each of which having a power level comparable to authentic ones, the steering vector corresponding to spoofing signals ($\boldsymbol{b}$) can be extracted because all spoofing signals are coming from the same direction. This method

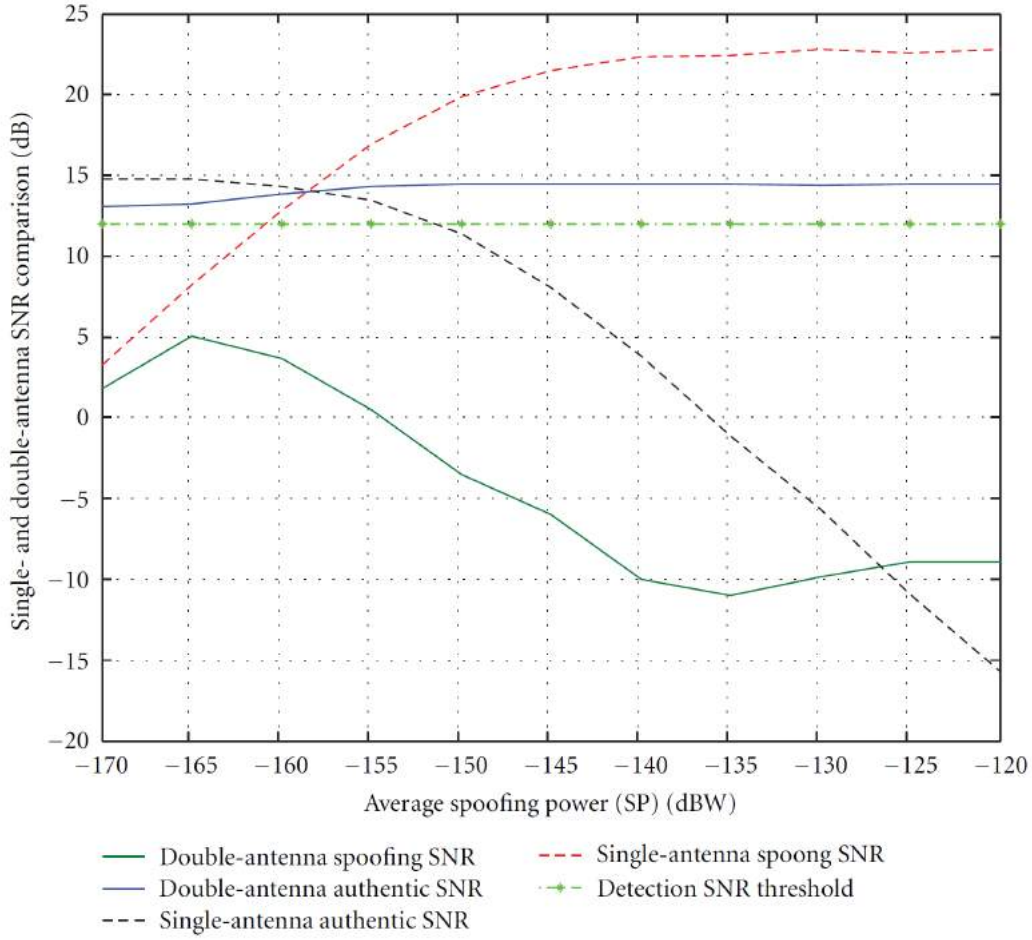


FIGURE 4.7: Authentic and spoofed SNR variations as a function of average spoofing power. From [10].

does not need array calibration or any prior information regarding antenna array orientation and can be employed as an in-line stand-alone antenna combining block that mitigates the spoofing signals at before entering the conventional GNSS receivers.

Figure 4.7 shows the average SNR of the authentic and spoofing signals as a function of the average input spoofing power for both the single-antenna and the proposed double antenna receivers. For the case of single-antenna receiver, the authentic SNR decreases as the input spoofing power increases. However, it is observed that after proper combining of the signals of both antennas, the SNR of the authentic signal almost remains constant while the spoofing SNR is always far below the detection threshold for different input spoofing powers.

The spoofing mitigation technique proposed in [33] successfully mitigates the spoofing signals as long as their TSP is considerably higher than the average power of authentic signals. Nevertheless, in some cases it might unintentionally reduce the power of some authentic signals due to the inherent cone of ambiguity in the double-antenna beam pattern. This problem can be solved by employing larger antenna arrays because the ambiguity region of antenna beam pattern considerably decreases as the number of array elements increases. This spoofing mitigation technique might not perform well in the case of multiple-antenna spoofing transmission.

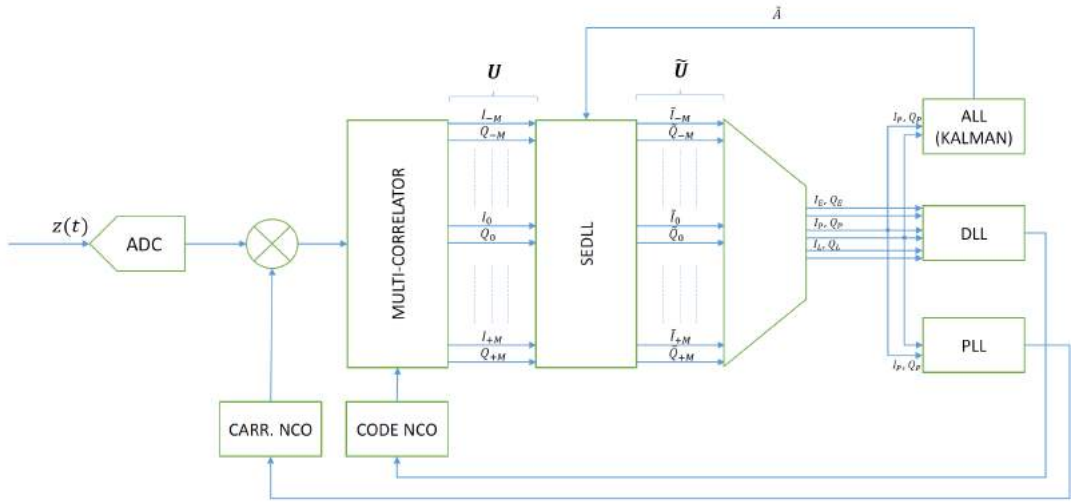


FIGURE 4.8: Block diagram of the SEDLL receiver architecture. From [34].

4.2.3 Spoofing Estimating Delay Lock Loop (SEDLL)

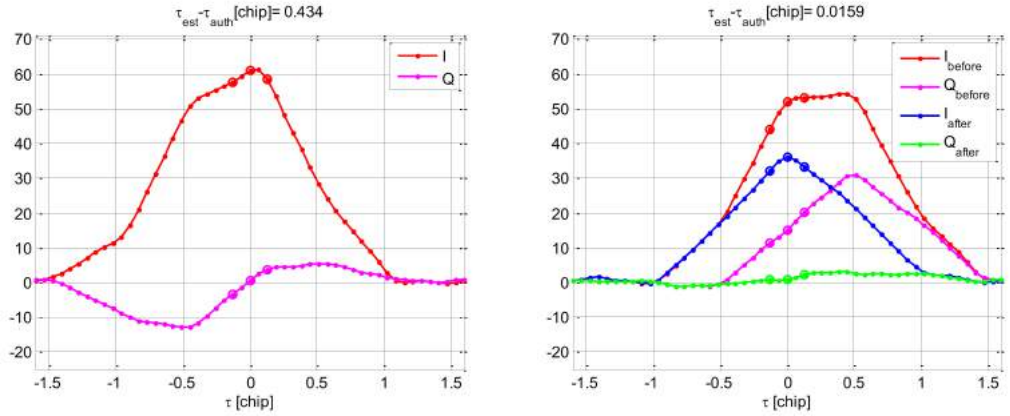
The SEDLL [34] is another promising technique, which is based on the Multipath Estimating Delay Lock Loop (MEDLL) approach. The MEDLL applies maximum likelihood estimation (MLE) in order to decrease the position error caused by multipath propagation. MEDLL largely reduces code and carrier tracking errors by simultaneously estimating the parameters of LOS and multipath signals.
The following adaptations of the MEDLL have been identified, in order to cope with spoofing specific features:

- *Algorithm initialization*: since MEDLL assumes that the authentic signal is associated with the highest peak, but the spoofer power might be greater than the authentic, a proper adaptation of the MEDLL shall be made in order to properly initialize the iterative cancellation and prevent the algorithm to cancel out the authentic peak.
- *Multi-correlator receiver*: multipath cancellation techniques are typically effective for almost synchronized, i.e. a spoofer whose delay respect to prompt correlator is in the order of few tents of chips. To address unsynchronized spoofers the monitoring correlation window shall be enlarged by increasing the number of correlators per tracking channel.

To give a brief mathematical model behind this technique, we start from the CAF of Eq. (2.13) for a single LOS path and, neglecting the Doppler estimation error, the complex baseband model of the k-th correlator output S_k at a given instant is

$$S_k = \sum_{n=0}^{P-1} \alpha_n R(\tau - \tau_n)_k e^{j\theta_n} + \eta_k \tag{4.9}$$

where $R(\tau - \tau_n)_k$ is the reference ACF, shifted by τ_n and evaluated on the k-th correlator. P is the number of path considered and η_k is a correlated Gaussian noise component. The term $\alpha_n = A_n \operatorname{sinc}(\Delta f_D T_s)$, θ_n is the phase misalignment among the n-th path and the estimated PLL phase and τ_n is the code error among the n-th path and the code delay estimated by the DLL.



(A) Standard DLL (B) SEDLL

FIGURE 4.9: SEDLL Spoofing cancellation. From [34].

The rationale behind MEDLL is to find, for all the P paths, the best estimate of the tuples $(\hat{\alpha}_n, \hat{\tau}_n, \hat{\theta}_n)$ in the ML sense, i.e. find the $\hat{S}_k = \sum_{n=0}^{P-1} \hat{\alpha}_n R(\tau - \hat{\tau}_n)_k e^{j\hat{\theta}_n}$ that minimize the quadratic norm $\left\|\boldsymbol{U} - \hat{\boldsymbol{U}}\right\|$, with $\boldsymbol{U}$ and $\hat{\boldsymbol{U}}$ vector notation for the correlator output. The estimation is performed in an iterative way: the algorithm starts estimating the main path and neglect $P-1$ paths; then, estimate two paths, neglecting $P-2$ paths, using a convenient number of steps; the process continues estimating path by path up to P.
In order to deal with the fact that MEDLL assumes that the authentic signal is associated with the highest peak, SEDLL introduces an ALL to track the amplitude of the authentic signal implemented as a Kalman filter. The Kalman is based on the observations of the amplitude and tracks the two state $x = (A, \dot{A})^{\mathsf{T}}$, i.e. the amplitude and amplitude rate. The SEDLL algorithm performs the MEDLL steps with this initial guess:

$$(\hat{a}_0^0, \hat{\tau}_0^0, \hat{\theta}_0^0) = (\tilde{A}, 0, 0)\,, \tag{4.10}$$

where $\tilde{A}$ is the predicted authentic signal amplitude as from the Kalman filter prediction stage. Delay and phase are set to 0 since it is assumed that both the DLL and PLL are tracking the authentic signal. This assumption is valid if the SEDLL is effective in canceling the spoofer. The block diagram of SEDLL is depicted in Fig. 4.8. In Fig. 4.9 a comparison of a standard DLL (on the left) with the SEDLL (on the right) is shown (plotted curves are for I and Q). In this case the spoofer is centered at 0.5 chip of delay with a phase of 45° and a amplitude of 3 dB greater than authentic signal. The standard DLL experience a code error of about 0.43 chip, while the SEDLL is able to reach 0.016 chip of error.

The main drawback of this technique comes with its sensitivity during the initialization stages. In the SEDLL architecture evolution it is foreseen to perform a combination with a spoofing detection mechanism, such as SQM metrics, in order to switch the SEDLL on only when needed. SEDLL in fact slightly degrades the DLL and PLL performance, in terms of variance of the estimates.

4.2.4 Spoofing Detection, Classification and Cancellation (SDCC)

This technique is proposed in [35] and it is divided in three stages. The first stage of the SDCC architecture is detection of a spoofing attack. Among many spoofing detection methods proposed in the literature, three low computational complexity

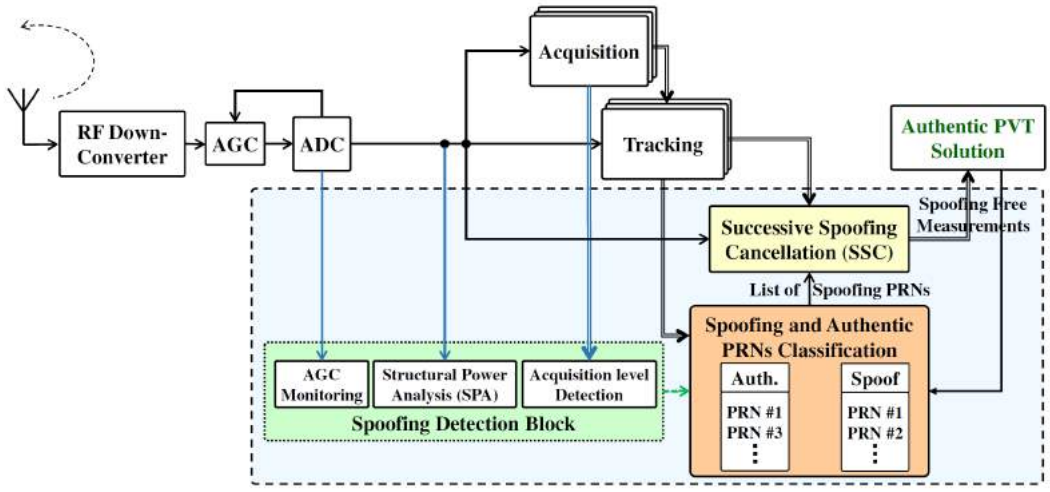


FIGURE 4.10: Block diagram of the SDCC receiver architecture. From [10].

and effective techniques are considered where include AGC gain level or ADC sample histogram monitoring, structural power analysis and acquisition level detection. The techniques check for abnormally high AGC gain levels or an unusual structural power content of the received signals to flag the presence of a possible spoofing attack. The modified signal acquisition stage includes searching all possible code phase and carrier Doppler bins and passing all the signals that are above the designated acquisition threshold to the tracking stage. Occurrence of two or more detectable signals in the acquisition stage may indicate that the receiver is under a spoofing attack and enables the spoofing detection flag.

After detecting all visible satellites which are above the acquisition threshold, all the detected signals including the authentic and spoofing signals will be tracked. In the case of a spoofing attack, the receiver requests the operator to briefly move the receiver antenna for authentic/spoofing classification. The input of the classification unit as shown in Fig. 4.10 is the tracked signal parameters including raw carrier Doppler measurements. The receiver motion can be detected by incorporating a low-cost IMU in the receiver. The authors in [28] have proposed a method based on taking pairwise correlation between signal observations to discriminate the spoofing signals from the authentic ones. Based on the measured correlation coefficient values, signals are sorted in two groups, namely spoofing and authentic. The spoofing group is the signal set that is highly correlated, and the authentic group is the set that is uncorrelated. The proper placement of the members in the authentic and spoofing groups can be reassessed after the PVT solution as the set of measurements in each group should provide the lowest navigation solution residuals.

After authentic and spoofing signal classification, SDCC enters the spoofing cancellation stage using the successive spoofing cancellation (SSC) method. The input of this processing unit, as shown in Fig. 4.10, is raw IF samples, the list of spoof PRNs and the tracked signal parameters of all channels. In this stage, the receiver continuously tracks all spoofing and authentic signals to provide accurate measurements of the signal parameters including code offset, Doppler frequency, carrier phase and signal amplitude. After reaching a reliable tracking performance for each individual spoofing channel, the tracked spoofing signals are reconstructed and removed from the original digitized IF samples to provide a spoofing-free IF sample set. After spoofing mitigation, the SDCC architecture runs acquisition again

to detect potential authentic and spoofing signals that were not detected in the first acquisition process.

Table 4.2 provides a summarized comparison among the previously discussed spoofing mitigation algorithms.

Table 4.2: Summary of spoofing mitigation techniques.

Anti-spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
Vestigial signal detection	Authentic signal is still present and can be detected	High	Medium	Multiple receiver channels	High
Multi-antenna null steering	Spoofing signals coming from the same direction	Medium	High	Multiple receiver antennas	High
SEDLL	Similarity to multipath	Medium	Medium	Multiple correlators and ALL	High
SDCC	Higher power and multiple correlation peaks for the same PRN	Medium	High	AGC monitoring, structural power analysis and synthetic array	Medium

Chapter 5

Optimal Spoofing Attacks against Signal Quality Monitoring Techniques

5.1 Spoofing Scenario

Recalling the description of a general model for a spoofing attack in Section 3.1, we restrict the formulation to a single satellite attack. Therefore, an authentic GNSS signal at the front-end output takes the form

$$r_{\mathrm{a}}(t) = A_{\mathrm{a}} D_{\mathrm{a}}(t - t_{\mathrm{p,a}}) C_{\mathrm{a}}(t - \tau_{\mathrm{a}}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D,a}})t + \phi_{\mathrm{a}}\right]} + n_{\mathrm{a}}(t)\,, \tag{5.1}$$

where the subscript 'a' stands for "authentic". On the other hand, the corresponding spoofing signal can be written in the form

$$r_{\mathrm{s}}(t) = A_{\mathrm{s}} D_{\mathrm{s}}(t - t_{\mathrm{p,s}}) C_{\mathrm{s}}(t - \tau_{\mathrm{s}}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D,s}})t + \phi_{\mathrm{s}}\right]} + n_{\mathrm{s}}(t)\,, \tag{5.2}$$

where the subscript 's' stands for "spoofing". The total received signal at the victim receiver is

$$r(t) = r_{\mathrm{a}}(t) + r_{\mathrm{s}}(t)\,. \tag{5.3}$$

The impact of a spoofing attack can be better described deriving the CAF relative to Eq. (5.3) that, extending the result in Eq. (2.13), becomes

$$S = ADR(\Delta\tau)\,\mathrm{sinc}(\Delta f_{\mathrm{D}} T_{\mathrm{coh}}) \mathrm{e}^{j\Delta\phi} + A_{\mathrm{s}} D_{\mathrm{s}} R_{\mathrm{s}}(\Delta\tau_{\mathrm{s}})\,\mathrm{sinc}\left(\Delta f_{\mathrm{D,s}} T_{\mathrm{coh}}\right) \mathrm{e}^{j\Delta\phi_{\mathrm{s}}} + \eta\,, \tag{5.4}$$

where $\Delta\tau_{\mathrm{s}} = \tau_{\mathrm{s}} - \hat{\tau}$ is the spoofer code delay error, $\Delta\phi_{\mathrm{s}} = \phi_{\mathrm{s}} - \hat{\phi}$ is the spoofer carrier phase error, $\Delta f_{\mathrm{D,s}} = f_{\mathrm{D,s}} - \hat{f}_{\mathrm{D}}$ is the spoofer Doppler error and $R_{\mathrm{s}}(\Delta\tau_{\mathrm{s}})$ is the normalized cross-correlation function between $C(kT_{\mathrm{s}})$ and $C_{\mathrm{s}}(kT_{\mathrm{s}})$ at lag $\Delta\tau_{\mathrm{s}}$. Therefore, during a spoofing attack, the correlator outputs are, in general, different from the case where only the authentic signal is present.
Finally, let's make some assumption on the spoofing scenario:

- No multipath.
- The attacker knows its position.
- The attacker knows the position of the victim and therefore he has knowledge of the amplitude A_{a}, the code delay τ_{a} and the Doppler frequency $f_{D,\mathrm{a}}$. As regards the phase ϕ_{a}, we take into consideration two possibilities: one in which the spoofer knows it, the other in which he don't.
  In order to formalize this assumption, the spoofer estimates the authentic signal

that is received by the victim receiver as

$$\tilde{r}_{\mathrm{a}}(t) = A_{\mathrm{a}} D_{\mathrm{a}}(t - t_{\mathrm{p,a}}) C_{\mathrm{a}}(t - \tau_{\mathrm{a}}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D,a}})t + \tilde{\phi}_{\mathrm{a}}\right]} + n_{\mathrm{a}}(t)\,, \tag{5.5}$$

where

$$\tilde{\phi}_{\mathrm{a}} = \begin{cases} \phi_{\mathrm{a}}\,, & \text{if the authentic phase is known}\,, \\ \sim \mathcal{U}([0, 2\pi])\,, & \text{if the authentic phase is unknown}\,, \end{cases} \tag{5.6}$$

while, as anticipated, all the other parameters of the authentic signal are assumed known by the spoofer.

Finally, the attacks that we are going to investigate consider a lift-off-aligned approach, in which the spoofer begins its attack with code and Doppler frequency aligned to the authentic signal and then gradually modifies his parameters, namely A_{s}, τ_{s} and $f_{D,\mathrm{s}}$, in order to take control of the victim receiver and lead it to the desired position.

5.2 A Trivial Attack

This attack considers the transmission of the signal of Eq. (5.2) with

$$C_{\mathrm{s}} = C_{\mathrm{a}}\,, \tag{5.7}$$

$$\phi_{\mathrm{s}} = \begin{cases} \phi_{\mathrm{a}}\,, & \text{if the authentic phase is known}\,, \\ \sim \mathcal{U}([0, 2\pi])\,, & \text{if the phase authentic is unknown}\,, \end{cases} \tag{5.8}$$

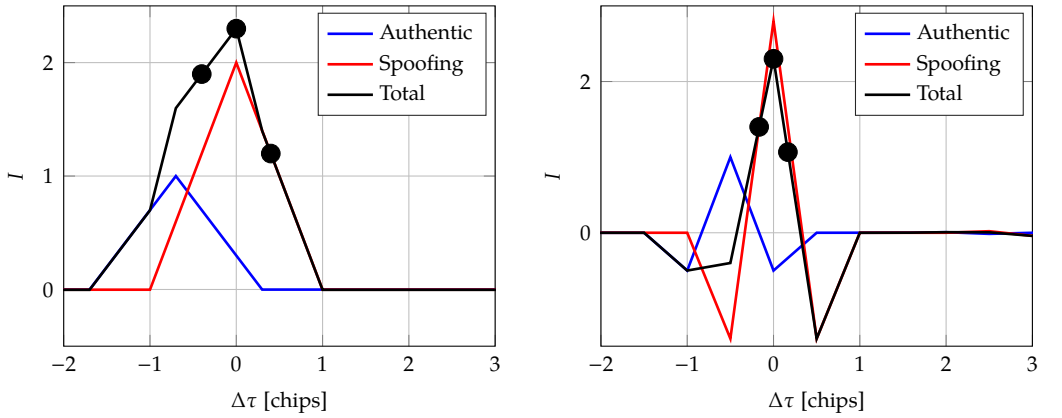
that is a signal with the same PRN code as the authentic signal.
An example of this attack in given in Fig. 5.1 for a GPS and a Galileo signal. It represents a snapshot of the in-phase correlator function of authentic, spoofing and total signal during the lift-off phase of the attack. As can be seen, early, late and prompt correlators assume a relative abnormal position with respect to that of an authentic signal in Fig. 2.9. Signal quality monitoring techniques leverage this abnormality to detect the spoofing attack, as we will se in the next section.

5.3 Signal Quality Monitoring Techniques

SQM techniques have long been employed to monitor the GPS correlation peak quality in multipath fading environments. The interaction between spoofing and authentic signals can affect the correlator output in a way similar to that of multipath components. Therefore, reference [14] has extended the previously proposed SQM techniques to detect spoofing attacks on tracking receivers working in LOS conditions. Different metrics have been proposed in order to detect any abnormal asymmetry and/or flatness of correlation peaks that is imposed by the interaction between authentic and spoofing signals and are based on combining three or more correlator outputs.

5.3.1 Metrics

There are various metrics proposed in the literature and a summary is provided here:



(A) BPSK(1) signal. Correlator spacing $d = 0.8$. Authentic code delay $\tau_a = -0.7$.

(B) BOC(1,1) signal. Correlator spacing $d = 0.33$. Authentic code delay $\tau_a = -0.5$.

FIGURE 5.1: Normalized correlation function of authentic, spoofing and total signals for two differently modulated signals as a function of $\Delta\tau$. Early, late and prompt in-phase correlator outputs of the total correlator function are also shown.

- **Delta metric (DM)**. The delta metric is defined as [14]

$$\Delta_\alpha = \frac{I_{-\alpha} - I_\alpha}{I_0} . \tag{5.9}$$

  It is based on the difference between the outputs of two correlators that are symmetric with respect to the prompt correlator. Therefore, it is easy to see that the mean value of Δ_α will tend to zero in a clean data set, and in case of asymmetries, Δ_α will be a positive or a negative number, based on the delay and phase of the spoofing signal.

- **Double delta metric (DDM)**. The double delta metric is defined as [36]

$$\Delta\Delta_{\alpha_1,\alpha_2} = \Delta_{\alpha_1} - \Delta_{\alpha_2} = \frac{[I_{-\alpha_1} - I_{\alpha_1}] - [I_{-\alpha_2} - I_{\alpha_2}]}{I_0} , \tag{5.10}$$

  with $\alpha_1 > \alpha_2$. Initially introduced as a DLL discriminator for multipath mitigation [37], this metric has been slightly modified as a proposal to provide spoofing detection. It is computed as the difference between two DMs, leading to a zero mean value in a clean data set.

- **Ratio metric (RM)**. The ratio metric is defined as [14]

$$RA_\alpha = \frac{I_{-\alpha} + I_\alpha}{I_0} . \tag{5.11}$$

  Similarly to the DM, it is used to detect distortions of the correlation function; it is based on observing the sum of early and late correlator, w.r.t. the prompt one.

- **Asymmetric ratio metric (ARM)**. The asymmetric ratio metric is defined as [36]

$$ARA_\alpha = \frac{I_\alpha}{I_0} , \tag{5.12}$$

$$ARA_{-\alpha} = \frac{I_{-\alpha}}{I_0} , \tag{5.13}$$

where the first one can be called asymmetric late ratio metric (ALRM) and the second one can be called asymmetric early ratio metric (AERM), according to the type of correlator at the numerator. These metrics are used to detect a flattened or a more pointed correlation peak, by looking to the ratio between an early/late and the prompt correlation outputs.

- **Early-late phase metric (ELPM)**. The early-late phase metric is defined as [38]

$$ELP_\alpha = \tan^{-1}\left(\frac{Q_\alpha}{I_\alpha} - \frac{Q_{-\alpha}}{I_{-\alpha}}\right). \tag{5.14}$$

  This metric has been proposed for multipath detection for L1 and L2C signals. It computes the phase difference between the early and late correlators. Moreover, it is one of the only proposed signal quality metric to incorporate the quadrature component in calculations.

- **Magnitude difference metric (MDM)**. The magnitude difference metric is defined as [13]

$$MD_\alpha = \frac{|S_{-\alpha}| - |S_\alpha|}{|S_0|}. \tag{5.15}$$

  This metric checks for symmetry like the DM, but operates with the CAF magnitude instead, therefore making use also of the quadrature component.

Now we can compute the detection threshold for each metric in order to satisfy a desired false alarm probability.

5.3.2 Detection thresholds

In general, the proposed metrics are functions of the correlator outputs, which are Gaussian random variables whose statistics are calculated in Appendix B. Therefore, we can write them in a general form as

$$Y = g(X_1, \ldots, X_N), \tag{5.16}$$

where Y is a generic metric and X_i, $i = 1, \ldots, N$ are generic in-phase or in-quadrature correlator outputs. Their cumulative distribution function (CDF) can be derived numerically with

$$\begin{aligned} F_Y(y) &= P\left[Y \leq y\right] \\ &= P\left[g(X_1, \ldots, X_N) \leq y\right] \\ &= \iint_D f_{X_1,\ldots,X_N}(x_1, \ldots, x_N) dx_1 \ldots dx_N, \end{aligned} \tag{5.17}$$

where $D = \left\{(x_1, \ldots, x_N) \mid g(x_1, \ldots, x_N) < y\right\}$. In order to find the probability density function (PDF) of Y, it is sufficient to differentiate $F_Y(y)$:

$$f_Y(y) = \frac{dF_Y(y)}{dy}. \tag{5.18}$$

Finally, the upper and lower detection thresholds are calculated such that

$$P\left[Y < \gamma_{\mathrm{l}}\right] = \int_{-\infty}^{\gamma_{\mathrm{l}}} f_Y(y)dy = P_{\mathrm{fa}}/2\,, \tag{5.19}$$

$$P\left[Y > \gamma_{\mathrm{u}}\right] = \int_{\gamma_{\mathrm{u}}}^{\infty} f_Y(y)dy = P_{\mathrm{fa}}/2\,, \tag{5.20}$$

where P_{fa} is the desired false alarm probability, which is defined as the probability that the receiver reports the presence of spoofing, even if the signal is authentic. On the other side, we can define the probability of detection P_{d} as the probability that the receiver detects a spoofing signal when it is truly present.

5.4 Nulling Attack

An attack that is able to achieve optimal results against the signal quality monitoring techniques described above is the nulling. Some hints about this attack have already been given in Section 3.4: in a nutshell, it aims at reproducing in the victim receiver a signal equal to the authentic signal that the victim would receive if he really was in the spoofed location. This is done by superposing two signals:

- A replica of the authentic signal in phase opposition with it, leading to the cancellation of the legit signal.
- An authentic-like signal with the parameters that leads the victim receiver to the desired spoofing location.

Therefore, the mathematical formulation of the spoofing signal is

$$r_{\mathrm{s}}(t) = \bar{r}(t) - \tilde{r}_{\mathrm{a}}(t)\,, \tag{5.21}$$

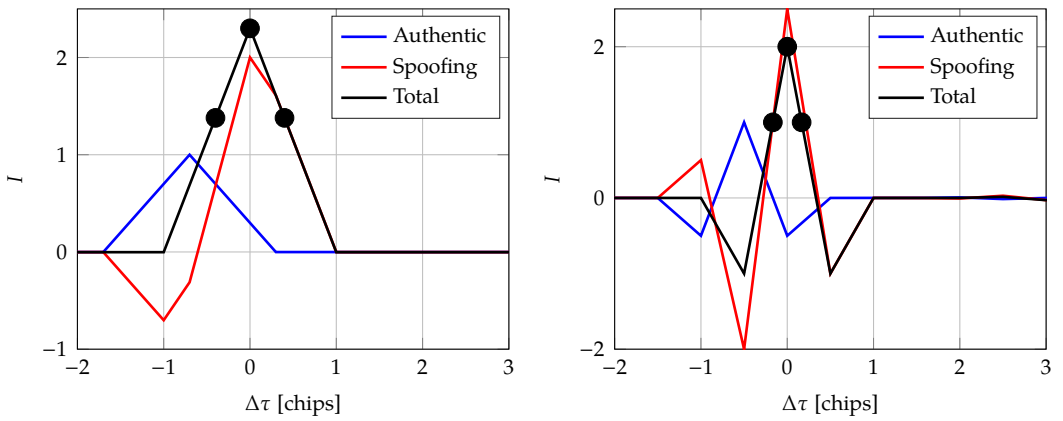
where

$$\bar{r}(t) = AD(t - t_{\mathrm{p}})C_{\mathrm{a}}(t - \tau)\mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}}+f_{\mathrm{D}})t+\phi\right]}\,, \tag{5.22}$$

is the target total received signal where all the parameters are decided by the spoofer in order to force the desired spoofing location.
An example of this attack in given in Fig. 5.2 for a GPS and a Galileo signal. As in the trivial attack example, it represents a snapshot of the in-phase correlator function of authentic, spoofing and total signal during the lift-off phase of the attack. As anticipated, the total signal is an authentic-like signal where the authentic signal is completely canceled out.

5.5 Optimal Attack

The aim of the attack is to make sure that the probability of detection of the spoofing signal is the smallest possible. As seen above, an attack that is able to achieve great results is the nulling attack. However, comparable performance can be obtained by using a minor amount of energy. Indeed, instead of reproducing an entirely authentic-like signal, why not spoof a signal that looks authentic only on the correlators which are used for the tracking and for the SQM metrics? The basic idea is to create a spoofing signal with the minimum energy such that is "trackable" and which generates a SQM metric value as close as possible to that of an authentic signal.



(A) BPSK(1) signal. Correlator spacing $d = 0.8$. Authentic code delay $\tau_a = -0.7$.

(B) BOC(1,1) signal. Correlator spacing $d = 0.33$. Authentic code delay $\tau_a = -0.5$.

FIGURE 5.2: Normalized correlation function of authentic, spoofing and total signals for two differently modulated signals as a function of $\Delta\tau$. Early, late and prompt in-phase correlator outputs of the total correlator function are also shown.

In order to give a mathematical formulation to the problem described above, in some circumstances it is useful to think in the frequency domain. Therefore, the Fourier transform notation of the signals involved in given in Table 5.1.

5.5.1 Constraints

There are three type of constraints on the signal that is received by the victim receiver:

- It must be tracked by the receiver, of course.
- The SQM metric computed from it must assume values as close as possible to the values generated by an authentic signal.
- Around the correlators, it must be seen as similar as possible to an authentic signal by the receiver, such that a small lack of synchronization does not compromise the attack.

These points are analyzed one by one in the following.

Trackability As a first requirement, the total signal received by the victim must be tracked by the receiver. Given that every DLL discriminator watches at the unbalance

TABLE 5.1: Signals involved in the attack in their time and frequency domain version.

Signal	Time domain	Frequency domain
Local replica (Eq. (2.11))	$\hat{r}(t)$	$\hat{\mathcal{R}}(f)$
Authentic signal estimate (Eq. (5.5))	$\tilde{r}_a(t)$	$\tilde{\mathcal{R}}_a(f)$
Spoofing signal (Eq. (5.2))	$r_s(t)$	$\mathcal{R}_s(f)$
Total signal (Eq. (5.3))	$r(t)$	$\mathcal{R}(f)$
CAF (Eq. (5.4))	$S(\tau)$	$\mathcal{S}(f)$

between the in-phase CAF components at the early and late correlators (with distance α_{DLL} chips from the prompt correlator), the conditions to be satisfied are

$$\begin{cases} I_{-\alpha_{\mathrm{DLL}}} - I_{\alpha_{\mathrm{DLL}}} = 0\,, \\ Q_{-\alpha_{\mathrm{DLL}}} = 0\,, \\ Q_{\alpha_{\mathrm{DLL}}} = 0\,, \end{cases} \tag{5.23}$$

where the last two conditions must hold for those discriminators that use the in-quadrature components for their code delay estimate.
Focusing on the first condition of Eq. (5.23), given that $I = \mathrm{Re}\{S\}$, it becomes

$$\mathrm{Re}\{S_{-\alpha_{\mathrm{DLL}}}\} - \mathrm{Re}\{S_{\alpha_{\mathrm{DLL}}}\} = 0\,, \tag{5.24}$$

and switching to frequency domain we obtain

$$\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \mathcal{S}(f)\left(\mathrm{e}^{-j2\pi f(-\alpha_{\mathrm{DLL}})T_\mathrm{c}} - \mathrm{e}^{-j2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}}\right)df\right\} = 0\,, \tag{5.25}$$

where $F_\mathrm{s} = 1/T_\mathrm{s}$. Now, by the cross-correlation theorem $\mathcal{S}(f) = \mathcal{R}^*(f)\hat{\mathcal{R}}(f)$, so Eq. (5.25) can be written as

$$\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \mathcal{R}^*(f)\hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right)df\right\} = 0\,, \tag{5.26}$$

where $\mathcal{R}^*(f) = \tilde{\mathcal{R}}_\mathrm{a}^*(f) + \mathcal{R}_\mathrm{s}^*(f)$, leading to

$$\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \left(\tilde{\mathcal{R}}_\mathrm{a}^*(f) + \mathcal{R}_\mathrm{s}^*(f)\right)\hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right)df\right\} = 0\,. \tag{5.27}$$

Now we write the above formula as

$$\begin{aligned} &\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \mathcal{R}_\mathrm{s}^*(f)\hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right)df\right\} \\ &= -\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \tilde{\mathcal{R}}_\mathrm{a}^*(f)\hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right)df\right\}, \end{aligned} \tag{5.28}$$

where we call

$$\hat{\mathcal{R}}_{\mathrm{DLL}}(f) = \hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right), \tag{5.29}$$

$$b_{\mathrm{DLL}} = -\int_0^{F_\mathrm{s}} \tilde{\mathcal{R}}_\mathrm{a}^*(f)\hat{\mathcal{R}}(f)2j\sin\left(2\pi f\alpha_{\mathrm{DLL}}T_\mathrm{c}\right)df\,, \tag{5.30}$$

so that Eq. (5.28) becomes

$$\mathrm{Re}\left\{\int_0^{F_\mathrm{s}} \mathcal{R}_\mathrm{s}^*(f)\hat{\mathcal{R}}_{\mathrm{DLL}}(f)df\right\} = \mathrm{Re}\{b_{\mathrm{DLL}}\}\,, \tag{5.31}$$

which, finally, can be rewritten as

$$\mathrm{Re}\left\{\langle\hat{\mathcal{R}}_{\mathrm{DLL}}, \mathcal{R}_\mathrm{s}\rangle\right\} = \mathrm{Re}\{b_{\mathrm{DLL}}\}\,, \tag{5.32}$$

where $\langle \cdot, \cdot \rangle$ stands for the inner product in $\mathscr{H}_2$. Now, the last two conditions of Eq. (5.23) must be considered, and, after some calculations they become

$$\begin{cases} \mathrm{Im}\left\{\langle \hat{\mathcal{R}}_{\mathrm{E,DLL}}, \mathcal{R}_{\mathrm{s}} \rangle\right\} = \mathrm{Im}\{b_{\mathrm{E,DLL}}\}\,, \\ \mathrm{Im}\left\{\langle \hat{\mathcal{R}}_{\mathrm{L,DLL}}, \mathcal{R}_{\mathrm{s}} \rangle\right\} = \mathrm{Im}\{b_{\mathrm{L,DLL}}\}\,, \end{cases} \tag{5.33}$$

where

$$\hat{\mathcal{R}}_{\mathrm{E,DLL}}(f) = \hat{\mathcal{R}}(f)\mathrm{e}^{-j2\pi f(-\alpha_{\mathrm{DLL}})T_{\mathrm{c}}}\,, \tag{5.34}$$

$$b_{\mathrm{E,DLL}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}_{\mathrm{a}}^*(f)\hat{\mathcal{R}}(f)\mathrm{e}^{-j2\pi f(-\alpha_{\mathrm{DLL}})T_{\mathrm{c}}}df \tag{5.35}$$

and

$$\hat{\mathcal{R}}_{\mathrm{L,DLL}}(f) = \hat{\mathcal{R}}(f)\mathrm{e}^{-j2\pi f\alpha_{\mathrm{DLL}}T_{\mathrm{c}}}\,, \tag{5.36}$$

$$b_{\mathrm{L,DLL}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}_{\mathrm{a}}^*(f)\hat{\mathcal{R}}(f)\mathrm{e}^{-j2\pi f\alpha_{\mathrm{DLL}}T_{\mathrm{c}}}df\,, \tag{5.37}$$

which concludes the constraints for the DLL discriminator.
Some DLL discriminator and all the PLL and FLL discriminators make use of the prompt correlator, therefore we set a condition to ensure that it has only the in-phase component:

$$\begin{cases} I_0 = A \\ Q_0 = 0 \end{cases} \quad \Leftrightarrow \quad S_0 = A\,, \tag{5.38}$$

with $A \in \mathbb{R}$. Using similar calculations than those made above, the resulting condition becomes:

$$\langle \hat{\mathcal{R}}_{\mathrm{PLL}}, \mathcal{R}_{\mathrm{s}} \rangle = b_{\mathrm{PLL}}\,, \tag{5.39}$$

where

$$\hat{\mathcal{R}}_{\mathrm{PLL}}(f) = \hat{\mathcal{R}}(f)\,, \tag{5.40}$$

$$b_{\mathrm{PLL}} = A - \int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}_{\mathrm{a}}^*(f)\hat{\mathcal{R}}(f)df\,. \tag{5.41}$$

Finally, Eqs. (5.32), (5.33) and (5.39) are the conditions such that the signal received by the victim receiver is trackable.

SQM Metric Undetectability Among the features which the signal received by the victim mush have, the second requirement is that its probability of detection should be as close as possible to the probability of false alarm. In order to accomplish this, it is sufficient to set

$$(1-\epsilon)M_{\mathrm{a}} \leq M(S_{-\alpha_{\mathrm{SQM}}}, S_0, S_{\alpha_{\mathrm{SQM}}}) \leq (1+\epsilon)M_{\mathrm{a}}\,, \tag{5.42}$$

where M is a generic metric among those presented in the previous section and it is written as a function of the prompt, early and late correlators (the last two with distance α_{SQM} chips from the prompt one). Moreover, M_{a} is the value that the metric M assumes when the signal is authentic and it depends on the values assumed by the autocorrelation function R on the SQM correlators. Finally, ϵ is a parameter that specify the precision with which we want to be close to the authentic metric value.

Using similar calculations of those done in the tracking on Eq. (5.42), the constraints for the metrics that depends only on the in-phase components of the correlator outputs can be summarized in the common expression

$$\pm \operatorname{Re}\left\{\langle \hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}, \mathcal{R}_{\mathrm{s}} \rangle\right\} \leq \pm \operatorname{Re}\left\{b^{\pm}_{\mathrm{SQM}}\right\}, \tag{5.43}$$

where $\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f)$ and $b^{\pm}_{\mathrm{SQM}}$ are different for every metric and they are defined as follows:

- Delta metric:

$$\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f) = \hat{\mathcal{R}}(f)\left[2j\sin\left(2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\right], \tag{5.44}$$

$$b^{\pm}_{\mathrm{SQM}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left[2j\sin\left(2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\right] df, \tag{5.45}$$

  with

$$M_{\mathrm{a}} = \frac{R(-\alpha_{\mathrm{SQM}}) - R(\alpha_{\mathrm{SQM}})}{R(0)}. \tag{5.46}$$

- Double delta metric:

$$\begin{aligned}\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f) = \hat{\mathcal{R}}(f)\Big[&2j\sin\left(2\pi f \alpha_{1,\mathrm{SQM}} T_{\mathrm{c}}\right) \\ &-2j\sin\left(2\pi f \alpha_{2,\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\Big],\end{aligned} \tag{5.47}$$

$$\begin{aligned}b^{\pm}_{\mathrm{SQM}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\Big[&2j\sin\left(2\pi f \alpha_{1,\mathrm{SQM}} T_{\mathrm{c}}\right) \\ &-2j\sin\left(2\pi f \alpha_{2,\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\Big] df,\end{aligned} \tag{5.48}$$

  with

$$M_{\mathrm{a}} = \frac{\left[R(-\alpha_{1,\mathrm{SQM}}) - R(\alpha_{1,\mathrm{SQM}})\right] - \left[R(-\alpha_{2,\mathrm{SQM}}) - R(\alpha_{2,\mathrm{SQM}})\right]}{R(0)}. \tag{5.49}$$

- Ratio metric:

$$\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f) = \hat{\mathcal{R}}(f)\left[2\cos\left(2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\right], \tag{5.50}$$

$$b^{\pm}_{\mathrm{SQM}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left[2\cos\left(2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}\right) - (1 \pm \epsilon) M_{\mathrm{a}}\right] df, \tag{5.51}$$

  with

$$M_{\mathrm{a}} = \frac{R(-\alpha_{\mathrm{SQM}}) + R(\alpha_{\mathrm{SQM}})}{R(0)}. \tag{5.52}$$

- Asymmetric ratio metric (early correlator):

$$\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f) = \hat{\mathcal{R}}(f)\, \mathrm{e}^{-j2\pi f(-\alpha_{\mathrm{SQM}})T_{\mathrm{c}}}, \tag{5.53}$$

$$b^{\pm}_{\mathrm{SQM}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left[\mathrm{e}^{-j2\pi f(-\alpha_{\mathrm{SQM}})T_{\mathrm{c}}} - (1 \pm \epsilon) M_{\mathrm{a}}\right] df, \tag{5.54}$$

  with

$$M_{\mathrm{a}} = \frac{R(-\alpha_{\mathrm{SQM}})}{R(0)}. \tag{5.55}$$

- Asymmetric ratio metric (late correlator):

$$\hat{\mathcal{R}}^{\pm}_{\mathrm{SQM}}(f) = \hat{\mathcal{R}}(f)\, \mathrm{e}^{-j2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}}\,, \tag{5.56}$$

$$b^{\pm}_{\mathrm{SQM}} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left[\mathrm{e}^{-j2\pi f \alpha_{\mathrm{SQM}} T_{\mathrm{c}}} - (1 \pm \epsilon) M_{\mathrm{a}}\right] df\,, \tag{5.57}$$

with

$$M_{\mathrm{a}} = \frac{R(\alpha_{\mathrm{SQM}})}{R(0)}\,. \tag{5.58}$$

As regards early-late phase and magnitude difference metrics, they are based on non-linear combinations of the in-phase and in-quadrature components and therefore they cannot included in our attack strategy. However, it must be said that in order to mislead the ELPM, it would be sufficient for the spoofing signal to be in-phase with the authentic signal. The same reasoning can be done with the MDM, with a further condition that the in-phase correlators should satisfy the delta metric.

Authentic Signal Similarity In order for the spoofing signal to be robust to non-perfect code delay synchronization with the authentic signal, we must ensure that the slope of the correlation function around the in-phase correlator outputs of the total received signal is equal to that of the authentic signal. In this way the value assumed by the correlator outputs will be always within the regular range as if the signal was authentic. The condition to accomplish this task is

$$\left.\frac{dI(\tau)}{d\tau}\right|_{\tau=\pm\alpha} = D_{\mathrm{a}}\,, \tag{5.59}$$

with

$$D_{\mathrm{a}} = \left.\frac{dR(\tau)}{d\tau}\right|_{\tau=\pm\alpha}\,, \tag{5.60}$$

where D_{a} is the slope of the autocorrelation function R at the correlators of interest. As usual, after some calculations Eq. (5.59) can be written as

$$\mathrm{Re}\left\{\langle \hat{\mathcal{R}}_{\mathrm{E,DER},i}, \mathcal{R}_{\mathrm{s}}\rangle\right\} = \mathrm{Re}\{b_{\mathrm{E,DER},i}\}\,, \qquad \text{for } i = \mathrm{DLL}, \mathrm{SQM}\,, \tag{5.61}$$

where

$$\hat{\mathcal{R}}_{\mathrm{E,DER},i}(f) = \hat{\mathcal{R}}(f)\left(j2\pi f \mathrm{e}^{-j2\pi f(-\alpha_i)T_{\mathrm{c}}} - D_{\mathrm{a}}\right)\,, \tag{5.62}$$

$$b_{\mathrm{E,DER},i} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left(j2\pi f \mathrm{e}^{-j2\pi f(-\alpha_i)T_{\mathrm{c}}} - D_{\mathrm{a}}\right) df\,, \tag{5.63}$$

for early correlators and

$$\mathrm{Re}\left\{\langle \hat{\mathcal{R}}_{\mathrm{L,DER},i}, \mathcal{R}_{\mathrm{s}}\rangle\right\} = \mathrm{Re}\{b_{\mathrm{L,DER},i}\}\,, \qquad \text{for } i = \mathrm{DLL}, \mathrm{SQM}\,, \tag{5.64}$$

where

$$\hat{\mathcal{R}}_{\mathrm{L,DER},i}(f) = \hat{\mathcal{R}}(f)\left(j2\pi f \mathrm{e}^{-j2\pi f \alpha_i T_{\mathrm{c}}} - D_{\mathrm{a}}\right)\,, \tag{5.65}$$

$$b_{\mathrm{L,DER},i} = -\int_0^{F_{\mathrm{s}}} \tilde{\mathcal{R}}^{*}_{\mathrm{a}}(f)\hat{\mathcal{R}}(f)\left(j2\pi f \mathrm{e}^{-j2\pi f \alpha_i T_{\mathrm{c}}} - D_{\mathrm{a}}\right) df\,, \tag{5.66}$$

for late correlators.

5.5.2 Optimization Problem

The energy of the spoofing signal is defined as

$$E_{\mathrm{s}} = \langle \mathcal{R}_{\mathrm{s}}, \mathcal{R}_{\mathrm{s}} \rangle = \int_0^{F_{\mathrm{s}}} \left| \mathcal{R}_{\mathrm{s}}(f) \right|^2 df \,, \tag{5.67}$$

therefore the optimization problem can be written as

$$\begin{aligned}
\mathcal{R}_{\mathrm{s}}^*(f) = \underset{\mathcal{R}_{\mathrm{s}}(f)}{\arg\min} \quad & E_{\mathrm{s}} \\
\text{s.t.} \qquad & \mathrm{Re}\left\{ \langle \hat{\mathcal{R}}_{\mathrm{DLL}}, \mathcal{R}_{\mathrm{s}} \rangle \right\} = \mathrm{Re}\{ b_{\mathrm{DLL}} \}, \\
& \mathrm{Im}\left\{ \langle \hat{\mathcal{R}}_{\mathrm{E,DLL}}, \mathcal{R}_{\mathrm{s}} \rangle \right\} = \mathrm{Im}\{ b_{\mathrm{E,DLL}} \}, \\
& \mathrm{Im}\left\{ \langle \hat{\mathcal{R}}_{\mathrm{L,DLL}}, \mathcal{R}_{\mathrm{s}} \rangle \right\} = \mathrm{Im}\{ b_{\mathrm{L,DLL}} \}, \\
& \langle \hat{\mathcal{R}}_{\mathrm{PLL}}, \mathcal{R}_{\mathrm{s}} \rangle = b_{\mathrm{PLL}}, \\
& \mathrm{Re}\left\{ \langle \hat{\mathcal{R}}^{+}_{\mathrm{SQM}}, \mathcal{R}_{\mathrm{s}} \rangle \right\} \leq \mathrm{Re}\left\{ b^{+}_{\mathrm{SQM}} \right\}, \\
& -\mathrm{Re}\left\{ \langle \hat{\mathcal{R}}^{-}_{\mathrm{SQM}}, \mathcal{R}_{\mathrm{s}} \rangle \right\} \leq -\mathrm{Re}\left\{ b^{-}_{\mathrm{SQM}} \right\}, \\
& \mathrm{Re}\left\{ \langle \hat{\mathcal{R}}_{\mathrm{E,DER},i}, \mathcal{R}_{\mathrm{s}} \rangle \right\} = \mathrm{Re}\{ b_{\mathrm{E,DER},i} \}, \quad i = \mathrm{DLL}, \mathrm{SQM}, \\
& \mathrm{Re}\left\{ \langle \hat{\mathcal{R}}_{\mathrm{L,DER},i}, \mathcal{R}_{\mathrm{s}} \rangle \right\} = \mathrm{Re}\{ b_{\mathrm{L,DER},i} \}, \quad i = \mathrm{DLL}, \mathrm{SQM},
\end{aligned} \tag{5.68}$$

where the first four constraints are relative to the trackability, the fifth and sixth concern the undetectability and the last two ensure the right slope on the correlator outputs.

The first step to solve this optimization problem is to derive an orthonormal basis for the set of signals

$$\begin{aligned}
\mathcal{B} = \{ & \hat{\mathcal{R}}_{\mathrm{DLL}}(f), \hat{\mathcal{R}}_{\mathrm{E,DLL}}(f), \hat{\mathcal{R}}_{\mathrm{L,DLL}}(f), \hat{\mathcal{R}}_{\mathrm{PLL}}(f), \hat{\mathcal{R}}^{+}_{\mathrm{SQM}}(f), \hat{\mathcal{R}}^{-}_{\mathrm{SQM}}(f), \\
& \hat{\mathcal{R}}_{\mathrm{E,DER},i}(f), \hat{\mathcal{R}}_{\mathrm{L,DER},i}(f) \} \,, \qquad i = \mathrm{DLL}, \mathrm{SQM} \,,
\end{aligned} \tag{5.69}$$

and this can be done by applying the Graham-Schmidt orthonormalization procedure to the above set, obtaining

$$\hat{\mathcal{B}} = \{ \hat{\mathcal{R}}_i(f) \} \,, \qquad i = 1, \ldots, K \,, \tag{5.70}$$

that is a set of orthonormal functions of cardinality $K \leq |\mathcal{B}|$, which we take as a basis of a signal space. Since this basis is derived from $\mathcal{B}$, all the functions in $\mathcal{B}$ belong to the signal space generated by $\hat{\mathcal{B}}$.
At this point, since all the constraints are in the form of inner products between the functions of $\mathcal{B}$ and $\mathcal{R}_{\mathrm{s}}(f)$, we can state that the signal $\mathcal{R}_{\mathrm{s}}(f)$ of minimum energy must lie in the same signal space as the elements in $\mathcal{B}$. This fact can be translated into defining

$$\mathcal{R}_{\mathrm{s}}(f) = \sum_{i=1}^{K} r_i \hat{\mathcal{R}}_i(f) \,, \tag{5.71}$$

that is, the spoofing signal can be written as a linear combination of the functions of basis $\hat{\mathcal{B}}$.

From this fact, the energy of $\mathcal{R}_{\mathrm{s}}(f)$ can be expressed as

$$E_{\mathrm{s}} = \sum_{i=1}^{K} |r_i|^2 df \,. \tag{5.72}$$

Moreover, leaving aside for the moment the $\mathrm{Re}\{\cdot\}$ and $\mathrm{Im}\{\cdot\}$ operators, each equality constraint can be rewritten as

$$\sum_{i=1}^{K} \hat{\mathcal{R}}_{\star}(f) r_i^* \hat{\mathcal{R}}_i^*(f) = b_{\star} \,, \tag{5.73}$$

where $\star$ is a placeholder for a specific signal of $\mathcal{B}$. Using a matrix notation, the above formula is equivalent to

$$\begin{bmatrix} \hat{\mathcal{R}}_{\star}(f)\hat{\mathcal{R}}_1^*(f) & \cdots & \hat{\mathcal{R}}_{\star}(f)\hat{\mathcal{R}}_K^*(f) \end{bmatrix} \begin{bmatrix} r_1^* \\ \vdots \\ r_K^* \end{bmatrix} = b_{\star} \,. \tag{5.74}$$

This is a complex linear equation, but now we have to deal with the fact that all but one of the constraints are encapsulated in a $\mathrm{Re}\{\cdot\}$ or $\mathrm{Im}\{\cdot\}$ operator. In order to solve this problem, we exploit the matrix representation of a complex number, that is

$$x + jy \leftrightarrow \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \,, \tag{5.75}$$

which allows to reformulate Eq. (5.74) as

$$\mathbf{A}_{\star}\mathbf{r} = \mathbf{b}_{\star} \tag{5.76}$$

with

$$\mathbf{A}_{\star} = \begin{bmatrix} \mathbf{A}_{\star,\mathrm{RE}} \\ \mathbf{A}_{\star,\mathrm{IM}} \end{bmatrix} \tag{5.77}$$

$$= \begin{bmatrix} \mathrm{Re}\{\hat{\mathcal{R}}_{1,\star}(f)\} & -\mathrm{Im}\{\hat{\mathcal{R}}_{1,\star}(f)\} & \cdots & \mathrm{Re}\{\hat{\mathcal{R}}_{K,\star}(f)\} & -\mathrm{Im}\{\hat{\mathcal{R}}_{K,\star}(f)\} \\ \mathrm{Im}\{\hat{\mathcal{R}}_{1,\star}(f)\} & \mathrm{Re}\{\hat{\mathcal{R}}_{1,\star}(f)\} & \cdots & \mathrm{Im}\{\hat{\mathcal{R}}_{K,\star}(f)\} & \mathrm{Re}\{\hat{\mathcal{R}}_{K,\star}(f)\} \end{bmatrix} \,, \tag{5.78}$$

$$\mathbf{r} = \begin{bmatrix} \mathrm{Re}\{r_1\} \\ -\mathrm{Im}\{r_1\} \\ \vdots \\ \mathrm{Re}\{r_K\} \\ -\mathrm{Im}\{r_K\} \end{bmatrix} \,, \tag{5.79}$$

$$\mathbf{b}_{\star} = \begin{bmatrix} \mathrm{Re}\{b_{\star}\} \\ \mathrm{Im}\{b_{\star}\} \end{bmatrix} \,, \tag{5.80}$$

where $\hat{\mathcal{R}}_{i,\star}(f) = \hat{\mathcal{R}}_{\star}(f)\hat{\mathcal{R}}_i^*(f)$, $i = 1, \ldots, K$. Now, we can extend this result to those constraints that contain the $\mathrm{Re}\{\cdot\}$ or $\mathrm{Im}\{\cdot\}$ operators. In particular, for the first ones Eq. (5.76) becomes

$$\mathbf{A}_{\star,\mathrm{RE}}\mathbf{r} = \mathbf{b}_{\star} \,, \tag{5.81}$$

and for the second ones Eq. (5.76) turns into

$$\mathbf{A}_{\star,\mathrm{IM}}\mathbf{r} = \mathbf{b}_{\star} \,, \tag{5.82}$$

where $\mathbf{A}_{\star,\mathrm{RE}}$ and $\mathbf{A}_{\star,\mathrm{IM}}$ are defined in Eq. (5.77). Given that Eqs. (5.81) and (5.82) are real equations, they can be extended to the inequality constraints.

Now, by using the results of Eqs. (5.72), (5.74), (5.81) and (5.82), we can reformulate the optimization problem of Eq. (5.68) as

$$\begin{aligned}
\mathcal{R}_{\mathrm{s}}^{*}(f) = \underset{r_1,\ldots,r_K}{\arg\min} \quad & E_{\mathrm{s}} \\
\text{s.t.} \quad & \mathbf{A}_{\mathrm{DLL,RE}}\mathbf{r} = \mathbf{b}_{\mathrm{DLL}}, \\
& \mathbf{A}_{\mathrm{E,DLL,IM}}\mathbf{r} = \mathbf{b}_{\mathrm{E,DLL}}, \\
& \mathbf{A}_{\mathrm{L,DLL,IM}}\mathbf{r} = \mathbf{b}_{\mathrm{L,DLL}}, \\
& \mathbf{A}_{\mathrm{PLL}}\mathbf{r} = \mathbf{b}_{\mathrm{PLL}}, \\
& \mathbf{A}^{+}_{\mathrm{SQM,RE}}\mathbf{r} \leq \mathbf{b}^{+}_{\mathrm{SQM}}, \\
& -\mathbf{A}^{-}_{\mathrm{SQM,RE}}\mathbf{r} \leq -\mathbf{b}^{-}_{\mathrm{SQM}}, \\
& \mathbf{A}_{\mathrm{E,DER,RE}}\mathbf{r} = \mathbf{b}_{\mathrm{E,DER},i}, \quad i = \mathrm{DLL}, \mathrm{SQM}, \\
& \mathbf{A}_{\mathrm{E,DER,RE}}\mathbf{r} = \mathbf{b}_{\mathrm{L,DER},i}, \quad i = \mathrm{DLL}, \mathrm{SQM},
\end{aligned} \tag{5.83}$$

where $\mathcal{R}_{\mathrm{s}}^{*}(f)$ is the desired optimal spoofing signal that, in the time domain, becomes $r_{\mathrm{s}}^{*}(t) = \mathcal{F}^{-1}[\mathcal{R}_{\mathrm{s}}^{*}(f)]$.

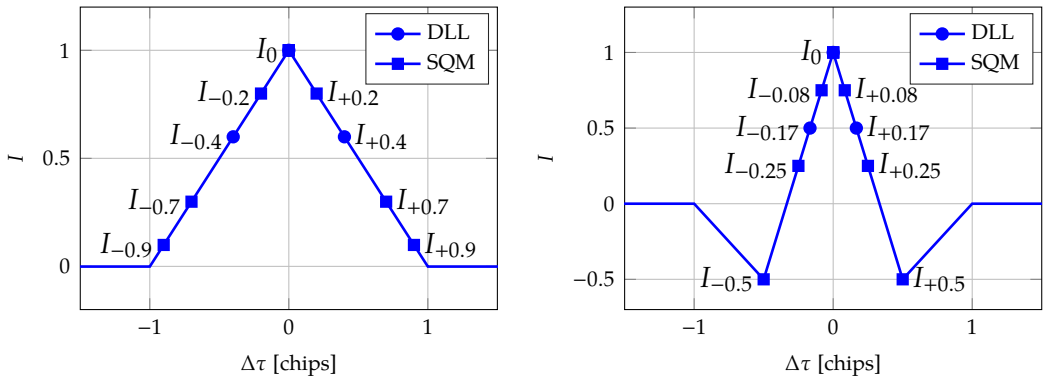
Chapter 6

Security Evaluation of the Signal Quality Monitoring Techniques

All the plots shown in this Chapter are obtained through running MATLAB® scripts. Unless otherwise indicated, the parameters that are used in the simulations are those reported in Table 6.1. Moreover, in Fig. 6.1 the ACF of the BPSK(1) and BOC(1,1) signals are represented; the BPSK(1) modulation is used in the GPS L1 C/A signal, while the BOC(1,1) one is used in Galileo E1B/E1C signals in combination with the BOC(6,1) modulation, therefore, it is trivial to extend the obtained results for the total modulation. The default correlators that will be used are reported in Table 6.1.

As an example of how the proposed algorithm works, in Fig. 6.2 the in-phase correlator outputs of the authentic, spoofing and total signals are represented in a snapshot of the optimal attack with the default parameters for a GPS signal. As we can see, the DLL correlators exhibit the same value, while the SQM correlators are such the SQM metrics return a value that is the same as an authentic one. Moreover, the slope of the correlation function around all the correlators is very similar to that of a standard signal. In order to evaluate the performance of the SQM metrics, a snapshot of a lift-off-aligned attack with the proposed optimal spoofing signal will be considered and 10^6 attempts of the attack during this snapshot will be performed. This strategy will be used to make three comparison between attacks by varying some parameters of Table 6.1:

- Different authentic code delays τ_a. We will see how the performance change with respect to of the relative code delay distance between the authentic and the spoofing signals.



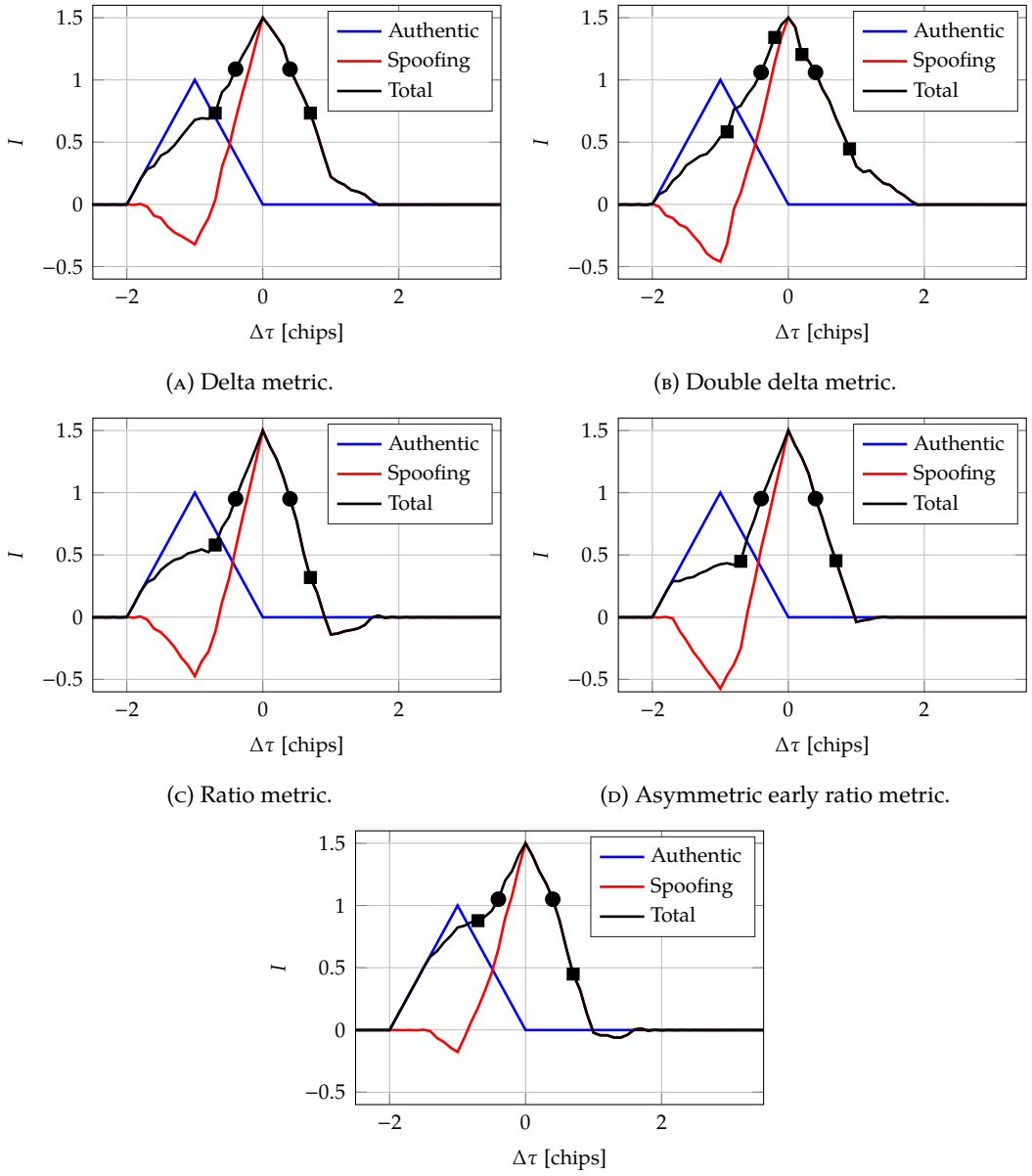
(A) BPSK(1) signal.

(B) BOC(1,1) signal.

FIGURE 6.1: Normalized ACF of the two signals that are used in the simulations.

- Comparison between different metric precisions ϵ. As ϵ increases, we will expect an improvement of the performance while the spoofer will be spending less energy.
- Nulling and optimal attack with unknown authentic phase $\tilde{\phi}$a. We will see if the nulling attack will remain better than the proposed attack.

The comparisons will be in terms of the receiver operating characteristic (ROC), that is a graphical plot of the probability of detection against the probability of false alarm. Moreover, the normalized energy of the spoofing and the total signal will be also given and they will be useful to for the performance evaluation.
Finally, a simulation of a lift-off-aligned attack will be performed.



(A) Delta metric.

(B) Double delta metric.

(C) Ratio metric.

(D) Asymmetric early ratio metric.

(E) Asymmetric late ratio metric.

FIGURE 6.2: Authentic, spoofing and total correlation function during a snapshot of the optimal attack with default parameters (BPSK(1,1) signal).

TABLE 6.1: Default parameters.

Type	Parameter	Value
General	Number of attempts	10^6 attempts
	f_{IF}	0 Hz
	M	1
	C/N_0	45 dB − Hz
	Upsampling factor	10 (for BPSK(1)) – 12 (for BOC(1,1))
Local replica $\hat{r}(t)$ (Eq. (2.11))	$\hat{\tau}$	0 chip
	$\hat{f}_{\text{D}}$	0 Hz
	$\hat{\phi}$	0 rad
Authentic signal $r_{\text{a}}(t)$ (Eq. (5.1))	A_{a}	1
	D_{a}	1
	C_{a}	PRN 1
	τ_{a}	−1 chip
	$f_{\text{D,a}}$	0 Hz
	ϕ_{a}	0 rad
Authentic signal estimate $\tilde{r}_{\text{a}}(t)$ (Eq. (5.5))	$\tilde{\phi}_{\text{a}}$	0 rad
Total signal for nulling attack $\bar{r}(t)$ (Eq. (5.22))	A (also for optimal attack)	1.5
	D	1
	τ	0 chip
	f_{D}	0 Hz
	ϕ	0 rad
DLL/PLL discriminator	$d_{\text{DLL}} = d_{\text{PLL}}$	0.8 chip (for BPSK(1)) – 0.33 chip (for BOC(1,1))
SQM metric	d_{SQM}	1.4 chip (for BPSK(1)) – 0.5 chip (for BOC(1,1))
	$d_{\text{SQM,1}}$ (only for double delta metric)	1.8 chip (for BPSK(1)) – 1 chip (for BOC(1,1))
	$d_{\text{SQM,2}}$ (only for double delta metric)	0.4 chip (for BPSK(1)) – 0.167 chip (for BOC(1,1))
	ϵ	0

6.1 Comparison between different authentic code delays

This Section provides a performance comparison of the SQM metrics between five different authentic code delays: $\tau_a = 0, -0.5, -1, -1.5, -2$. The results for the BPSK(1) signal are reported in Fig. 6.3 and Table 6.2, while for the BOC(1,1) signal in Fig. 6.4 and Table 6.3.

First of all, we can see that for $\tau_a = 0$, the probability of false alarm and the probability of detection coincide, which means the total signal is an ideal authentic-like signal. Moreover, the energy used by the spoofer and the energy of the total received signal is pretty similar for all the metrics. From these two facts, it is reasonable to assume that the spoofing signal is almost equal for all the metrics.

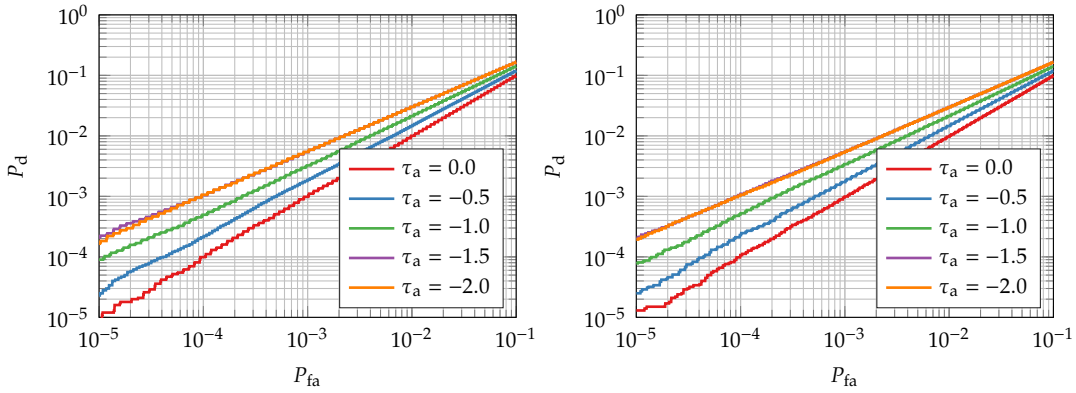
Secondly, we can notice from the ROCs that the performance increases as the relative delay between authentic and spoofing signal increases for all the metrics. In order to explain this behavior, we should recall that the thresholds used by the receiver to detect spoofing are a function of the desired probability of false alarm and of the probability density function of the metric. The metric PDF, in turn, depends on the correlator values which are a function of C/N_0, leading the thresholds to be themselves a function of C/N_0. In particular, as the carrier-to-noise ratio increases, the thresholds narrow toward the authentic metric value, and vice versa.
Now, from Tables 6.2 and 6.3 we can see that, for an increasing $|\tau_a|$ also the total energy grows, leading to a higher C/N_0 and thus to a narrowing of the thresholds. However, as we can see from the example in Fig. 6.2, the correlator values remain in a range corresponding to that of an authentic signal of power less than the actual total signal, but the thresholds are set for an authentic signal with the power of the total signal, and thus with higher correlator values, that is, with a different metric PDF.
Moreover, we can notice that with $\tau_a = -1.5, -2$ for BPSK(1) and with $\tau_a = -1, -1.5, -2$ for BOC(1,1) the performance are pretty the same, and this can be viewed as a sort of saturation of the performance for relative delays between spoofing and authentic signals higher than $|\tau_a| = 2$. This is because, at this point, the authentic signal is no longer contributing to the correlators of the receiver and, therefore, the shape of the spoofing signal can remain constant.

Moreover, in order to compare the results for the various metrics, we can notice that the performance are quite similar. There are only a couple of outliers, one for each constellation.
For the BPSK(1) signal, we can see that the asymmetric late ratio metric reaches the saturation performance already for $\tau_a = -1.5, -2$. This behavior can interpreted noting that the late correlator is in the opposite side of the "direction" of the authentic signal and, therefore, it is no more influenced by the spoofing signal earlier than the other correlators and this affect the performance of the metric, that is mainly based on it.
For what concern the outlier between the BOC(1,1) results, the performance of the double delta metric for $\tau_a = 0$ are unpredictably good. This should be dued to a numerical approximation error in doing the derivatives in a discrete frequency domain and it will have to be handled at best.

Finally, to make a comparison between the BPSK and BOC modulations, we can see that the performance are very similar. The main difference is that the performance of the BOC(1,1) signal saturate at a lower $|\tau_a|$ than the BPSK(1) signal. This can be explained by the fact that the correlators of the BOC(1,1) signal have a smaller spacing between them, and therefore the interference with the authentic signal disappear earlier.

TABLE 6.2: Spoofing and total energy for different authentic code delays (BPSK(1) signal).

E_s | E	Authentic code delay τ_a [chips]				
	0	-0.5	-1	-1.5	-2
DM	0.26 | 2.26	1.51 | 2.51	2.58 | 2.93	2.31 | 3.19	2.26 | 3.26
DDM	0.27 | 2.27	1.55 | 2.51	2.73 | 2.81	2.37 | 3.14	2.28 | 3.27
RM	0.26 | 2.26	1.63 | 2.39	2.72 | 2.77	2.29 | 3.20	2.26 | 3.26
AERM	0.25 | 2.25	1.61 | 2.40	2.82 | 2.67	2.33 | 3.17	2.26 | 3.25
ALRM	0.25 | 2.25	1.56 | 2.46	2.44 | 3.08	2.26 | 3.25	2.26 | 3.25



(A) Delta metric.

(B) Double delta metric.

(C) Ratio metric.

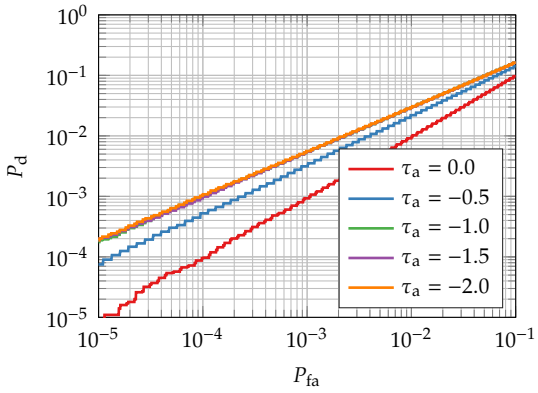
(D) Asymmetric early ratio metric.

(E) Asymmetric late ratio metric.

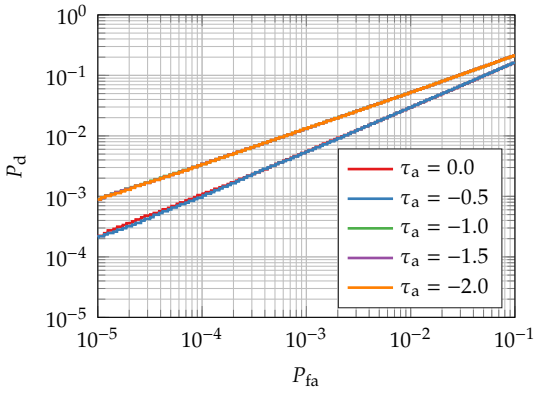
FIGURE 6.3: ROC for different authentic code delays (BPSK(1) signal).

TABLE 6.3: Spoofing and total energy for different authentic code delays (BOC(1,1) signal).

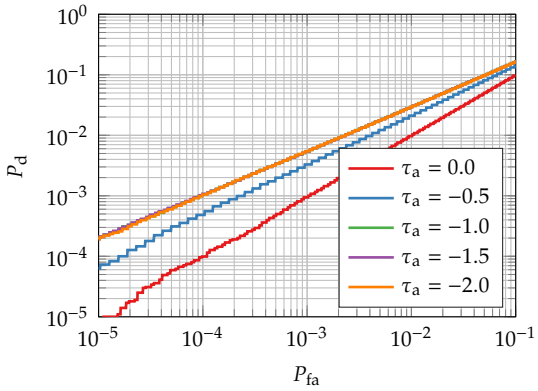
E_s | E	Authentic code delay τ_a [chips]				
	0	-0.5	-1	-1.5	-2
DM	0.28 | 2.28	4.21 | 2.86	2.33 | 3.23	2.28 | 3.28	2.28 | 3.28
DDM	0.99 | 2.99	5.21 | 3.20	3.29 | 3.82	3.08 | 3.98	2.98 | 3.99
RM	0.29 | 2.29	4.27 | 2.79	2.42 | 3.16	2.28 | 3.29	2.28 | 3.29
AERM	0.28 | 2.28	4.22 | 2.83	2.41 | 3.17	2.28 | 3.28	2.28 | 3.28
ALRM	0.28 | 2.28	4.14 | 2.94	2.33 | 3.23	2.28 | 3.28	2.28 | 3.28



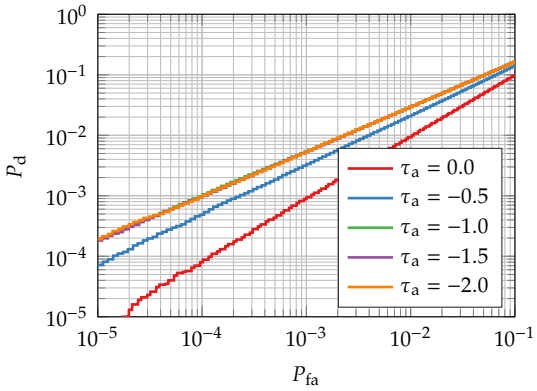
(A) Delta metric.



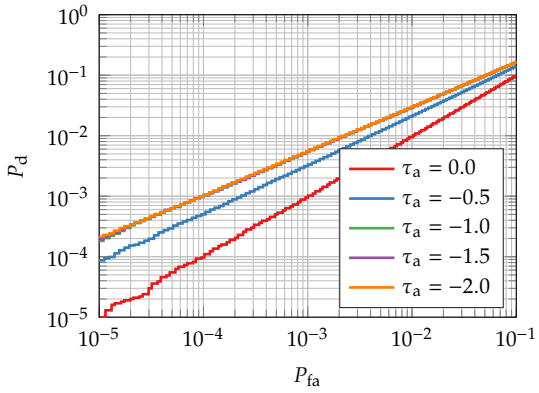
(B) Double delta metric.



(C) Ratio metric.



(D) Asymmetric early ratio metric.



(E) Asymmetric late ratio metric.

FIGURE 6.4: ROC for different authentic code delays (BOC(1,1) signal).

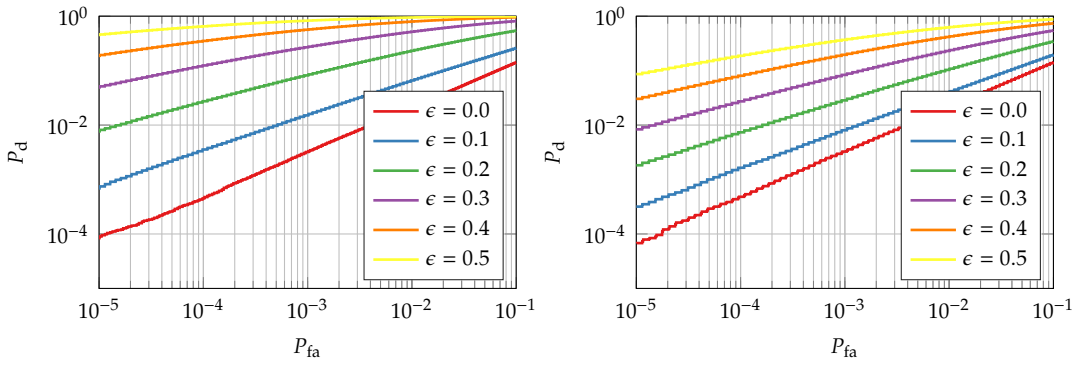
6.2 Comparison between different metric precisions

This Section provides a performance comparison of the SQM metrics between six different metric precisions: $\epsilon = 0, 0.1, 0.2, 0.3, 0.4, 0.5$. The results for the BPSK(1) signal are reported in Fig. 6.5 and Table 6.4. The delta metric and the double delta metric are not present; indeed, the extremes of the range in which the values of the metric should stay are $(1 \pm \epsilon)M_a$ (see Eq. (5.42)), where M_a is the value that the metric assumes when the signal is authentic and it depends on the values assumed by the ACF on the SQM correlators. Therefore, since for the DM and the DDM $M_a = 0$, both the extremes would be equal to M_a, leading to the same result as $\epsilon = 0$.

The main result that stands out from the ROCs is that the all the three metrics gain in performance as ϵ increases because the spoofing signal is using less energy making a compromise on his detectability.

Table 6.4: Spoofing and total energy for different metric precisions (BPSK(1) signal).

E_s | E	Metric precision ϵ					
	0	0.1	0.2	0.3	0.4	0.5
DM	2.72 | 2.77	2.58 | 2.93	2.58 | 2.93	2.58 | 2.93	2.58 | 2.93	2.58 | 2.93
DDM	2.58 | 2.93	2.73 | 2.81	2.73 | 2.81	2.73 | 2.81	2.73 | 2.81	2.73 | 2.81
RM	2.72 | 2.77	2.65 | 2.78	2.59 | 2.80	2.54 | 2.84	2.51 | 2.88	2.48 | 2.94
AERM	2.48 | 2.94	2.75 | 2.68	2.69 | 2.69	2.93 | 2.71	2.58 | 2.74	2.54 | 2.78
ALRM	2.54 | 2.78	2.41 | 3.09	2.40 | 3.10	2.39 | 3.13	2.39 | 3.13	2.39 | 3.13



(A) Ratio metric.

(B) Asymmetric early ratio metric.

(C) Asymmetric late ratio metric.

Figure 6.5: ROC for different metric precisions (BPSK(1) signal).

Table 6.5: Spoofing and total energy with unknown authentic phase (BPSK(1) signal).

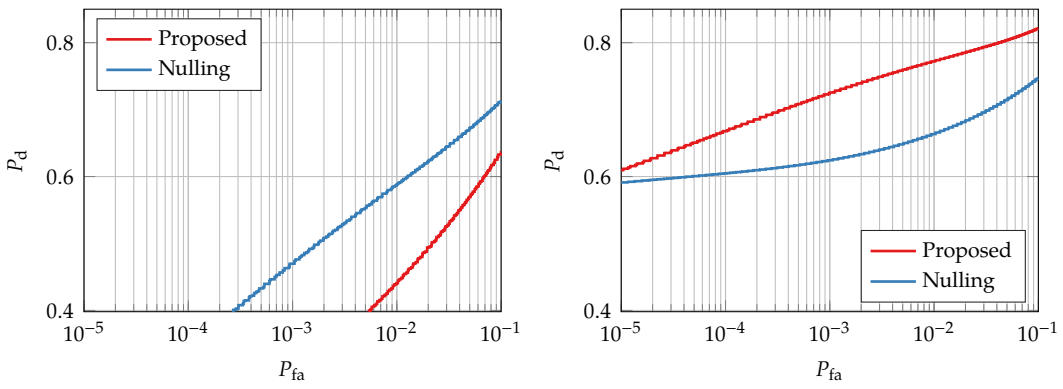
$\bar{E}_s$ | $\bar{E}$	Optimal	Nulling
DM	2.58 | 3.58	
DDM	2.73 | 3.73	
RM	2.74 | 3.75	3.25 | 4.25
AERM	2.42 | 3.41	
ALRM	2.84 | 3.86	

6.3 Comparison between nulling and optimal attack with unknown authentic phase

This Section provides a performance comparison of the SQM metrics between nulling and the proposed attack with unknown authentic phase. In order to evaluate the performance for this scenario, the two attacks have been performed for $\tilde{\phi}_a = 0, \pi/4, \pi/2, 3\pi/4, \pi$ (the three remaining angles to complete the trigonometric circle are not considered due to symmetry) and then the mean of the probability of detection and of the energies has been taken. A dense angular sampling was not considered, to save computational time. The results for the BPSK(1) signal are reported in Fig. 6.7 and Table 6.5.

First of all, we can notice that in this scenario the performance of the SQM metrics increases drastically, as expected. Indeed, not knowing the authentic phase is a realistic as much as a dramatic disadvantage for the attacker, because this means that he must try a random phase.
Another thing that stands out is that the performance are quite different for the various metrics, at least lingering over the shape of the curves. Actually, the only metric which differs substantially to the worse from the others is the delta metric.

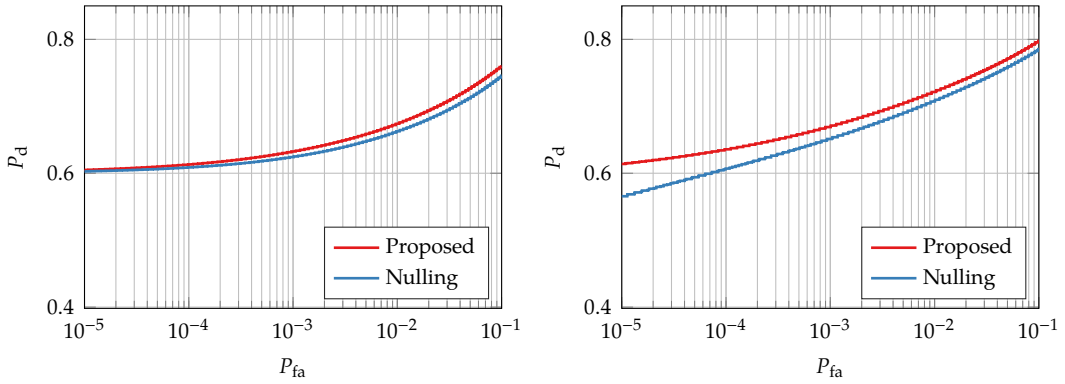
Secondly, to make a comparison between optimal and nulling attacks, we can see that in three of five cases (double delta, ratio and asymmetric early ratio metrics) the nulling one performs better, in one case (delta metric) the optimal does better and in the last case (asymmetric late ratio metric) they split the victory. However, in all the cases the optimal attack utilizes less energy.



(a) Delta metric.

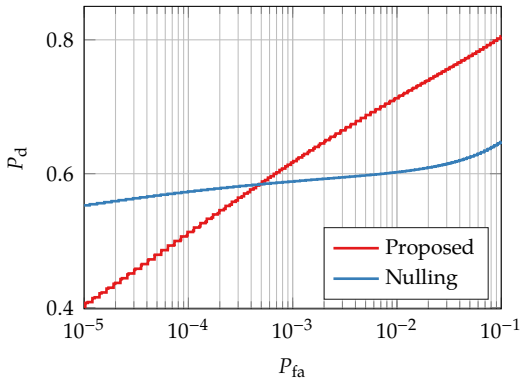
(b) Double delta metric.

Figure 6.6: ROC with unknown authentic phase (BPSK(1) signal) (continued).



(A) Ratio metric.

(B) Asymmetric early ratio metric.



(C) Asymmetric late ratio metric.

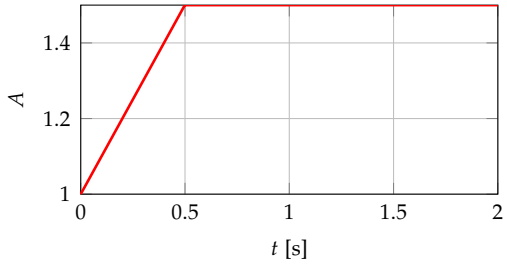
FIGURE 6.7: ROC with unknown authentic phase (BPSK(1) signal) (continued).

6.4 Simulation of a lift-off-aligned attack

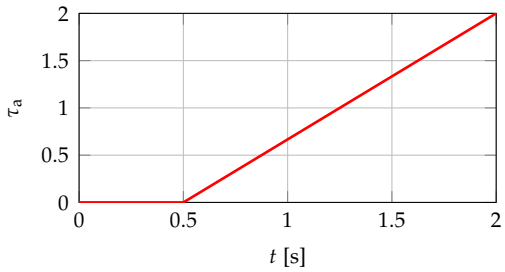
This final Section attempts to give the reader an idea of how a lift-off-aligned attack is performed, without any pretense to be a realistic simulation. In this context, the evolution of the prompt correlator value A and of the authentic code delay τ_a is represented in Fig. 6.8 as a function of time. Moreover, it has to be specified that a metric precision of $\epsilon = 0.1$ has been used in order to give a little more freedom to the attacker to see what will be his behavior. Finally, a probability of false alarm $P_{fa} = 10^{-2}$ has been set. The resulting attack is reported in Fig. 6.9.

First being all, from the evolution of A and τ_a we can deduce that the spoofer starts his attack aligned to the victim, while he is increasing the prompt correlator value. Then, at a certain point A stabilize to a constant value while the lift-off phase begins, with the spoofing signal moving away from the authentic signal.

As a second step, we can analyze the metrics' evolution. We can notice that the thresholds change as the attack moves on, allowing us to realize that the C/N_0 also changes. Moreover, some metric has some variations of his mean value, which signify that the attacker is taking advantage of the degrees of liberty given by the metric precision. Finally, given that the attack is composed by 2000 time steps, we can see that the empirical values of the metrics go beyond the thresholds with a probability very similar (a little worse, as expected) to the fixed $P_{fa} = 10^{-2}$.

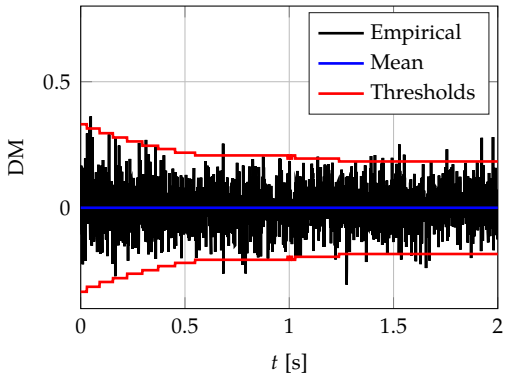


(A) Prompt correlator value.

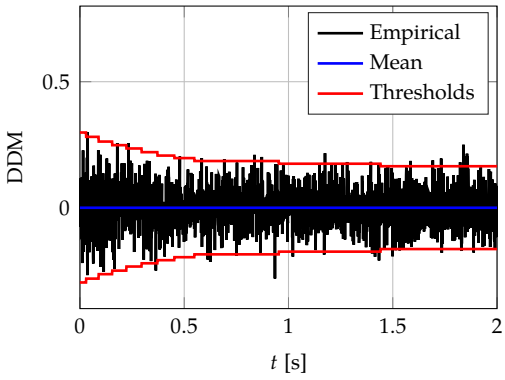


(B) Authentic code delay value.

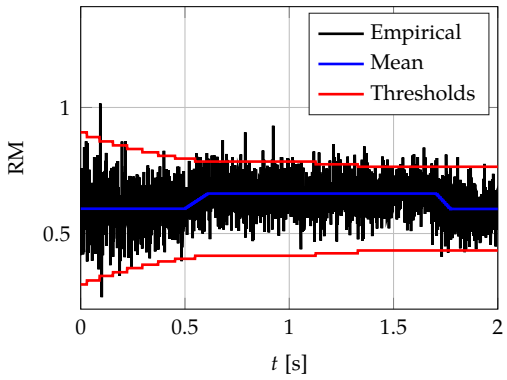
FIGURE 6.8: Evolution of the amplitude of the prompt correlator and the authentic code delay for the lift-off-aligned attack.



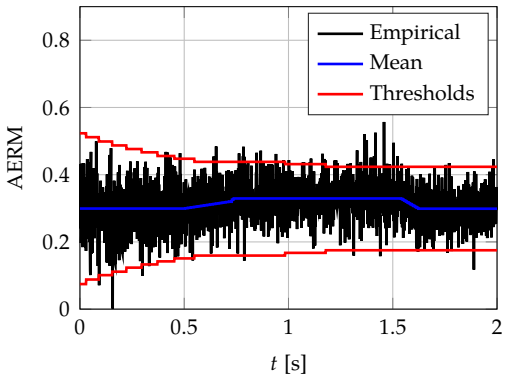
(A) Delta metric.



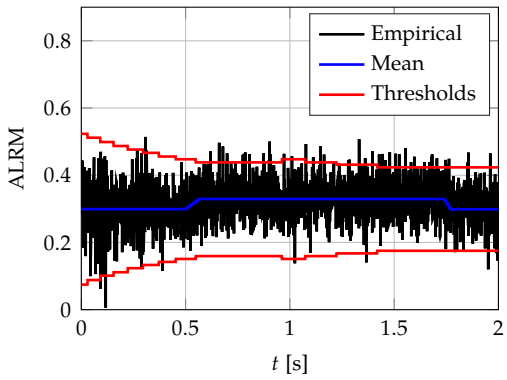
(B) Double delta metric.



(C) Ratio metric.



(D) Asymmetric early ratio metric.



(E) Asymmetric late ratio metric.

FIGURE 6.9: Simulation of a lift-off-aligned attack (BPSK(1) signal) (continued).

Chapter 7

Conclusions and Future Work

Spoofing attack on GNSS receivers has been considered as a serious threat to safety of life applications; since there is enough motivation for illicit application of spoofers, the realization of spoofers is not prohibitively costly. As such, it is anticipated that many research activities will be conducted on increasing the security of GNSS receivers against spoofing and jamming attacks.
In this Thesis different spoofing/anti-spoofing scenarios were described and the vulnerabilities of GNSS that can potentially be exploited by a spoofer were discussed. Moreover, an optimal attack against the anti-spoofing SQM techniques has been proposed; in particular, a mathematical model has been developed in order to derive the spoofing signal that the spoofer has to transmit to the victim to take the control of his receiver. We have seen that the proposed algorithm generate a spoofing signal that passes the SQM defence with low probability of detection; indeed, it satisfies three main constraints: the DLL correlator outputs of the total signal received by the victim are at the same height, leading to a smooth tracking process; the SMQ correlator outputs of the total received signal are such that the value of the SQM metrics is authentic-like; finally, the slope around all the correlator outputs is similar to that of an authentic signal, providing robustness against minor code delay misalignments. Finally, the security evaluations of the SQM techniques against the proposed attack has been provided, showing that the total received signal is reported as a spoofed signal with a probability of detection not much higher than the probability of false alarm set by the receiver for an authentic signal. In particular, the only thing that helps the receiver to realize that a spoofing attack is going on is that C/N_0 is high in relation to the value of the correlator outputs. However, we have also seen that, if the attacker does not know the phase of th authentic signal, the security performance of the SQM techniques increases drastically, as expected for such a scenario.

For what concern the future work, the SQM defense and the proposed attack should be implemented on a realistic testbed in order to understand if the performance evaluated in simulation will be confirmed.
Secondly, an improvement of the SQM techniques should be considered. In particular, the detection mechanism should be developed as a composite hyphotesis test, such as the GLRT, that permits to consider a wide class of attacks in the calculation of the detection thresholds. Another possibility should be to combine more than one metric in the statistical test, with a view to leave the attacker with less degrees of freedom in choosing the structure of the spoofing signal.
Moreover, it should be resolved the main limitation of the SQM techniques, that is, they are actually not able to discriminate between spoofing and multipath; indeed, both signals generates similar effects on the correlator outputs. One possibility is to leverage the fact that the multipath components generally have smaller amplitude that the authentic signal from which they are generated and that they are always late with respect to it. Specifically, a composite hypothesis test should be realized in

which there are multiple alternate hypothesizes: spoofing, multipath and spoofing together with multipath.
Finally, the SQM techniques should be combined with different anti-spoofing that works on other blocks of the receiver in order to provide security on more levels, that is, in a multilayer perspective.

Appendix A

Relation between C/N_0 and pre-correlation noise power

At the output of the front-end, a complex GNSS signal for a single satellite can be modeled as

$$r(k;\tau,\phi,f_{\mathrm{D}},A) = AD(kT_{\mathrm{s}}-\tau)C(kT_{\mathrm{s}}-\tau)\mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}}+f_{\mathrm{D}})kT_{\mathrm{s}}+\phi\right]} + n(kT_{\mathrm{s}}) \ , \tag{A.1}$$

where T_{s} is the sampling time interval and f_{IF} is the intermediate frequency (IF) at which the signal is down-converted by the front end. Moreover, D is the navigation data symbol sequence, C is the spreading code sequence with a chip duration of T_{c} and n is the noise. Finally, A is the signal amplitude, τ is the code delay, f_{D} is the carrier Doppler frequency shift and ϕ is the carrier-phase delay. For the sake of simplicity, the dependency of the various functions on τ, ϕ, f_{D} and A will be dropped. The noise term, called thermal noise, is induced by the antenna and the front-end themselves and it is assumed to be and additive white Gaussian noise (AWGN) [39]. Therefore, each sample can be modeled as a complex Gaussian random variable

$$n \sim \mathcal{CN}\left(0,\sigma_n^2\right) \ , \tag{A.2}$$

with zero mean and variance σ_n^2 and it is independent and identically distribute w.r.t the other samples.
The navigation data symbols D can be written in Cartesian form as $D = D_{\mathrm{I}} + jD_{\mathrm{Q}}$, where D_{I} and D_{Q} are the in-phase and quadrature components, respectively. Similarly, the noise can be written in its baseband representation, that is $n = n_{\mathrm{I}} + jn_{\mathrm{Q}}$, where each component is a Gaussian random variable with zero mean and variance

$$\sigma_{n_{\mathrm{I}}}^2 = \sigma_{n_{\mathrm{Q}}}^2 = \frac{\sigma_n^2}{2} \ . \tag{A.3}$$

Using the notation with baseband components, the signal in Eq. (A.1) can be written as

$$r(k) = A(D_{\mathrm{I}}(k) + jD_{\mathrm{Q}}(k))C(k)\mathrm{e}^{j\theta(k)} + n_{\mathrm{I}}(k) + jn_{\mathrm{Q}}(k) \ , \tag{A.4}$$

where $\theta(k) = 2\pi(f_{\mathrm{IF}}+f_{\mathrm{D}})kT_{\mathrm{s}}+\phi$. This results in the following in-phase and quadrature branches:

$$r_{\mathrm{I}}(k) = AD_{\mathrm{I}}(k)C(k)\cos(\theta(k)) - AD_{\mathrm{Q}}(k)C(k)\sin(\theta(k)) + n_{\mathrm{I}}(k) \ , \tag{A.5}$$

$$r_{\mathrm{Q}}(k) = AD_{\mathrm{I}}(k)C(k)\sin(\theta(k)) + AD_{\mathrm{Q}}(k)C(k)\cos(\theta(k)) + n_{\mathrm{Q}}(k) \ . \tag{A.6}$$

The power of the baseband signals D_{I} and D_{Q} multiplied by the spreading code C is equal to 1 because they are based on binary waveforms of amplitude ±1. Therefore,

the power of an I/Q component of the useful signal is [39]

$$P_{D_\mathrm{I}} = P_{D_\mathrm{Q}} = \frac{A^2}{2} \,, \tag{A.7}$$

leading to a total power per branch of

$$P_{r_\mathrm{I}} = P_{r_\mathrm{Q}} = P_{D_\mathrm{I}} + P_{D_\mathrm{Q}} = A^2 \,. \tag{A.8}$$

On the other hand, the noise power is [39]

$$\sigma_n^2 = N_0 B_\mathrm{s} = N_0 \frac{1}{T_\mathrm{s}} \,, \tag{A.9}$$

where N_0 is the noise power density and B_s is the bandwidth of the signal at the front-end output.
From Eqs. (A.7) and (A.9), the relation between C/N_0 and the complex noise power is given by

$$C/N_0 = \frac{P_{r_\mathrm{I}}}{N_0} = \frac{A^2}{\sigma_n^2 T_\mathrm{s}} = \frac{A^2}{2\sigma_{n_I}^2 T_\mathrm{s}} \,. \tag{A.10}$$

Obviously, if the received signal has only the in-phase component D_I, the power to be used in the above formula is P_I, resulting in $C/N_0 = A^2/(2\sigma_n^2 T_\mathrm{s})$.
Finally, in order to derive the relation of the noise power with the SNR at the output of the front-end, it is sufficient to divide C/N_0 by the bandwidth of the signal B_s.

Appendix B

Statistics of the correlator output

The correlator output whose delay is α chips from the prompt one can be written as

$$S_\alpha = ADR(\Delta\tau + \alpha)\,\mathrm{sinc}\,(\Delta f_\mathrm{D} T_\mathrm{coh})\mathrm{e}^{j\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right)} + \eta_\alpha \tag{B.1}$$

where $\Delta\tau = \tau - \hat{\tau}$ is the code delay error, $\Delta\phi = \phi - \hat{\phi}$ is the carrier phase error and $\Delta f_\mathrm{D} = f_\mathrm{D} - \hat{f}_\mathrm{D}$ is the Doppler error. Moreover, $R(\Delta\tau)$ is the ACF of $C(kT_\mathrm{s})$ at lag $\Delta\tau$ and η_α is the noise after the correlation operation. In Eq. (B.1) the sinc function is defined as $\mathrm{sinc}(x) = \sin(\pi x)/(\pi x)$.
The noise can be modeled as a complex Gaussian random variable

$$\eta_\alpha \sim \mathcal{CN}\left(0, \sigma^2_{\eta_\alpha}\right)\,, \tag{B.2}$$

with zero mean and variance $\sigma^2_{\eta_\alpha}$ and it is independent and identically distribute w.r.t the other samples.
The navigation data symbols D can be written in Cartesian form as $D = D_\mathrm{I} + jD_\mathrm{Q}$, where D_I and D_Q are the in-phase and quadrature components, respectively. Similarly, the noise can be written in its baseband representation, that is $\eta_\alpha = \eta_{I_\alpha} + j\eta_{Q_\alpha}$, where each component is a Gaussian random variable with zero mean and variance

$$\sigma^2_{\eta_{I_\alpha}} = \sigma^2_{\eta_{Q_\alpha}} = \frac{\sigma^2_{\eta_\alpha}}{2}\,. \tag{B.3}$$

Using the notation with baseband components, the signal in Eq. (B.1) can be written as

$$S_\alpha = A(D_\mathrm{I}(k) + jD_\mathrm{Q}(k))R(\Delta\tau + \alpha)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh})\mathrm{e}^{j\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right)} + \eta_{I_\alpha} + j\eta_{Q_\alpha}\,, \tag{B.4}$$

Therefore, the in-phase and quadrature components of the CAF are given by

$$\begin{aligned} I_\alpha = {} & AD_\mathrm{I}R(\Delta\tau + \alpha)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh})\cos\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right) \\ & - AD_\mathrm{Q}R(\Delta\tau + \alpha)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh})\sin\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right) + \eta_{I_\alpha}\,, \end{aligned} \tag{B.5}$$

$$\begin{aligned} Q_\alpha = {} & AD_\mathrm{I}R(\Delta\tau + \alpha)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh})\sin\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right) \\ & + AD_\mathrm{Q}R(\Delta\tau + \alpha)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh})\cos\left(\Delta\phi + \pi\Delta f_\mathrm{D} T_\mathrm{coh}\right) + \eta_{Q_\alpha}\,. \end{aligned} \tag{B.6}$$

Assuming a perfect synchronization between the receiver and the received signal, the I/Q components becomes

$$I_\alpha = AD_\mathrm{I}R(\alpha) + \eta_{I_\alpha}\,, \tag{B.7}$$

$$Q_\alpha = AD_\mathrm{Q}R(\alpha) + \eta_{Q_\alpha}\,. \tag{B.8}$$

The post-correlation noise η_α referred to a correlator of delay α can be written as a function of the pre-correlation noise n, that is

$$\begin{aligned}\eta_\alpha &= \frac{1}{M}\sum_{k=1}^{M} n(k)\hat{r}_\alpha^*(k) \\ &= \frac{1}{M}\sum_{k=1}^{M} n(k)C^*(kT_\mathrm{s}-\hat{\tau}_\alpha)\mathrm{e}^{-j\left[2\pi(f_\mathrm{IF}+\hat{f}_\mathrm{D})kT_\mathrm{s}+\hat{\phi}\right]}\end{aligned} \tag{B.9}$$

and so its two components can be written as

$$\eta_{I_\alpha} = \frac{1}{M}\sum_{k=1}^{M}\left[n_\mathrm{I}(k)\cos\left(\hat{\theta}(k)\right)+n_\mathrm{Q}(k)\sin\left(\hat{\theta}(k)\right)\right]C^*(kT_\mathrm{s}-\hat{\tau}_\alpha)\,, \tag{B.10}$$

$$\eta_{Q_\alpha} = \frac{1}{M}\sum_{k=1}^{M}\left[n_\mathrm{I}(k)\sin\left(\hat{\theta}(k)\right)-n_\mathrm{Q}(k)\cos\left(\hat{\theta}(k)\right)\right]C^*(kT_\mathrm{s}-\hat{\tau}_\alpha)\,, \tag{B.11}$$

The expected value of the I/Q components of a correlator output with delay α is

$$\mu_{I_\alpha} = \mathbb{E}\left[I_\alpha\right] = \mathbb{E}\left[AD_\mathrm{I}R(\alpha)+\eta_{I_\alpha}\right] = AD_\mathrm{I}R(\alpha)\,, \tag{B.12}$$

$$\mu_{Q_\alpha} = \mathbb{E}\left[Q_\alpha\right] = \mathbb{E}\left[AD_\mathrm{Q}R(\alpha)+\eta_{Q_\alpha}\right] = AD_\mathrm{Q}R(\alpha)\,. \tag{B.13}$$

The covariance between two I/Q correlators of delay α_i and α_j is

$$\begin{aligned}\sigma^2_{I_{\alpha_i},I_{\alpha_j}} &= \mathbb{E}\left[\left(I_{\alpha_i}-\mu_{I_{\alpha_i}}\right)\left(I_{\alpha_j}-\mu_{I_{\alpha_j}}\right)\right] \\ &= \mathbb{E}\left[\eta_{I_{\alpha_i}}\eta_{I_{\alpha_j}}\right] \\ &= \mathbb{E}\left[\left(\frac{1}{M}\sum_{k=1}^{M}\left[n_\mathrm{I}(k)\cos\left(\hat{\theta}(k)\right)+n_\mathrm{Q}(k)\sin\left(\hat{\theta}(k)\right)\right]C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_i})\right)\right. \\ &\quad\left.\cdot\left(\frac{1}{M}\sum_{k=1}^{M}\left[n_\mathrm{I}(k)\cos\left(\hat{\theta}(k)\right)+n_\mathrm{Q}(k)\sin\left(\hat{\theta}(k)\right)\right]C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_j})\right)\right] \\ &= \mathbb{E}\left[\frac{1}{M^2}\sum_{k=1}^{M}\left[n_\mathrm{I}(k)\cos\left(\hat{\theta}(k)\right)+n_\mathrm{Q}(k)\sin\left(\hat{\theta}(k)\right)\right]^2 C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_i})C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_j})\right] \\ &= \frac{1}{M^2}\sum_{k=1}^{M}\left[\mathbb{E}\left[n_\mathrm{I}^2(k)\right]\cos^2\left(\hat{\theta}(k)\right)+\mathbb{E}\left[n_\mathrm{Q}^2(k)\right]\sin^2\left(\hat{\theta}(k)\right)\right]C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_i})C^*(kT_\mathrm{s}-\hat{\tau}_{\alpha_j}) \\ &= \frac{1}{M^2}\sigma^2_{n_\mathrm{I}}MR(\left|\alpha_i-\alpha_j\right|) \\ &= \frac{\sigma^2_{n_\mathrm{I}}}{M}R(\left|\alpha_i-\alpha_j\right|)\,,\end{aligned} \tag{B.14}$$

$$\sigma^2_{Q_{\alpha_i},Q_{\alpha_j}} = \frac{\sigma^2_{n_\mathrm{Q}}}{M}R(\left|\alpha_i-\alpha_j\right|)\,, \tag{B.15}$$

where it has been exploited the fact that the noise samples are i.i.d. The covariance between an in-phase correlator of delay α_i and a quadrature correlator of delay α_j is

$$\begin{aligned}
\sigma^2_{I_{\alpha_i},Q_{\alpha_j}} &= \mathbb{E}\left[\left(I_{\alpha_i} - \mu_{I_{\alpha_i}}\right)\left(Q_{\alpha_j} - \mu_{Q_{\alpha_j}}\right)\right] \\
&= \mathbb{E}\left[\eta_{I_{\alpha_i}}\eta_{Q_{\alpha_j}}\right] \\
&= \mathbb{E}\left[\left(\frac{1}{M}\sum_{k=1}^{M}\left[n_{\mathrm{I}}(k)\cos\left(\hat{\theta}(k)\right) + n_{\mathrm{Q}}(k)\sin\left(\hat{\theta}(k)\right)\right]C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_i})\right)\right. \\
&\quad \left.\cdot\left(\frac{1}{M}\sum_{k=1}^{M}\left[n_{\mathrm{I}}(k)\sin\left(\hat{\theta}(k)\right) - n_{\mathrm{Q}}(k)\cos\left(\hat{\theta}(k)\right)\right]C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_j})\right)\right] \\
&= \frac{1}{M^2}\sum_{k=1}^{M}\left[\mathbb{E}\left[n_{\mathrm{I}}^2(k)\right]\cos\left(\hat{\theta}(k)\right)\sin\left(\hat{\theta}(k)\right) - \mathbb{E}\left[n_{\mathrm{Q}}^2(k)\right]\sin\left(\hat{\theta}(k)\right)\cos\left(\hat{\theta}(k)\right)\right] \\
&\quad \cdot C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_i})C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_j}) \\
&= \frac{1}{M^2}\sum_{k=1}^{M}\left[\mathbb{E}\left[n_{\mathrm{I}}^2(k)\right] - \mathbb{E}\left[n_{\mathrm{Q}}^2(k)\right]\right]\cos\left(\hat{\theta}(k)\right)\sin\left(\hat{\theta}(k)\right) \\
&\quad \cdot C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_i})C^*(kT_{\mathrm{s}} - \hat{\tau}_{\alpha_j}) \\
&= 0\,, \qquad \text{(B.16)} \\
\sigma^2_{Q_{\alpha_i},Q_{\alpha_j}} &= 0\,, \qquad \text{(B.17)}
\end{aligned}$$

Finally, this Thesis assumes real navigation data symbols, that is $D = D_{\mathrm{I}}$, permitting us to consider only the in-phase components of the CAF in the above calculations.

Appendix C

Relation between C/N_0 and post-correlation noise power

Starting from Eqs. (B.7) and (B.8), the power of the baseband signals D_{I} and D_{Q} is equal to 1 because they are based on binary waveforms of amplitude ±1. Therefore, the power of an I/Q component of the useful signal is

$$P_{I_\alpha} = P_{Q_\alpha} = A^2 R^2(\alpha) \, . \tag{C.1}$$

On the other hand, the noise power is

$$\sigma_n^2 = N_0 B_{\mathrm{coh}} = N_0 \frac{1}{T_{\mathrm{coh}}} \, , \tag{C.2}$$

where N_0 is the noise power density and B_{coh} is the bandwidth of the signal at the correlator output.
From Eqs. (C.1) and (C.2), the relation between C/N_0 and the complex noise power is given by

$$C/N_0 = \frac{P_{I_\alpha}}{N_0} = \frac{A^2 R^2(\alpha)}{\sigma_\eta^2 T_{\mathrm{coh}}} = \frac{A^2 R^2(\alpha)}{2\sigma_{\eta_I}^2 T_{\mathrm{coh}}} \, . \tag{C.3}$$

Finally, in order to derive the relation of the noise power with the SNR at the output of the front-end, it is sufficient to divide C/N_0 by the bandwidth of the signal B_{coh}.

Bibliography

[1] B. Motella, M. Pini, and F. Dovis, "Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers", *GPS Solutions*, vol. 12, no. 2, pp. 77–86, 2008.

[2] D. Shepard, "Characterization of receiver response to spoofing attacks", PhD thesis, 2011.

[3] F. Dovis, *GNSS Interference Threats and Countermeasures*. Artech House, 2015.

[4] A. Grant and P. Williams, "Gnss solutions: What is the effect of gps jamming on maritime safety", *Inside GNSS*, vol. 4, no. 1, 2009.

[5] M. Wildemeersch, E. C. Pons, A. Rabbachin, and J. F. Guasch, "Impact study of unintentional interference on gnss receivers", *EC Joint Research Centre Scientific and Technical Reports, Institute for the Protection and Security of the Citizen, European Union*, 2010.

[6] M. Pini, B. Motella, L. Pilos, L. Vesterlund, D. Blanco, F. Lindstrom, and C. Maltoni, "Robust on-board ship equipment: The triton project", in *Proceedings of the 10th International Symposium Information on Ships, Hamburg, Germany*, vol. 190, 2014.

[7] U. News. (2013). Ut austin researchers successfully spoof an $80 million yacht at sea, [Online]. Available: `https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea` (visited on 07/03/2018).

[8] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable gps civilian spoofer", in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[9] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer", in *Proceedings of the ION International Technical Meeting*, 2009, pp. 124–130.

[10] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques", *International Journal of Navigation and Observation*, vol. 2012, 2012.

[11] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems", in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, 2001, pp. 1543–1552.

[12] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for gps signal spoofing", in *ION GNSS*, vol. 5, 2005, pp. 13–16.

[13] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil gps anti-spoofing", in *Proceedings of the ION GNSS Meeting*, 2011.

[14] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil gps receivers", in *Proceedings of the 2010 international technical meeting of the Institute of Navigation*, 2001, pp. 698–712.

[15] J. S. Subirana, J. J. Zornoza, and M. Hernàndez-Pajares, "Gnss data processing. volume 1: Fundamentals and algorithms", *ESA Communications ESTEC, PO Box*, vol. 299, 2013.

[16] P. Teunissen and O. Montenbruck, *Springer handbook of global navigation satellite systems*. Springer, 2017.

[17] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media, 2007.

[18] J. M. Samper, J. M. Lagunilla, and R. B. Perez, *GPS and Galileo: Dual RF Front-end receiver and Design, Fabrication, And Test (Communication Engineering)*. McGraw-Hill Professional, 2008.

[19] E. Garbin Manfredini, "Signal processing techniques for gnss anti-spoofing algorithms", PhD thesis, Politecnico di Torino, 2017.

[20] C. Günther, "A survey of spoofing and counter-measures", *Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

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

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

[23] T. E. Humphreys, "Detection strategy for cryptographic gnss anti-spoofing", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[24] J. T. Curran and C. O'Driscoll, "Message authentication as an anti-spoofing mechanism", Working Paper, June, Tech. Rep., 2017.

[25] D. M. Akos, "Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc)", *Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[26] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for gps l1 c/a signals", *Navigation*, vol. 61, no. 1, pp. 1–11, 2014.

[27] M. L. Psiaki, B. W. O'hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, "Gnss spoofing detection using two-antenna differential carrier phase", 2014.

[28] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver", *GPS world*, vol. 21, no. 9, pp. 27–33, 2010.

[29] M. L. Psiaki, S. P. Powell, and B. W. O'hanlon, "Gnss spoofing detection using high-frequency antenna motion and carrier-phase data", in *Proceedings of the ION GNSS+ Meeting*, 2013, pp. 2949–2991.

[30] K. Ali, X. Chen, and F. Dovis, "On the use of multipath estimating architecture for spoofer detection", in *Localization and GNSS (ICL-GNSS), 2012 International Conference on*, IEEE, 2012, pp. 1–6.

[31] J. M. Parro-Jimènez, J. A. Lòpez-Salcedo, R. T. Ioannides, and M. Crisci, "Frequency-domain code replica detection for a gnss receiver", in *Localization and GNSS (ICL-GNSS), 2013 International Conference on*, IEEE, 2013, pp. 1–6.

[32] C. E. McDowell, *Gps spoofer and repeater mitigation system using digital spatial nulling*, US Patent 7,250,903, 2007.

[33] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity gps anti-spoofing method using a multi-antenna array", *a a*, vol. 2, p. 2, 2012.

[34] S. Fantinato, G. Gamba, M. Anghileri, R. Ioannides, O. Pozzobon, and J. A. Rodriguez, "The spoofing estimating delay lock loop", in *Proc. 7th ESA Workshop Satellite Navig. Technol. Eur. Workshop on GNSS Signals Signal Processing,(NAVITEC)*, 2014.

[35] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (sdcc) receiver architecture for a moving gnss receiver", *GPS Solutions*, vol. 19, no. 3, pp. 475–487, 2015.

[36] A. Jafarnia-Jahromi, A. Broumandan, S. Daneshmand, G. Lachapelle, and R. T. Ioannides, "Galileo signal authenticity verification using signal quality monitoring methods", in *Proceedings of the IEEE International Conference on Localization and GNSS (ICL-GNSS 2016), Barcelona, Spain*, 2016, pp. 28–30.

[37] J. Jones, P. Fenton, B. Smith, *et al.*, "Theory and performance of the pulse aperture correlator", in *Proceedings of ION GPS*, vol. 2004, 2004.

[38] O. M. Mubarak and A. G. Dempster, "Analysis of early late phase in single-and dual-frequency gps receivers for multipath detection", *GPS solutions*, vol. 14, no. 4, pp. 381–388, 2010.

[39] J. Leclère, R. J. Landry, and C. Botteron, "How does one compute the noise power to simulate real and complex gnss signals?", Tech. Rep., 2016.