Università degli Studi di Padova

Department of Information Engineering

Ph.D. Course in Information Engineering

Science and Information Technology Curriculum

XXXIV Cycle

Signal Processing Techniques for the Protection of GNSS Signals and URLLC Networks

Coordinator
Prof. Andrea Neviani

Supervisor
Prof. Nicola Laurenti
Università degli Studi di Padova

Co-supervisor
Dr. Paolo Baracca
Nokia Bell Labs Stuttgart

Ph.D. Candidate
Leonardo Chiarello

Academic Year 2020/2021

"*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

Signal Processing Techniques for the Protection of GNSS Signals and URLLC Networks

Wireless communications have evolved rapidly during the last 20 years. Nowadays, not only people communicate with each other, but also people communicate with machines and also machines communicate with each other. In order to support these intense demands, research should develop innovative technologies, investigate their potential vulnerabilities and study tailored countermeasures. In this context, the aim of this Thesis is the proposal of signal processing techniques for the protection of global navigation satellite system (GNSS) signals and mobile networks, with particular focus to ultra-reliable low-latency communications (URLLC).

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, anti-spoofing and anti-jamming algorithms have become an important research topic within the GNSS discipline. As a first contribution, this Thesis provides the performance evaluation of i) signal quality monitoring (SQM) techniques for anti-spoofing and ii) an adaptive notch filter for anti-jamming, both implemented in a security-oriented GNSS software package. Then, the problem of detecting spoofing attacks for a GNSS receiver in space orbiting around the Earth is considered and a solution via fusion of consistency metrics is proposed.

Security has been one of the main drivers also in the design of the fifth generation (5G) of mobile communication systems by the 3rd Generation Partnership Project (3GPP), however with focus only at high layers to guarantee authentication, privacy and data integrity. On the other hand, jamming attacks for denial of service are a rising threat which can severely compromise the system performance, in particular in Industry 4.0 scenarios. This Thesis proposes a defense mechanism based on pseudo-random blanking of subcarriers with orthogonal frequency division multiplexing (OFDM) and designs a detector by applying the generalized likelihood ratio test (GLRT) on those subcarriers. The performance are evaluated against a smart jammer in single-cell single-user uplink scenario with additive white Gaussian noise (AWGN) and Rayleigh channel models. Then, this work is extended to investigate the problem of jamming detection and mitigation in a more realistic indoor factory deployment, where also a jamming mitigation with frequency hopping and random scheduling of user equipments (UEs) is proposed.

Acknowledgements

This Thesis was carried out at the Department of Information Engineering of the University of Padova from 2018 to 2021. Throughout the writing of this Thesis I have received a great deal of support and assistance.

First and foremost, I would like to thank my supervisor, Prof. Nicola Laurenti, whose expertise was invaluable in formulating the research questions and methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I would also like to extend my deepest gratitude to the GNSS research group at the University of Padova for the constructive collaboration and the valuable discussions. In particular, I thank Francesco Formaggio for all the work- and life-related advices, Silvia Ceccato for being my mentor, Francesco Ardizzon for the discussions on movies and workouts, Marco Ceccato for our so-called "Mobike project", Anna Poltronieri for all the jokes while being desk neighbours, Anna Valeria Guglielmi for being my ENSPACE project buddy, Prof. Stefano Tomasin for all the stimulating discussions, and Gianluca Caparra for the great collaboration in the MORE GOSSIP project.

I am also grateful to my colleagues from my internship at Nokia Bell Labs in Stuttgart for their wonderful collaboration. I would particularly like to single out my supervisor, Dr. Paolo Baracca, also being co-supervisor of my Ph.D. studies, for his patient support and for all of the opportunities I was given to further my research. A special thanks goes also to my collegues and friends Silvio M., Alessandro L., Marcus H., Fabiano L., Youri R., Mahmoud R., and Vladislav N.; it is their kind help and support that have made my study and life in Stuttgart a wonderful time.

I also wish to thank all my Ph.D. colleagues and friends which I met in the DEI's laboratories during these years: Alberto S., Alessandro B., Caterina R., Chiara P., Daniel Z., Danilo R., Davide M., Elvina G., Fabio C., Federico C., Federico M., Federico V., Felipe G. C., Francesco P., Gianluca A., Giulia C., Giulia M., Marco G., Martina C., Matteo D., Mattia L., Michele P., Paolo S., Paolo T., Sebastiano V., Thomas M., Tommaso Z., and Umberto M. With them I shared moments of deep anxiety but also of big excitement. I remember with particular pleasure the lunch times at Mensa Forcellini, the coffee and tea breaks spent at playing to the hangman game or to Live Quiz, and the drinks after work, especially during the University Wednesdays.

It is a pleasure to thank my friends of the Angolo Nerd, Marco, Riccardo, and Davide, for the wonderful times we shared, especially the Saturday night dinners discussing about technology and the evenings spent playing videogames, which gave me the necessary distractions from my research. In addition, I would like to thank my friends Luca and Giada for the many times we have been to the cinema together, without missing any movies from the Marvel Cinematic Universe.

Finally, my deep and sincere gratitude to my family for their continuous and unparalleled love, help and support. I am grateful to my sister, Linda, for always being there for me as a friend. I am forever indebted to my parents, Mauro and Tiziana, for giving me the opportunities and experiences that have made me who I am. They always supported me and let me freely pursue this path. This journey would not have been possible if not for them, and I dedicate this milestone to them.

Contents

List of Figures

List of Tables

List of Acronyms

3GPP	3rd Generation Partnership Project v, 2
5G	Fifth generation v, 2
6G	Sixth generation 61
ACF	Autocorrelation function 14
AGC	Automatic gain control 19
AOA	Angle of arrival 19
AP	Access point 6
AR	Autoregressive 41
AWGN	Additive white Gaussian noise v, 4
BER	Bit error rate 23
BLER	Block error rate xiv, 6
BPSK	Binary phase shift keying 15
BS	Base station 62
C/A	Coarse/acquisition 14
CAF	Cross ambiguity function 14
CDF	Cumulative distribution function 29
CRC	Cyclic redundancy check 5
CRPA	Controlled radiation pattern antenna 19
CS	Commercial service 23
DL	Downlink 64
DLL	Delay-locked-loop 15
DME	Distance measuring equipment 18
DoS	Denial of service 2
DSP	Digital signal processing 24
DST	Dempster-Shafer theory 55
DVB-T	Terrestrial digital video broadcasting 18
ECEF	Earth-centered earth-fixed 51
EESM	Exponential effective SINR metric 78
EGNOS	European geostationary navigation overlay system 5
ENSPACE	Enhanced Navigation in Space 3
ESA	European Space Agency 3
EU	European Union 18
FA	False alarm 65
FDD	Frequency division multiplexing 2
FDoA	Frequency difference of arrival 19
FEA	Forward estimation attack 25
FLL	Frequency-locked-loop 15
GEO	Geostationary Earth orbit 48
GLONASS	Global'naja navigacionnaja sputnikovaja sistema 27
GLRT	Generalized likelihood ratio test v, 6
GNSS	Global navigation satellite system v, 1
GPS	Global positioning system 1

GSA	European GNSS Agency 3
IAD	Inter-AP distance 75
IF	Intermediate frequency 12
ILS	Instrument landing system 18
IMU	Inertial measurement unit 22
InI	Indoor industrial 75
InO	Indoor office 75
InO	Inertial navigation system 19
IoT	Internet of things 2
JR	Joint reception 77
JTIDS	Joint tactical information distribution system 18
KPI	Key performance indicator 63
LEO	Low Earth orbit 48
LOS	Line-of-sight 3
LRT	Likelihood ratio test 50
LTE	Long term evolution 62
MBB	Mobile broadband 6
MD	Missed detection 6
MEO	Medium Earth orbit 48
MIDS	Multifunctional information distribution system 18
MIMO	Multiple-input multiple-output 2
MLE	Maximum likelihood estimate 65
MM	Moments method 54
MMSE	Minimum mean squared error 77
MOPS	Minimum operational performance standard 5
MORE GOSSIP	More GNSS Open Service Signal Integrity Protection and Authentication at the Physical Layer 3
MRC	Maximum ratio combining 77
MSE	Mean squared error 50
NCO	Numerically controlled oscillator 16
NMA	Navigation message authentication 23
NORAD	North American Aerospace Defense Command 50
NR	New radio 2
NWPR	Narrowband-wideband power ratio 54
OFDM	Orthogonal frequency division multiplexing v, 2
OS	Open service 24
OSNMA	Open service navigation message authentication 3
PATROL	Position Authenticated Tachograph for OSNMA Launch 3
PDCP	Packet data convergence protocol 61
PDF	Probability density function 30
PG	Plain gradient 41
PLL	Phase-locked-loop 15
PMF	Probability mass function 67
PPD	Personal privacy devices 18
PRB	Physical resource block 69
PRN	Pseudorandom noise 10
PVT	Position, velocity, and time 1
r.v.	Random variable 62
RAIM	Receiver autonomous integrity monitoring 22
RE	Resource element 62

RF	Radio frequency 10
RLRT	Roy's largest root test 82
RMSE	Root mean squared error 44
ROC	Receiver operating characteristic 34
RSCN	Real signal-complex noise 54
RSS	Received signal strength 19
SBAS	Satellite-based augmentation systems 5
SCER	Security code estimation and replay 25
SDR	Software defined radio 4
SE	Spectral efficiency xiv, 6
SGP	Simplified general perturbations 50
SGP4	Simplified general perturbations 4 49
SINR	Signal to interference plus noise ratio 63
SIS	Signal in space 10
SNR	Signal-to-noise ratio 54
SNV	Squared signal-to-noise variance 54
SQM	Signal quality monitoring v, 3
SV	Space vehicle 25
TACAN	Tactical air navigation 18
TDD	Time division duplex 2
TDoA	Time difference of arrival 19
TLE	Two-line orbital element set 50
TOA	Time of arrival 22
TOW	Time of week 23
U.S.	United States 9
UE	User equipment v, 6
UL	Uplink v, 6
URLLC	Ultra-reliable low-latency communications v, 2
VOR	Very high frequency omnidirectional range 18
WN	Week number 23

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

Chapter 1

Introduction

Wireless communication technology has evolved rapidly during the last 20 years. Nowadays, there are networks providing communication infrastructures to not only people but also to machines, such as unmanned air and ground vehicles, cars, household appliances and so on. There is no doubt that new wireless communication technologies must be developed, that support the data traffic in these emerging, large networks. While developing these technologies, it is also important to investigate the vulnerability of these technologies to different malicious attacks. Moreover, as these technologies evolve and spread, the concerns for security in all electronic and telecommunication systems increase as well. This concern applies to many different sectors of today's society, two of them being global navigation satellite systems (GNSSs) and mobile networks.

1.1 The Need for Protection of GNSS Signals

As technological advances are introduced in society and their use spreads among the people, more and more applications are found for each technology. 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.

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 threat posed by 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 GNSS, one of the most dangerous is the spoofing attack. It consists on the transmission of GNSS-like signals with the goal of taking control of the position, velocity, and 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.

On the other hand, jamming is the simplest-to-generate attack against GNSS systems among the artificial interferences. GNSS jammers broadcast an interference signal in one or several of the frequency bands used by the GNSS signals. This attack

can be categorized as denial of service (DoS) attack, since the true GNSS signal transmission is not modified or altered. The true signal is still available but it is masked by the jammer signal, whose power is usually orders of magnitude higher than the signals coming from the satellites. The GNSS signals coming from the satellites are below the noise level, because of the large transmitter–receiver distance (around twenty thousand kilometer) that causes a high signal attenuation.

In this context, the contribution of this Thesis is to provide design and performance evaluation of the some signal processing techniques for the protection of GNSS signals against both spoofing and jamming attacks.

1.2 The Need for Protection of Mobile Networks

The fifth generation (5G) of wireless cellular networks promises faster data rates and reliable service delivery. It is expected to enable many cutting-edge technologies such as internet of things (IoT), self-driving cars, and smart cities. In 2017, 3rd Generation Partnership Project (3GPP) released the specification of 5G new radio (NR), which has been the primary reference for the deployment of these networks. 5G NR architecture is built upon five fundamental pillars: new radio spectrum, massive multiple-input multiple-output (MIMO)/beamforming, multi-connectivity, network flexibility, and high level of security. 5G is operable on a new radio spectrum from below 1 GHz to up to 100 GHz. The 5G NR physical layer uses orthogonal frequency division multiplexing (OFDM) with a cyclic prefix on the downlink and either the OFDM or discrete Fourier transform-spread OFDM for uplink. The 5G NR frame is of 10 ms duration, which is divided into ten sub-frames; in each sub-frame there are multiple slots (their number depends on the numerology), each one containing fourteen OFDM symbols. 5G NR supports both the frequency division multiplexing (FDD) and time division duplex (TDD) modes [8].

As any wireless cellular networks, 5G networks are built upon open sharing of the communication medium, where the communication medium is the free space, making them prone to interference, which is one of the fundamental causes of degradation of the performance of wireless networks. If the level of obstruction is high, the receivers are not able to decode the transmitted signals. This weakness can be used by some adversary nodes to cause intentional interference and hinder legitimate user's communication over specific wireless channels. This is well-known as jamming attacks.

Jamming attacks pose serious risks to public communication services [9], [10]. In early 1900, jamming attacks were used in military battles. Nowadays, jamming attacks can be launched to hinder public communication services. Several jammer devices are available in the market at a low cost. In addition, the most sophisticated jamming attacks can be implemented with a price as low as 1000 $ using low-cost software-defined radio tools, and some primary programming skills. Furthermore, 5G is expected to be the infrastructure for emergency services, natural disasters rescue, public safety, and military communications making jamming attacks a real threat.

In this context, the contribution of this Thesis is to provide design and performance evaluation of a signal processing technique for the protection of 5G and beyond networks, with particular focus to ultra-reliable low-latency communications (URLLC) communications, against jamming attacks.

1.3 Contribution

This doctoral Thesis is based on the work done during three years of Ph.D. studies. The majority of works that reached publication in international conferences are presented and treated throughout the chapters of the thesis. In this Section a brief description of the research activity conducted during the three years is provided, even for the topics not included in this thesis.

During my first two years of Ph.D. my research activity focused on the study and on the development of techniques for the protection of GNSS signals and it was carried out within the following three projects:

- More GNSS Open Service Signal Integrity Protection and Authentication at the Physical Layer (MORE GOSSIP), a project funded by the European Space Agency (ESA) on authentication and integrity protection of GNSS Open Service;
- Enhanced Navigation in Space (ENSPACE), a project funded by the European GNSS Agency (GSA) on innovative software application for enhanced space navigation, positioning and timing. The consortium is composed by Qascom (prime contractor), University of Padova, Spirent Communications, GEA Space, Endurosat and Euroconsult;
- Position Authenticated Tachograph for OSNMA Launch (PATROL), a project funded by the GSA on development, supply and testing of a Galileo open service navigation message authentication (OSNMA). The consortium is composed by Qascom (prime contractor), FDC, ST Microelectronics, GMV, Actia and University of Padova.

During my third and last year of Ph.D. I spent a period abroad for an internship at Nokia Bell Labs Stuttgart where my research activity focused on the development and performance evaluation of novel jamming detection and mitigation techniques working at the physical layer and tailored for 5G URLLC.

An overview of the research activity done within these projects follows.

1.3.1 Signal Processing Techniques for a Security-Oriented GNSS Software Package

The focus of this Ph.D. was not only on research, but involved the development of a GNSS software simulator and a GNSS software receiver. While there are other more sophisticated tools for GNSS simulation and evaluation, the community is still missing a platform to test security aspects of GNSS. The tools we developed at the University of Padova are indeed security-oriented and serve as a powerful validation tool for part of the research results presented in this Thesis.

The research activity carried out alongside the development of the software package can be divided into different topics.

Signal quality monitoring (SQM) techniques SQM techniques have been previously employed to monitor the GPS correlation peak quality in multipath fading environments and for monitoring of evil waveforms. The interaction between spoofing and authentic signals can affect the correlator output in a way similar to that of multipath components. Therefore, in the literature SQM techniques have been extended to detect spoofing attacks on tracking receivers working in line-of-sight (LOS) conditions, and 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.

During the first year of my Ph.D., these techniques has been implemented in MATLAB language within a simple ad-hoc scenario with additive white Gaussian noise (AWGN) channel, and the performance evaluation has been carried out for different metrics, for different authentic C/N_0 and against three types of attack. Then, during the second year, these techniques has also been implemented as a module of the software receiver developed in Python language. The performance of the different metrics has been evaluated for different metrics, for different authentic C/N_0 and against an attack where the attacker sends a spoofing signal with the same shape of an authentic signal (classic attack), without knowing the phase of the authentic signal at the receiver. The attack has been implemented as a module of the software simulator developed in C++ languag. Finally, the implementation of the SQM techniques in the software receiver has been validated. The results are presented in Chapter 3.

Jamming for the interference of GNSS signals During the first year, the capabilities of current software defined radios (SDRs) in generating a fast random frequency hopping jamming and a fast deterministic frequency hopping jamming have been experimentally analyzed. This has been accomplished by comparing the expected spectrogram with the spectrogram generated by a spectrum analyzer.

Notch filter During the second year, an adaptive notch filter [11] has been implemented as a module of the software receiver developed in Python language within the MORE GOSSIP project. Its performance has been tested against a deterministic step frequency hopping jamming. In particular, in this type of jamming, the attacker generates a narrowband signal with variable central frequency. The results are presented in Chapter 3.

PVT module During the second year, a PVT module has been implemented in the software receiver developed in Python language within the MORE GOSSIP project. The module takes as input the observables that is outputted by the tracking block (code delay and Doppler frequency) and the navigation message that is outputted by the demodulation block. The module outputs position, velocity and time of the receiver.

1.3.2 Detection of GNSS Spoofing by a Receiver in Space

The use of the consistency checks for the detection of GNSS spoofing signals on space receivers has been investigated. In particular, the problem of detecting spoofing attacks for a GNSS receiver in space orbiting around the Earth has been considered. Since for a receiver in space the access to the so called signals of opportunity is limited, it is more practical to rely in the signal itself for detecting anomalies and checking the consistency of its measurements with the computed orbital position. Three different consistency checks has been considered: on the overall received GNSS signal power at the front-end; on the estimated C/N_0 for the signal coming from each satellite in view; on the final computed position at the receiver output. Moreover, a fusion method that combines soft outputs from the three checks to provide a more reliable and robust detection has been devised. The proposed techniques have been tested in a realistic simulation environment showing that, although the position consistency check is by far the most reliable, the proper fusion of the soft information from all three allow to further improve the detection rates in different conditions significantly. This research

activity led to the publication of a conference paper [12]. The results are presented in Chapter 4.

1.3.3 Detection of SBAS Data Spoofing

Augmentation of a global navigation satellite system (GNSS) is a method of improving the navigation system's attributes, such as accuracy, reliability, and availability, through the integration of external information into the calculation process. Satellite-based augmentation systems (SBAS) support wide-area or regional augmentation through the use of additional satellite-broadcast messages. Using measurements from the ground stations, correction messages are created and sent to one or more satellites for broadcast to end users as differential signal.

A consistency check based on SBAS data has been designed in order to detect simplistic attacks generated not following the specifications of the minimum operational performance standard (MOPS). In particular, this check monitors the decoded European geostationary navigation overlay system (EGNOS) bits to detect major inconsistencies. Specifically, the algorithm foresees the following steps:

- Grabs the SBAS decoded bits.
- Preliminary checks: monitors the preamble to verify that it follows the reference pattern and performs the parity check to verify that the cyclic redundancy check (CRC) parity bits are consistent with the rest of the message.
- Message type filtering: verifies that the received message type is among the usable data.
- SBAS data checks: monitors the IODP, the IODI, the IODS, the IODF, and the IODM fields of the SBAS message to verify that they follow the reference pattern.
- Maximum update interval check: monitors that two messages of the same type are received within the maximum update interval defined in the MOPS.

This procedure does not protect the user from a wide range of spoofing attacks. However, it prevents rough message forgery of an attacker that has low technical skills or low resources. This research activity has been part of a technical report internal to the project.

1.3.4 Jamming Detection and Mitigation for Indoor Industrial Scenarios

The 5th generation (5G) of mobile networks has been designed to tackle novel use cases such as industrial automation, intelligent transportation, and remote health. The challenges posed by these new scenarios in terms of latency and reliability have led to the term "ultra-reliable low-latency communications" (URLLC): the devices used for these applications generate packets that need to be transmitted and received over the wireless channel with extreme low-latency (up to 1 ms or less) and very high reliability. Mainly because of these extreme requirements, this type of traffic becomes very sensitive to some types of attackers, for instance jammers that maliciously inject interference into the network. Physical layer security techniques represent a good first defense against these attacks and therefore it is important to develop and evaluate novel techniques tailored for 5G URLLC.

As a first contribution, the problem of jamming detection in 5G and beyond communication systems has been considered and a defense mechanism based on pseudo-random blanking of subcarriers with OFDM has been proposed. Then, a detector has been designed by applying the generalized likelihood ratio test (GLRT) on those subcarriers, which resulted to be an energy detector on the received signal. Finally, the performance of the proposed technique has been evaluated against a smart jammer in single-cell single-user uplink (UL) scenario with AWGN and Rayleigh channel models. Namely, a jammer pursuing one of the following objectives has been considered: maximize its stealthiness, minimize spectral efficiency (SE) with mobile broadband (MBB) type of traffic, and maximize block error rate (BLER) with URLLC. Numerical results show that a smart jammer a) needs to compromise between missed detection (MD) probability and SE reduction with MBB traffic and b) can achieve low detectability and high system performance degradation with URLLC only if it has sufficiently high power. This research activity led to the publication of a conference paper [13]. The results are presented in Chapter 5.

This work has then been extended to investigate the problem of jamming detection and mitigation in a more realistic indoor factory deployment. In particular, two jamming detectors based on pseudo-random blanking of subcarriers with OFDM have been considered: the above-mentioned energy detector and a further detector that exploits antennas correlation at the receiver. Moreover, jamming mitigation with frequency hopping and random scheduling of user equipments (UEs) has been proposed. Then, the performance of the system has been evaluated in terms of achievable BLER with URLLC traffic and jamming MD probability. Simulations have been performed considering a 3GPP spatial channel model for the factory floor and with a jammer stationed outside the plant trying to disrupt communications inside the factory. Numerical results show that jamming resiliency increases when using a distributed access point (AP) deployment and exploiting channel correlation among antennas for jamming detection, while frequency hopping is helpful in jamming mitigation only for strict BLER requirements. This research activity led to the publication of a conference paper [14]. The results are presented in Chapter 6.

1.4 Thesis Outline

The Thesis is structured as follows:

- Chapter 2 first provides a brief description of the general architecture of GNSS systems; then, a delineation of the structure of the GNSS signals emitted by a satellite is presented, followed by a characterization of the building blocks of a typical GNSS receiver; finally, a brief introduction about jamming and spoofing threats for GNSS systems is given.

- Chapter 3 starts describing context and structure of the developed security-oriented GNSS software package; then, an assessment on the effectiveness of the SQM techniques for spoofing detection is presented; finally, the performance of a notch filter implementation in the software receiver.

- Chapter 4 presents a spoofing detection technique for a receiver in space via fusion of consistency metrics.

- Chapter 5 proposes a jamming detection scheme based on pseudo-random blanking of subcarriers with OFDM for 5G and beyond in Industry 4.0 scenarios; in particular, a detector is designed by applying the GLRT on those subcarriers;

then, the performance of the proposed technique is evaluated in a single cell-single user uplink scenario with AWGN and Rayleigh channels against a smart jammer.

- Chapter 6 presents design and performance evaluation for jamming resilient indoor factory deployments; at first, the scenario is described with a jammer outside a factory deployment with 3GPP spatial channel model; then, two jamming detectors based on pseudo-random blanking of subcarriers and a jamming mitigation scheme based on frequency hopping user scheduling are proposed; finally, the performance is evaluated for three different AP deployments in terms of achievable BLER with URLLC traffic and jamming detection probability.
- Finally, Chapter 7 draws some conclusions of the work presented within this Thesis.

Chapter 2

GNSS Overview

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.

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 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 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.

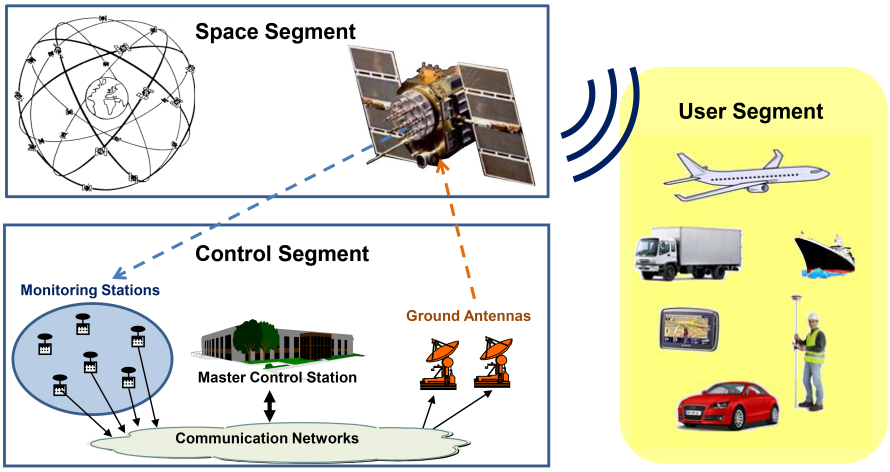


FIGURE 2.1: Pictorial sketch of the three segments in the GNSS architecture [15].

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.

2.2 GNSS Signals

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

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, $C(t)$: binary sequences 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:

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

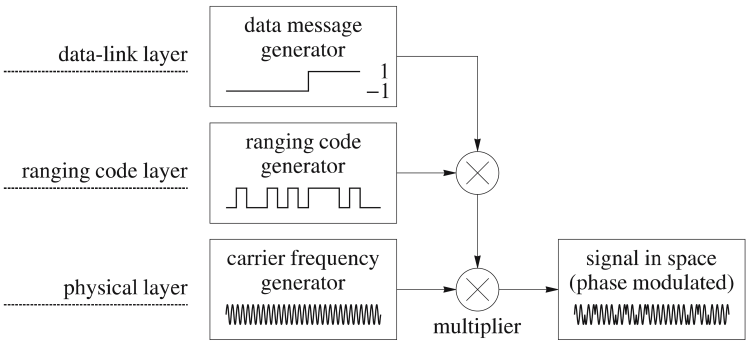


FIGURE 2.2: Composition of the navigation satellite signal [17].

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

2.3 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 SISs 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 variations might be present to accommodate different solutions. The basic building blocks of a generic GNSS receiver are as shown in Fig. 2.3.

2.3.1 Antennas

GNSS antennas are aim at capturing GNSS signals, with the associated amplification and filtering. It is the entry point from the space segment to the user segment, as it receives the signals to pre-process and feed as an analog electrical signal to the front end. 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

$$r_{\mathrm{RF}}(t) = a\sqrt{2P}D(t-t_{\mathrm{p}})C(t-\tau)\cos\left[2\pi(f_{\mathrm{RF}}+f_{\mathrm{D}})(t-t_{\mathrm{p}})+\phi_0\right]+n_{\mathrm{RF}}(t) \tag{2.2}$$

with

$$f_{\mathrm{D}} = -\frac{f_{\mathrm{RF}}}{c}\frac{\mathrm{d}t_{\mathrm{p}}}{\mathrm{d}t}\,, \tag{2.3}$$

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

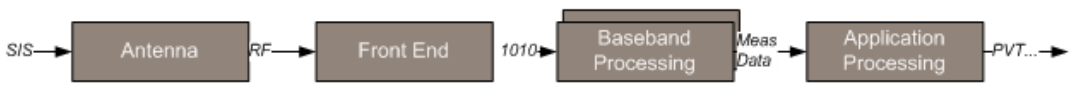


FIGURE 2.3: Generic receiver architecture [18].

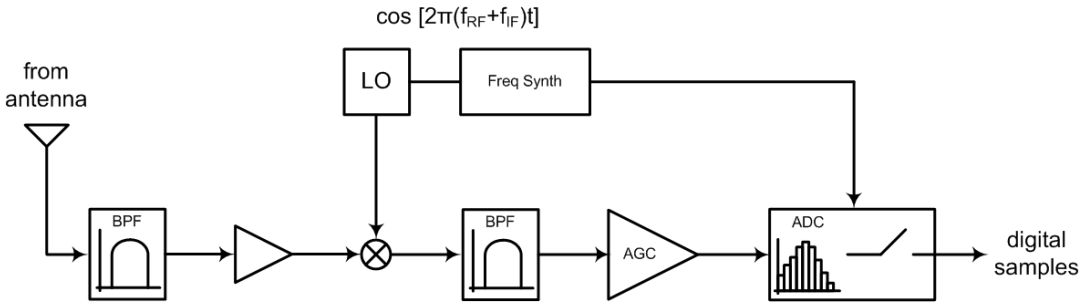


FIGURE 2.4: Example of GNSS receiver's front end structure [15].

shift (Hz) and $n_{\mathrm{RF}}(t)$ is the additive noise component at RF. In order to simplify the notation, Eq. (2.2) can be rewritten as

$$r_{\mathrm{RF}}(t) = AD(t - t_{\mathrm{p}})C(t - \tau)\cos\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D}})t + \phi\right] + n_{\mathrm{RF}}(t)\,, \tag{2.4}$$

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.

2.3.2 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 2.4 illustrates a typical front end structure in GNSS receivers. 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 an intermediate frequency (IF) digital signal.

From Eq. (2.2), the signal at the end of the front end for a single satellite can be modeled as

$$\begin{aligned} r_{\mathrm{IF}}(k) = {} & AD(kT_{\mathrm{s}} - t_{\mathrm{p}})C(kT_{\mathrm{s}} - \tau)\cos\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D}})kT_{\mathrm{s}} + \phi\right] + n_{\mathrm{IF}}(kT_{\mathrm{s}}) \\ & \text{for } k = 0, 1, 2, \ldots\,, \end{aligned} \tag{2.5}$$

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

2.3.3 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 each channel is integrated to derive a navigation solution. Figure 2.5 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

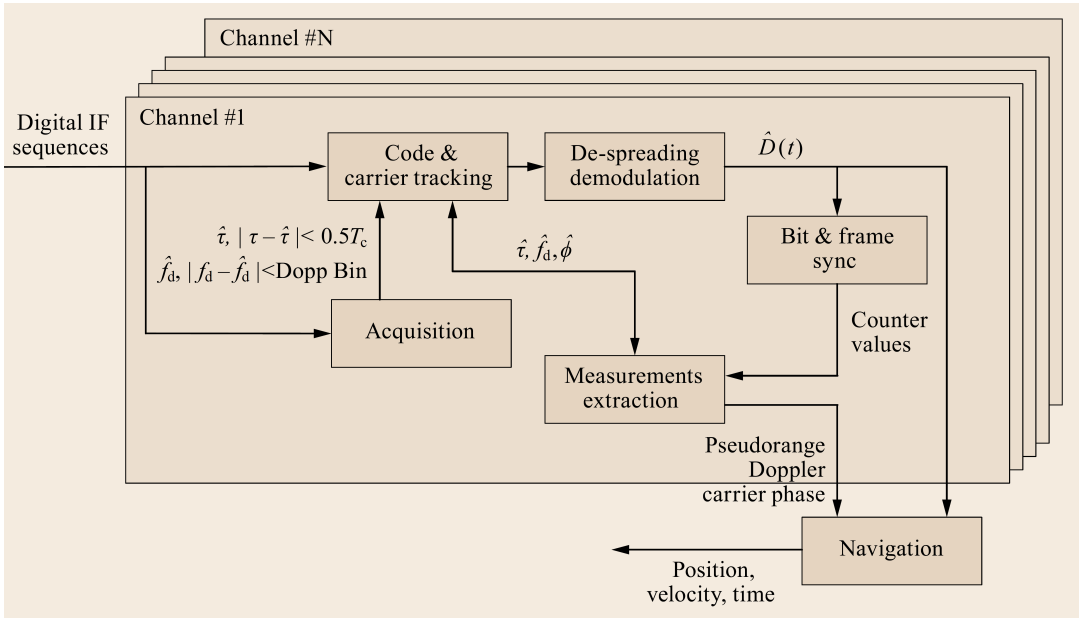


FIGURE 2.5: Block diagram of internal functions in a generic baseband processing block [16].

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

$$r(k;\tau,\phi,f_{\mathrm{D}},A) = AD(kT_{\mathrm{s}}-\tau)C(kT_{\mathrm{s}}-\tau)\mathrm{e}^{j[2\pi(f_{\mathrm{IF}}+f_{\mathrm{D}})kT_{\mathrm{s}}+\phi]} + n(kT_{\mathrm{s}}) \quad \text{for } k = 0,1,2,\dots , \tag{2.6}$$

where

$$n(kT_{\mathrm{s}}) \sim \mathcal{CN}\left(0,\sigma_n^2\right) , \tag{2.7}$$

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 $\tau, \phi, f_{\mathrm{D}}$ 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

$$\hat{r}_{\mathrm{IF}}(k) = C(kT_{\mathrm{s}}-\hat{\tau})\mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}}+\hat{f}_{\mathrm{D}})kT_{\mathrm{s}}+\hat{\phi}\right]} . \tag{2.8}$$

The correlation operation is given by

$$\mathrm{corr}\left[r(k),\hat{r}(k)\right] = \frac{1}{M}\sum_{k=1}^{M} r(k)\hat{r}^*(k) , \tag{2.9}$$

where $\mathrm{corr}(x,y)$ 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

$$S = ADR(\Delta\tau)\,\text{sinc}\,(\Delta f_{\text{D}} T_{\text{coh}})\text{e}^{j(\Delta\phi+\pi\Delta f_{\text{D}} T_{\text{coh}})} + \eta \tag{2.10}$$

where

$$\eta \sim \mathcal{CN}\left(0, \sigma_\eta^2\right) , \tag{2.11}$$

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. (2.10) 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

$$I = ADR(\Delta\tau)\,\text{sinc}(\Delta f_{\text{D}} T_{\text{coh}})\cos\left(\Delta\phi + \pi\Delta f_{\text{D}} T_{\text{coh}}\right) + \eta_I\,, \tag{2.12}$$

$$Q = ADR(\Delta\tau)\,\text{sinc}(\Delta f_{\text{D}} T_{\text{coh}})\sin\left(\Delta\phi + \pi\Delta f_{\text{D}} T_{\text{coh}}\right) + \eta_Q\,, \tag{2.13}$$

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

$$S_{\pm\alpha} = ADR(\Delta\tau \pm \alpha)\,\text{sinc}\,(\Delta f_{\text{D}} T_{\text{coh}})\text{e}^{j\Delta\phi} + \eta = I_{\pm\alpha} + jQ_{\pm\alpha}\,, \tag{2.14}$$

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

$$\hat{r}_{\mp\alpha}(k) = C(kT_{\text{s}} - \hat{\tau} \mp \alpha)\text{e}^{j\left[2\pi(f_{\text{IF}}+\hat{f}_{\text{D}})kT_{\text{s}}+\hat{\phi}\right]}\,. \tag{2.15}$$

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 SQM metrics) are reported:

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

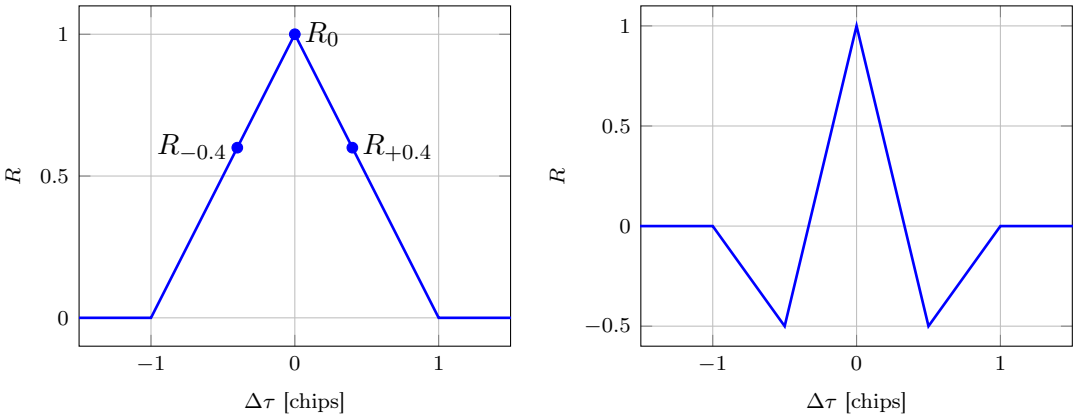
$$R(\Delta\tau) = \begin{cases} 1 - \frac{|\Delta\tau|}{T_c} & \text{for } |\Delta\tau| \le T_c\,, \\ 0 & \text{for } |\Delta\tau| > T_c\,, \end{cases} \tag{2.16}$$

  that is represented in Fig. 2.6A.

- **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 approximate form

$$R(\Delta\tau) = \begin{cases} 1 - \frac{3|\Delta\tau|}{T_c} & \text{for } |\Delta\tau| \le T_c/2\,, \\ -1 + \frac{|\Delta\tau|}{T_c} & \text{for } T_c/2 < |\Delta\tau| \le T_c\,, \\ 0 & \text{for } |\Delta\tau| > T_c\,, \end{cases} \tag{2.17}$$

  that is represented in Fig. 2.6B.



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

FIGURE 2.6: Normalized ACF of two differently modulated signals.

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.

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 2.7 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 a complex baseband signal, where real and imaginary parts are typically called I and Q signal components, respectively. 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 binary phase shift keying (BPSK) signal). They are, similar to the previous 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):

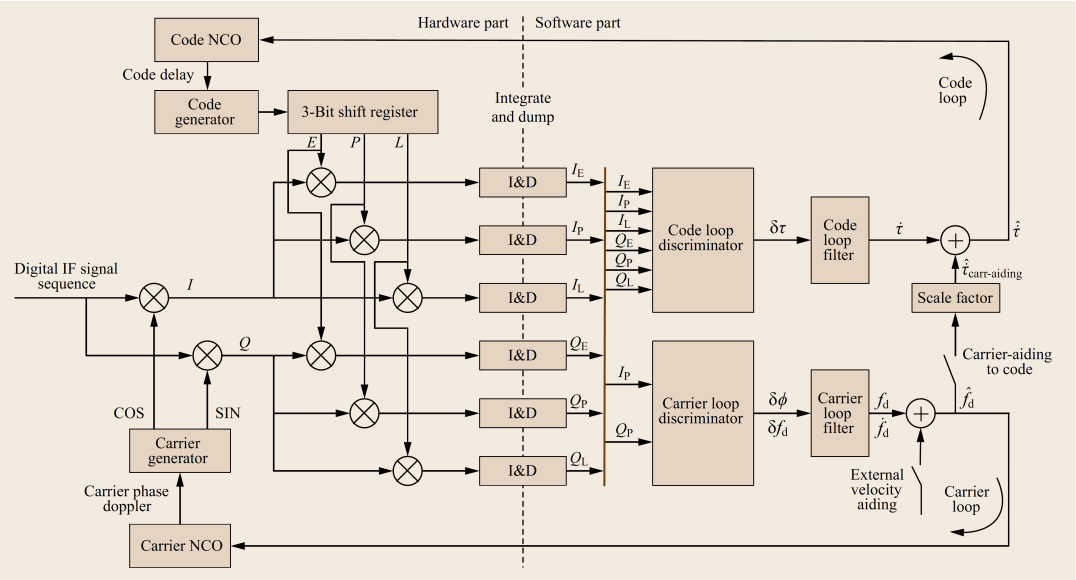


FIGURE 2.7: Block diagram of a GNSS signal tracking engine [16].

- **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.
- **DLL Discriminators.** The DLL discriminator uses the early and late branches rather than the prompt branch of the carrier loop. Figure 2.8 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.

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

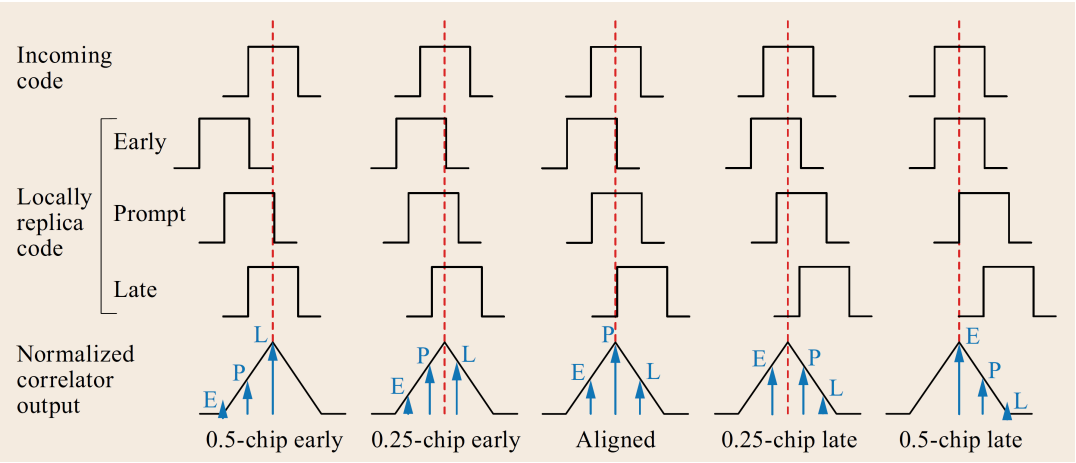


FIGURE 2.8: Early-minus-late DLL discriminator [16].

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 prompt correlator output. In fact, when a signal is being correctly tracked, the prompt correlator output can be mapped to the right symbol of the binary data sequence containing the navigation message.

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:

$$R = c(t_{\mathrm{r}}(T_2) - t^{\mathrm{s}}(T_1)) \tag{2.18}$$

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 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.

2.3.4 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.

2.4 Attacks to GNSS Receivers

If an interference signal $I(t)$ is present, it may cause a GNSS receiver to cease operation, generate random-like position estimates, or an intentionally set wrong position or time estimate. This depends on the received waveform $I(t)$.

There are two main families of intentional interferences that can affect GNSS systems and their users: spoofing and jamming. While a jammer can use a number of different signal modulations for $I(t)$ with high power to affect the availability of the GNSS satellite signals and its related services, a spoofer attempts to deceive the

GNSS user navigation by transmitting signals $I(t)$ with the same characteristics as the legitimate GNSS satellite signals $s(t)$. A spoofed GNSS receiver will then report a false position and/or timing information from its true one, also depending on the type of the attack accompanied with a confirmed integrity check.

2.4.1 The Jamming Threat

Interference and jamming have long been at the core of the focus of the GNSS community due to the impact that such kinds of threats have on GNSS signals. In the literature, unintentional interference from other communication systems affecting the low power GNSS signals are distinguished from jammers that intend to intentionally affect the operation of a GNSS receiver. Unintentional interference includes:

1. Out-of-band interference caused by harmonics and intermodulation products, as for example from terrestrial digital video broadcasting (DVB-T) signals [1], very high frequency omnidirectional range (VOR) plus instrument landing system (ILS) signals [19], multicarrier modulated satellite communication systems and amateur radio services.

2. In-band interference, including civilian and military terrestrial navigation systems as distance measuring equipment (DME) and tactical air navigation (TACAN), military spread-spectrum communication systems like the joint tactical information distribution system (JTIDS) and the multifunctional information distribution system (MIDS) as well as wind profiler radars and civilian radars (1215–1400 MHz) [20].

Intentional interference or jamming is achieved by using devices that can generate powerful signals in the GNSS band, causing a range of effects. A big class of them belong to the personal privacy devices (PPD) that are used as in-car jammers to avoid a vehicle being tracked for, e.g., road tolling [21], having effective ranges in the order from a few tens of meters to kilometers [22]. Although in U.S. and in several European Union (EU) countries, jamming devices are illegal to sell, there are devices that can be purchased through websites costing few tens of dollars. As a matter of fact, several jamming incidents have been reported involving the disruption of GNSS services in local harbors and airport traffic control management [23].

The effects of interference can be summarized as: loss of tracking, increased pseudorange errors, high demodulation error rates, denial of acquisition and false signal detection and continuous cycle slips. The effect of interference is described by the effective carrier to noise density ratio [24]. In this model, the jamming signal increases the noise in the estimates. The higher the jamming power and the better the interfering signal matches the satellite signal, the larger the increase of the noise. This is expressed as a reduction of the received signal to noise ratio C/N_0 to an effective ratio $C/N_{0,\text{eff}}$ described as

$$\frac{C}{N_{0,\text{eff}}} = \frac{C \int_{-B/2}^{B/2} G_s(f) df}{N_0 \int_{-B/2}^{B/2} G_s(f) df + J \int_{-B/2}^{B/2} G_s(f) G_I(f) df}, \tag{2.19}$$

$G_s(f)$ is the spectrum of $s(t)$, $G_I(f)$ is the spectrum of $I(t)$ and B denotes the receiver's front end bandwidth. Thus, by signal design, the overlap between $G_s(f)$ and $G_I(f)$ can be decreased, reducing the jammer's impact on the effective $C/N_{0,\text{eff}}$. Obviously the model assumes that amplifiers, filters and mixers operate in their linear region, which is completely false, if the jamming "saturates" the frontend of the receiver. Thus anti-jam capable GNSS receivers typically employ tailored RF front ends [25].

2.4.1.1 Anti-Jamming Techniques

While works that survey the field of jamming in GNSS systems are not available, the studies in [26]–[30] give nonetheless a good overview of issues caused by jamming and potential solutions.

The authors of [26] address the negative impact of jamming on the GNSS receiver performance and present three classes of jamming detection: at automatic gain control (AGC) level, at digital pre-correlation signal processing level, and at post-correlation domain level. However, no comparative performance analysis between these three different detection classes is provided, the main take-away message being that the interference detection can be done at different stages of the receiver.

The authors of [27] give a broad overview about increasing the robustness of GNSS in the presence of jamming and discuss InO/GNSS-coupled navigation (where InO stands for inertial navigation system), spatial filtering, and time-frequency filtering vector tracking. Again, no comparative performance between the different algorithms is given and the conclusions state that any of the studied approaches is beneficial for GNSS and they can detect or mitigate jamming.

Jamming mitigation based on beamforming techniques with multi-antenna GNSS receivers is the focus of [28]. While all the tested multi-antenna controlled radiation pattern antenna (CRPA) techniques are shown to be much better than single antenna techniques, no winning technology among the studied beamformers was selected. Then, [29] discuss the use of sparse arrays and sparse sampling to mitigate jamming in the context of GNSS. They use a co-array framework on single and multiple-antenna/CRPA receivers for improved beamforming, in order to estimate the jamming signal's angle of arrival (AOA) and to suppress it. In [30] the localization of jammers is addressed, and different approaches based on AOA, time difference of arrival (TDoA), frequency difference of arrival (FDoA) and received signal strength (RSS) were described and compared qualitatively. No quantitative analysis in terms of performance metrics was provided.

2.4.2 The Spoofing Threat

Spoofing is a more complex attack against GNSS systems than jamming. Spoofing attacks simulate or modify the true GNSS signals and rebroadcast it back. By doing this, the attacker can modify the PVT solution of a target victim receiver at his/her will. For spoofing to work, the receiver must continue to correctly operate, and for a successful attack against a sophisticated receiver, the fake signal must both jam the true signal and be indistinguishable from it, containing false but at the same time apparently true information.

The motivation for spoofing attacks arise from the pervasiveness of GNSS and their feasibility is due to the availability of both the most public civilian GNSS signal structure and the advancement in SDR technology. The awareness about the vulnerability of satellite positioning to signal forgery dates back to 2001–2003, with the well known Volpe report [31] and the paper [32]. But it is in the last ten years, since the proof that a spoofer fooling the civil GPS signals can be developed with low cost components [33], that the public interest has raised and literature production about GNSS spoofing aspects has significantly increased.

Another well-known example is a spoofing attack done by a team of scientists from the University of Texas that used a lab-built device to broadcast counterfeit GPS signal that were somewhat stronger than the real ones [7]. In this way, they took control of a luxury yacht's navigational system resetting the vessel's satellite navigation systems without the captain noticing it. The vessel's navigation system locked onto the fake

signal and, consequently, the system reported that it was off course, even though it was on the right track. Not realizing that the GPS signal was incorrect, the course was adjusted so that true vessel's track was inaccurate by a few degrees.

The complexity of the equipment setup necessary to carry out a GNSS spoofing attack is recognized as a non-negligible factor in the assessment of the potential danger: attacks with high level of associated complexity are less likely to be implemented on a large scale, or to low-revenue (under the spoofer's perspective) applications. In this light, [34]–[36] discuss evaluations of costs/difficulty associated to different kinds of attack, which, in general, are classified according to the receiver state, environment, etc.

The vulnerability of a receiver to a spoofing attack is explicitly addressed in [34], [37], which analyse the conditions in which a receiver may be deceived by false signals. Reference [37] investigates the vulnerability of the signal structure, identifying which signal components could be victims of forgery, namely the data bits and the pseudorange measurements. To obtain its goal, the malevolent spoofer takes advantage of the vulnerability of the civil GNSS at the signal processing level, since the signal structure is publicly known.

The survey [34] identifies the receiver vulnerabilities depending on the signal processing stage in which the receiver operates at the time of the onset of the attack; from that analysis, the tracking stage results the less vulnerable condition for a receiver, while the cold start offers the widest opportunities to the spoofer to succeed. This is the reason for which a feasible spoofing scenario often includes a preliminary jamming phase, used to force the receiver in a re-acquisition phase which leaves more room to vulnerability. In this light, [34] highlights the significant difference between tracking receivers and snapshot receivers; the former continuously estimate the frequency, delay, and phase of the signal, i.e., they extensively use prior knowledge about the signal; on the contrary the later sample the incoming signal in non-adjacent time windows and use each ordered set of samples to produce an estimate of the signal parameters. As a consequence, with respect to vulnerability, snapshot receivers behave like the acquisition stage of tracking receivers, and so they are particularly vulnerable to spoofing [34].

What is apparent from all the mentioned surveys is that in most cases vulnerability is a matter of lack of cross-checks and monitoring measures: since spoofing attacks realistically leave traces, the winning game should be the implementation of a number of "check points" in the receiving chain, where different metrics can be monitored in order to extract clues on the presence of non-authentic signals [3].

2.4.2.1 General Model of a Spoofing Attack

From Eq. (2.4), an authentic typical received GNSS signal takes the form

$$r_{\mathrm{a}}(t) = \sum_{i=1}^{N_{\mathrm{a}}} A_{\mathrm{a},i} D_{\mathrm{a},i}(t - t_{\mathrm{p,a},i}) C_{\mathrm{a},i}(t - \tau_{\mathrm{a},i}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D,a},i})t + \phi_{\mathrm{a},i}\right]}, \tag{2.20}$$

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. (2.2) and (2.4).

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

$$r_{\mathrm{s}}(t) = \sum_{i=1}^{N_{\mathrm{s}}} A_{\mathrm{s},i} D_{\mathrm{s},i}(t - t_{\mathrm{p,s},i}) C_{\mathrm{s},i}(t - \tau_{\mathrm{s},i}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{RF}} + f_{\mathrm{D,s},i})t + \phi_{\mathrm{s},i}\right]}\,, \tag{2.21}$$

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, $A_{\mathrm{s}}, \tau_{\mathrm{s}}, f_{\mathrm{D,s}}$ 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 $\tau_{\mathrm{s}}, \phi_{\mathrm{s}}, f_{\mathrm{D,s}}$ and A_{s} will be dropped. In this way, the total received signal at the victim receiver is

$$r(t) = r_{\mathrm{a}}(t) + r_{\mathrm{s}}(t) + n(t)\,, \tag{2.22}$$

where $n(t)$ is the noise term, whose main contribution is given by the receiver RF front end and it is common for both the authentic and spoofed signals.

2.4.2.2 Anti-Spoofing Techniques

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 level techniques*: data 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 inertial measurement unit (IMU) and Wi-Fi/cellular positioning.

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 RSS monitoring, received signal time of arrival (TOA) monitoring, spatial coherency analysis of received GNSS signals, SQM, cryptographic authentication, receiver autonomous integrity monitoring (RAIM) and consistency check among different sensors and constellations [32], [38]–[40].

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.

Chapter 3

Signal Processing Techniques for a Security-Oriented GNSS Software Package

3.1 Introduction

This Chapter provides a brief description of context and structure of the security-oriented GNSS software package developed at the University of Padova, followed by Section 3.2 (SQM techniques) and Section 3.3 (notch filter) which are part of my contribution to the package.

3.1.1 Context and Motivation

In GNSS, signal authentication and cryptographic integrity protection must offer the assurance of the observation of satellite signals' travel time, given satellite positions and a common time reference. Spoofing being an upcoming threat for GNSS based applications, it requires the design of GNSS authentication schemes at the system and receiver level, since the authentication and integrity protection system shall allow to verify that:

- Essential data information, such as is time of week (TOW), week number (WN), and ephemeris are authentic;
- The observation of travel time is performed on authentic and integral signals.

The former requirement is commonly referred to as navigation message authentication (NMA) and can be fulfilled through the use of traditional cryptographic techniques such as digital signature. The difficulties in designing appropriate NMA systems are mostly due to the low available bandwidth and high bit error rate (BER) due to low received power and environment impairments such as deep fading. As such in the last few years, the focus has moved to different solutions based on protocols designed for wireless broadcast authentication such as TESLA [41], or signature amortization [42]. A possible way to increase the system robustness to the environmental effects is to increase its redundancy without imposing a threat to the NMA security, since it was shown in [43] that channel coding can be exploited to perform an estimation of the unpredictable bits in authentication data. Many works on the NMA topic have been done including OSNMA [44]–[47] and commercial service (CS) [48]–[51] that form the basis on the exploitation and optimization of the current activity.

The latter requirement requires technological solutions to make the replay attack more difficult. For instance, encrypting spreading codes is considered interesting for a signal level security solution, because it is a chip level modulation and thus is more

difficult for an attacker to estimate the signal and perform a replay attack in the fashion of [52], [53]. On this topic is worth to mention past proposals such as spread spectrum security codes [54],[55] and signal authentication sequences [56] and more recent works such as supersonic codes [57], [58] that are based on the use of code shift keying [59], [60]. This promising modulation achieves higher bit rates than binary modulations, and has been already proposed for satellite applications as it can pave the way for the delivery of new services. The key distribution mechanism, which is a critical element of any cryptographic scheme, has also been the focus of this activity, to identify appropriate key distribution mechanisms and key revocation strategies, tailored to GNSS systems for open service (OS) applications.

In a complementary fashion to the above described system side mechanisms, receiver side processing schemes for the detection of spoofed signals have also been considered. In fact, depending on the application scenario GNSS receiving devices may have access to signals of opportunity, mobile networks, or inertial measurement unit and other sensor information. Furthermore, direct analysis of the received signals, or checking the consistency of PVT history may be itself sufficient to detect the less sophisticated attacks.

The main objectives of this activity has thus been to provide the software and hardware tools, tuned to the specific applications, for their use in the ESTEC laboratory aiming to investigation, analyse and validate different signal and receiver processing concepts for the provision of authentication services in the next generation of GNSS systems, as well as optimize their parameters and, eventually, to propose effective original mechanisms.

In particular the delivered tools provide the capabilities to:

- Generate GNSS signals, with authentication capabilities on message and code levels
- Add advanced coding schemes for the authentication part
- Process these signals through a dedicated GNSS receiver platform with and without external aiding, extracting the authenticity capabilities of digital signal processing (DSP) schemes from the Rf interface to the PVT calculation
- Devise and simulate dissemination strategies that could enhance the authentication services
- Simulate a flexible spoofing device capable to accommodate all types of spoofing attacks both in software and hardware

The hardware spoofing device, is composed of SDR devices, a processing unit capable to reach real time or quasi real time performance, and GNSS reference receivers to validate the results.

3.1.2 Development of the Software Packages

A significant part of our work involved the design and implementation of a GNSS software simulator and receiver for the validation of the proposed security mechanisms. Several online tools simulate the transmission of the GNSS signal to a specific receiving position and time, or the receiver signal processing chain with flexible parameters. However, an open source tool was not found that allows to integrate, evaluate, and test security mechanisms for the Galileo constellation. Moreover none of the available tools generates both Galileo and GPS signals. For the above reasons we designed our

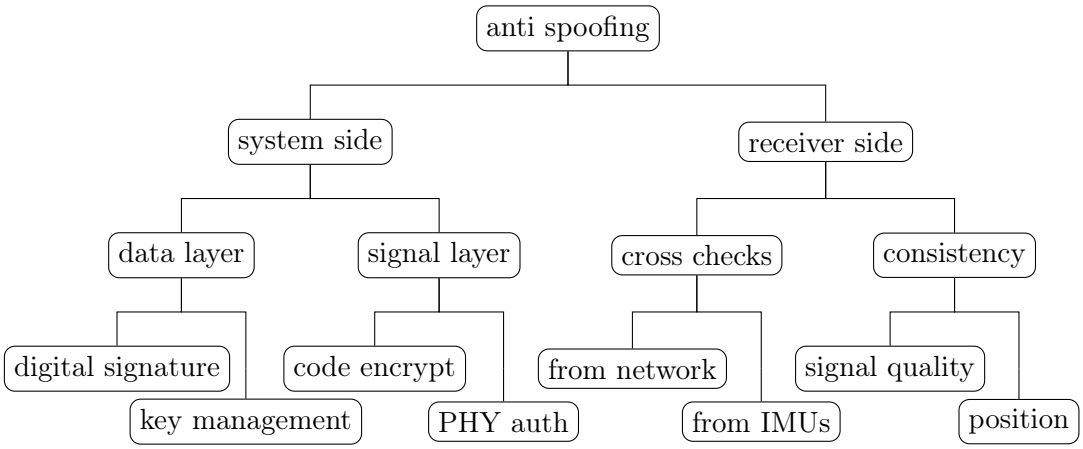


FIGURE 3.1: Contextual representation of the current and proposed solutions for authentication and integrity protection of GNSS signals in the security-oriented software package activity.

own software package, leaving room for the integration of any security feature and evaluation tools. The software is composed of two main packages, as detailed in the following.

GNSS Signal Simulator in C++ for Windows / MacOS This software simulates both GPS and Galileo signals. The software takes as input the receiver's position and time, the ephemeris file, and the operation mode parameters (nominal mode or attack evaluation) and outputs the I/Q samples of the baseband signal. It works in real time together with an SDR that modulates and transmits the samples at the GNSS central frequency and a commercial receiver for evaluation. The main novelty of the signal simulator is its capability of simulating data and signal layer attacks such as navigation message tampering, security code estimation and replay (SCER) attack, forward estimation attack (FEA), but also DoS attacks such as smart jamming. The GNSS signal simulator has been implemented in C++, and is based on an existing open source GPS-only signal simulator written in C. In designing the simulator the following choices have been made with the aim of building a simple, modular architecture, maintaining low execution time and allowing for easily adding new security features.

- In order to allow for real time signal generation the entire Doppler and pseudorange profile of the simulation is pre-computed for each satellite, given the prior knowledge on the user motion and satellite ephemeris. Thus, we replace the frequent Doppler update operation with a faster table lookup, removing the most critical bottleneck for the execution time.

- The key object in the simulations is the space vehicle (SV) object, which can be chosen as either a Galileo or GPS SV. In order to efficiently represent an attack scenario we simulate three different coexisting types of SVs: the legitimate SVs, as seen by the victim receiver, the attacker's SVs, as seen by the attacker and the false SVs, as seen in the spoofed position (controlled by the attacker).

- In order to guarantee the separation of the legitimate signal from the spoofing signal, we generate both outputs in parallel and mix them at the last step of the simulation, before modulation.

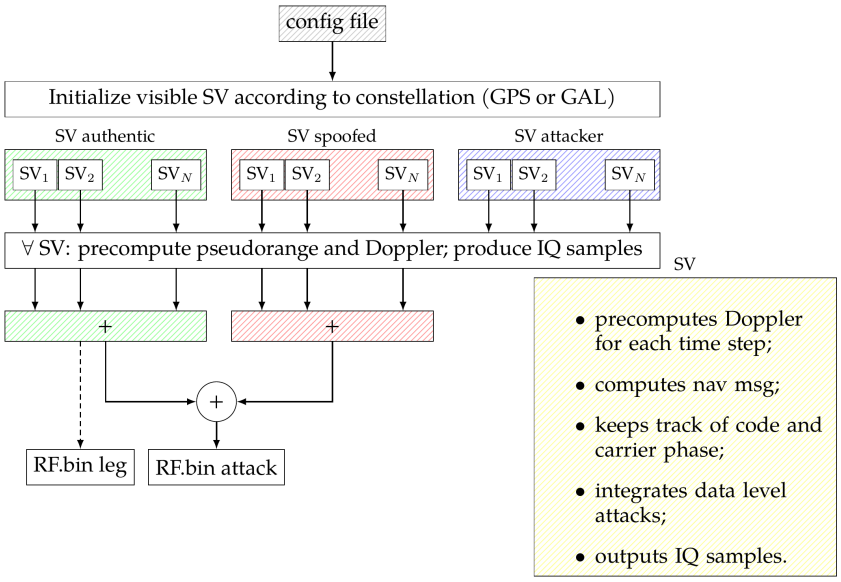


FIGURE 3.2: Block representation of the C++ GNSS software signal simulator.

- Parallel execution is made possible thanks to the thread library. All the operations relative to the signal generation for different SVs are executed in a parallel fashion, leading to a more efficient usage of the CPU and allowing real time execution.

A simple scheme of the simulator is represented in Fig. 3.2.

A GNSS Software Receiver in Python 3 Our software receiver takes as input the I/Q baseband samples (as generated by the signal simulator). It outputs results at several levels of the receiver's blocks: the statistical distribution of the sample values, the acquisition and tracking matrices with the code delay and carrier phase, the navigation message data, and the user's position and time. An option was inserted for testing different channel coding schemes in innovative/novel GNSS navigation messages. Moreover, an interface with the simulator couples the two pieces of software in order to perform a realistic SCER attack. The software receiver is capable of receiving both GPS and Galileo signals and is composed by the following blocks:

- a frequency analysis block that may reveal the presence of anomalies such as narrow-band interference;
- an acquisition block with user-controlled parameters such as the coherent integration time and the number of non coherent integration periods, as well as the thresholds to declare a signal as present;
- a tracking block, where the tracking loop parameters can be adjusted to follow specific receiver dynamics, that works in parallel across different satellites to reduce the execution time;
- a data demodulation block, where the navigation message

  fields are parsed to retrieve all the relevant parameters for the positioning block, and perform an integrity check against ill formed navigation messages;
- the position computation block.

A simple scheme of the receiver is represented in Fig. 3.3.

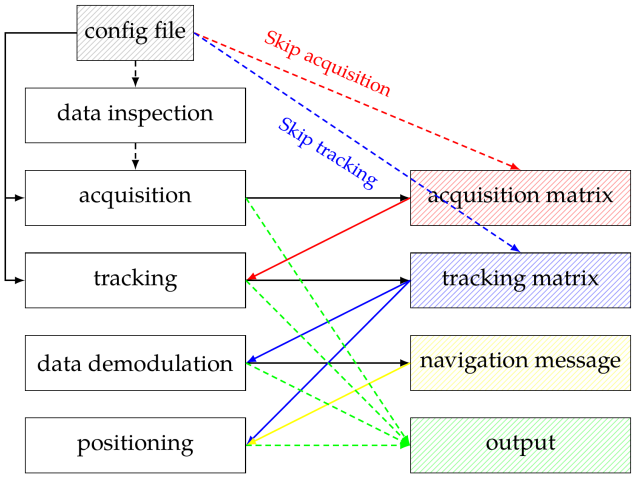


FIGURE 3.3: Block representation of the Python GNSS software receiver.

3.1.3 Construction of the Hardware Testbed

Another important contribution consisted in the integration in a hardware testbed of the required spoofer GNSS receiver and spoofed GNSS signal generators. In order to accomplish this aim, the following equipment has been procured:

- 3x u-blox M8 Timing GNSS Evaluation Kit (EVK-M8T): the kit includes an evaluation unit (GNSS receiver), an USB cable, and an active GPS/global'naja navigacionnaja sputnikovaja sistema (GLONASS)/BeiDou antenna with 3 m cable (see Fig. 3.4);
- 3x Nuand BladeRF x40 Rev. 2: the kit contains a bladeRF x40 (SDR), a USB 3.0 SS cable, and 2x SMA cables (see Fig. 3.5);
- 1x HP ProDesk 400 G4 Desktop Mini PC;
- 1x Google Pixel 3 XL (smartphone);
- 1x Huawei Mate 20 (smartphone).

FIGURE 3.4: U-blox M8 Timing GNSS Evaluation Kit (EVK-M8T).

FIGURE 3.5: Nuand BladeRF x40 Rev. 2.

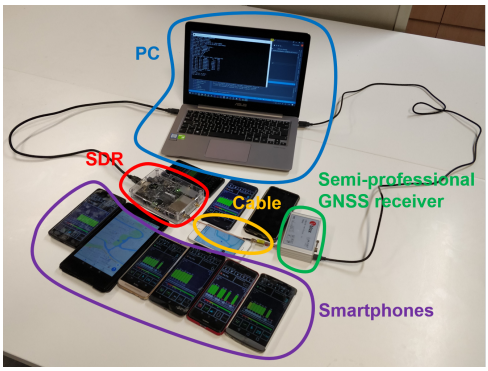


FIGURE 3.6: Testbed setup [61].

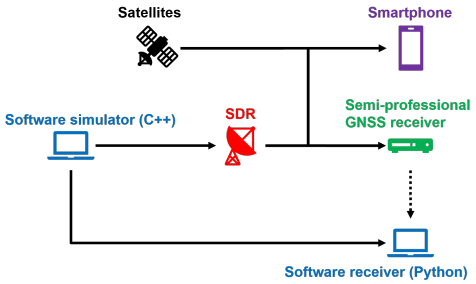


FIGURE 3.7: Testbed configurations.

The overall testbed, composed using the equipment listed above, is shown in Fig. 3.6 and it can be used in different configurations, as shown in Fig. 3.7. A list of all the possible configurations follows:

- Software simulator → Software receiver: the software simulator generates a binary file (containing the simulated RF signal) that is read by the software receiver, which generates some results.
- Software simulator → SDR → GNSS receiver: the software simulator generates a binary file (containing the simulated RF signal) that is sent to the SDR through an USB cable; then, the SDR modulates the baseband RF signal and sends it to the GNSS receiver through a SMA cable; finally, the GNSS receiver sends its results to the PC where they can be visualized through the u-center software installed on the PC.
- Software simulator → SDR → Smartphone: the software simulator generates a binary file (containing the simulated RF signal) that is sent to the SDR through an USB cable; then, the SDR modulates the baseband RF signal and sends it to the smartphone through a SMA cable (by leveraging its non-perfect isolation); finally, the applications running on the smartphone generate some results (for example, the application based on cellular network crosscheck developed within this activity).
- Satellites → GNSS receiver: the GNSS receiver receives the legacy GNSS signals in space, sends its results to the PC where they can be visualized through the u-center software installed on the PC.
- Satellites → Smartphone: the smartphone receives the legacy GNSS signals in space and the applications running on the smartphone generate some results.

3.2 Performance Assessment of SQM Techniques for Anti-Spoofing

3.2.1 SQM Techniques

SQM techniques have long been employed to monitor the GPS correlation peak quality in multipath fading environments and for monitoring of evil waveforms. The interaction between spoofing and authentic signals can affect the correlator output in a way similar to that of multipath components. Therefore, reference [40] 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.

There are various metrics proposed in the literature and, by defining I_{P}, I_{E} and I_{L} are the in-phase value of the promp, early and late SQM correlators, respectively, we consider the following [40], [62]:

- Delta metric:
$$DT = \frac{I_{\mathrm{E}} - I_{\mathrm{L}}}{I_{\mathrm{P}}}\,. \tag{3.1}$$
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.

- Ratio metric:
$$RT = \frac{I_{\mathrm{E}} + I_{\mathrm{L}}}{I_{\mathrm{P}}}\,. \tag{3.2}$$
Similarly to the delta metric, 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 early ratio metric:
$$AERT = \frac{I_{\mathrm{E}}}{I_{\mathrm{P}}}\,. \tag{3.3}$$
This metric is used to detect a flattened or a more pointed correlation peak, by looking to the ratio between an early and the prompt correlation outputs.

- Asymmetric late ratio metric:
$$ALRT = \frac{I_{\mathrm{L}}}{I_{\mathrm{P}}}\,. \tag{3.4}$$
This metric is used to detect a flattened or a more pointed correlation peak, by looking to the ratio between an late and the prompt correlation outputs.

3.2.2 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

$$Y = g(X_1, \ldots, X_N)\,, \tag{3.5}$$

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

$$\begin{aligned} F_Y(y) &= P\left[Y \leq y\right] \\ &= P\left[g(X_1, \ldots, X_N) \leq y\right] \\ &= \iint_D f_{X_1,\ldots,X_N}(x_1, \ldots, x_N) dx_1 \ldots dx_N \,, \end{aligned} \tag{3.6}$$

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

$$f_Y(y) = \frac{dF_Y(y)}{dy} \,. \tag{3.7}$$

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

$$P\left[Y < \gamma_\mathrm{l}\right] = \int_{-\infty}^{\gamma_\mathrm{l}} f_Y(y) dy = P_\mathrm{fa}/2 \,, \tag{3.8}$$

$$P\left[Y > \gamma_\mathrm{u}\right] = \int_{\gamma_\mathrm{u}}^{\infty} f_Y(y) dy = P_\mathrm{fa}/2 \,, \tag{3.9}$$

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.

3.2.3 Spoofing Scenario

Recalling the description of a general model for a spoofing attack in Section 2.4.2.1, we restrict the formulation to a single satellite attack. Therefore, an authentic GNSS signal at the front-end output takes the form

$$r_\mathrm{a}(t) = A_\mathrm{a} D_\mathrm{a}(t - t_{\mathrm{p,a}}) C_\mathrm{a}(t - \tau_\mathrm{a}) \mathrm{e}^{j\left[2\pi(f_\mathrm{IF} + f_{\mathrm{D,a}})t + \phi_\mathrm{a}\right]} \,, \tag{3.10}$$

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

$$r_\mathrm{s}(t) = A_\mathrm{s} D_\mathrm{s}(t - t_{\mathrm{p,s}}) C_\mathrm{s}(t - \tau_\mathrm{s}) \mathrm{e}^{j\left[2\pi(f_\mathrm{IF} + f_{\mathrm{D,s}})t + \phi_\mathrm{s}\right]} \,, \tag{3.11}$$

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

$$r(t) = r_\mathrm{a}(t) + r_\mathrm{s}(t) + n(t) \,. \tag{3.12}$$

The impact of a spoofing attack can be better described deriving the CAF relative to Eq. (3.12) that, extending the result in Eq. (2.10), becomes

$$S = ADR(\Delta\tau)\,\mathrm{sinc}(\Delta f_\mathrm{D} T_\mathrm{coh}) \mathrm{e}^{j\Delta\phi} + A_\mathrm{s} D_\mathrm{s} R_\mathrm{s}(\Delta\tau_\mathrm{s})\,\mathrm{sinc}\left(\Delta f_{\mathrm{D,s}} T_\mathrm{coh}\right) \mathrm{e}^{j\Delta\phi_\mathrm{s}} + \eta \,, \tag{3.13}$$

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 and the victim position.
- The attacker knows the amplitude A_{A}, the code delay τ_{A} and the Doppler frequency $f_{D,\mathrm{A}}$ of the authentic signal at the receiver, but the authentic phase ϕ_{A} is unknown to him.

  In order to formalize this assumption, the spoofer estimates the authentic signal that is received by the victim receiver as

$$\tilde{r}_{\mathrm{a}}(t) = A_{\mathrm{a}} D_{\mathrm{a}}(t - t_{\mathrm{p,a}}) C_{\mathrm{a}}(t - \tau_{\mathrm{a}}) \mathrm{e}^{j\left[2\pi(f_{\mathrm{IF}} + f_{\mathrm{D,a}})t + \tilde{\phi}_{\mathrm{a}}\right]} + n_{\mathrm{a}}(t)\,, \tag{3.14}$$

  where

$$\tilde{\phi}_{\mathrm{a}} = \sim \mathcal{U}([0, 2\pi])\,, \qquad \text{if the authentic phase is unknown}\,, \tag{3.15}$$

  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.

The SQM techniques will be tested against the following three types of attack.

Trivial attack This attack considers the transmission of the signal of Eq. (3.11) with

$$C_{\mathrm{s}} = C_{\mathrm{a}}\,, \tag{3.16}$$

$$\phi_{\mathrm{s}} = \begin{cases} \phi_{\mathrm{a}}\,, & \text{if the authentic phase is known}\,, \\ \sim \mathcal{U}([0, 2\pi])\,, & \text{if the phase authentic is unknown}\,, \end{cases} \tag{3.17}$$

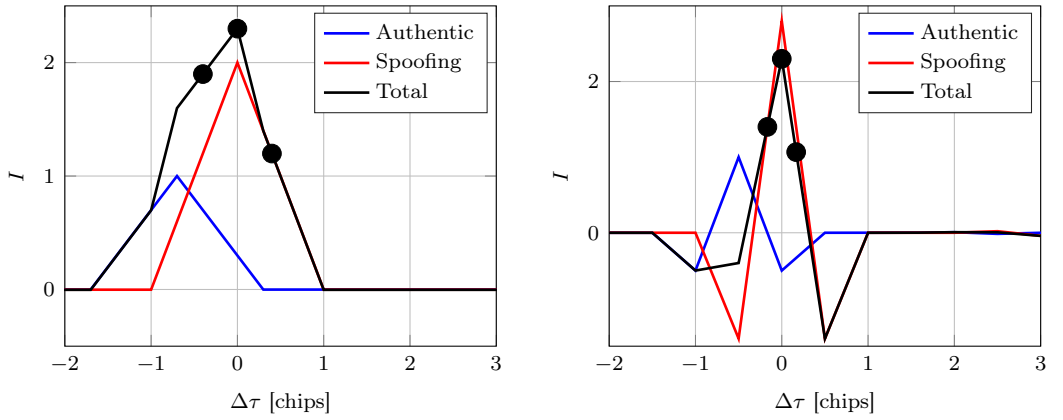
that is a signal with the same PRN code as the authentic signal.
An example of this attack in given in Fig. 3.8 for a GPS and a Galileo signal. It represents a snapshot of the in-phase correlator function of authentic, spoofing and total signal during the lift-off phase of the attack. As can be seen, early, late and prompt correlators assume a relative abnormal position with respect to that of an authentic signal in Fig. 2.6. Signal quality monitoring techniques leverage this abnormality to detect the spoofing attack, as we will se in the next section.

Nulling attack An attack that is able to achieve optimal results against the signal quality monitoring techniques described above is the nulling. In a nutshell, this attack 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

$$r_{\mathrm{s}}(t) = \bar{r}(t) - \tilde{r}_{\mathrm{a}}(t)\,, \tag{3.18}$$



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

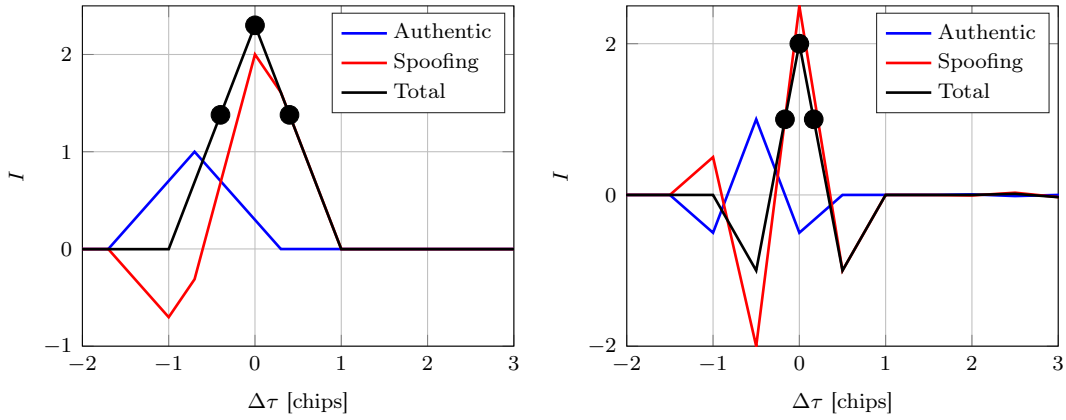
(B) BOC(1,1) signal. Correlator spacing $d = 0.33$. Authentic code delay $\tau_a = -0.5$.

FIGURE 3.8: 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.

where

$$\bar{r}(t) = AD(t - t_p)C_a(t - \tau)e^{j[2\pi(f_{IF}+f_D)t+\phi]}, \tag{3.19}$$

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. 3.9 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.

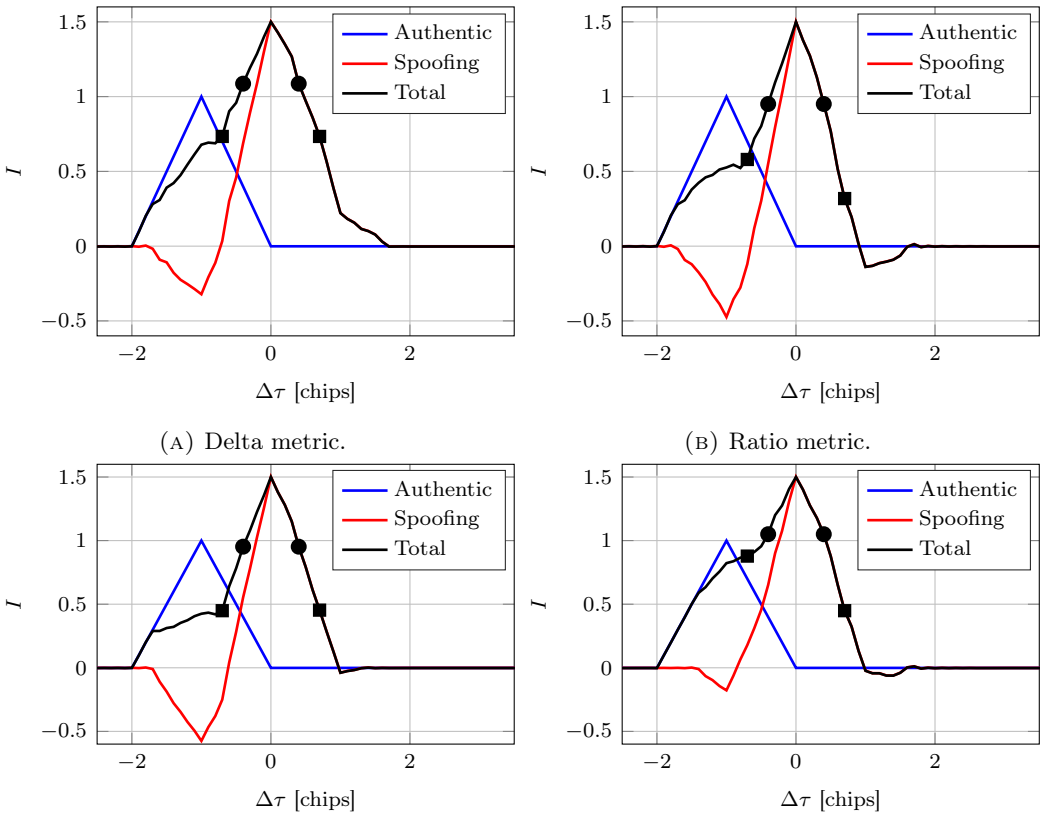


(A) BPSK(1) signal. Correlator spacing $d = 0.8$. Authentic code delay $\tau_a = -0.7$.

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

FIGURE 3.9: 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.

Energy optimal attack The attacker sends a spoofing signal with the minimum energy such that the total (authentic + spoofing) signal at the receiver is "trackable" and which generates a SQM metric value as close as possible to that of an authentic signal. The mathematical formulation of this attack is described in [63]. An example of this attack is shown in Fig. 3.10.



(A) Delta metric.

(B) Ratio metric.

(C) Asymmetric early ratio metric.

(D) Asymmetric late ratio metric.

FIGURE 3.10: Authentic, spoofing and total correlation function during a snapshot of the optimal attack with default parameters (BPSK(1,1) signal).

3.2.4 Performance of SQM Techniques via MATLAB Simulations

The performance the SQM techniques against the considered attacks have been evaluated for different values of authentic C/N_0 and τ_{A}, by means of MATLAB simulations with the following parameters:

- Attempts: 10^4,
- DLL correlator spacing: 0.8 chips,
- SQM correlator spacing: 1.4 chips.

The performance evaluation of the defense has been done in terms of probability of false alarm and probability of detection. In particular, in order to take into account the fact that the attacker ignores the authentic phase, the probability of detection for a given τ_{A} has been computed as the mean of the probabilities of detection derived by setting $\phi_{\mathrm{A}} = 0, \pi/16, \ldots, 15/16\pi, \pi$, while keeping fixed the phase of the spoofing signal.

In Figs. 3.11 to 3.14 the probability of detection is represented as a function of τ_{A} for a probability of false alarm of 10^{-3} and for the different SQM metrics. Several considerations can be made:

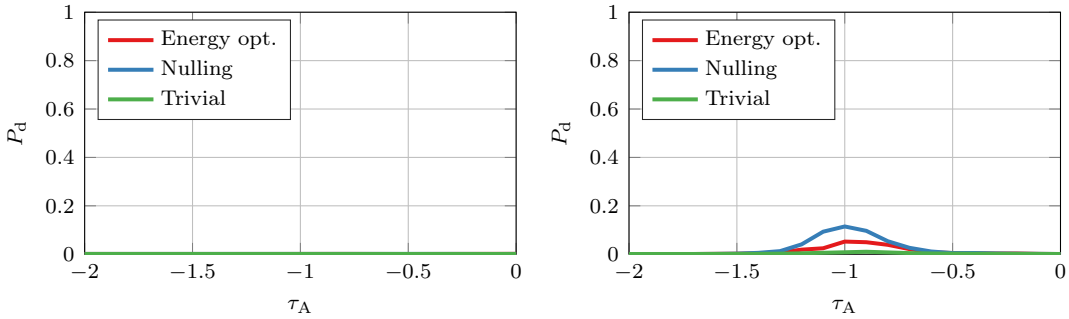
- As C/N_0 increases, the probability of detection increases as well for all the metrics. In particular, for $C/N_0 = 25$ dB/Hz the defense does not work at all, while acceptable performance can be reached for $C/N_0 = 55$ dB/Hz, although it is a quite unrealistic value for a terrestrial receiver.

- The performance for different τ_{A} depends on how much the SQM correlators are affected by the spoofing signal. For example, for $\tau_{\mathrm{A}} = -2$ chip the probability of detection is negligible, since the SQM correlators "see" only the spoofing signal and the authentic signal does not affect anymore the two correlators. Similar performance happens for $\tau_{\mathrm{A}} = 0$ chip, since, in this case, the attacker is not imposing a false PVT and the total signal has the same "shape" of an authentic one.

- The performance of the different metrics are, in general, different. However, while the delta metric has the worst performance, the three ratio metrics have comparable performance instead.

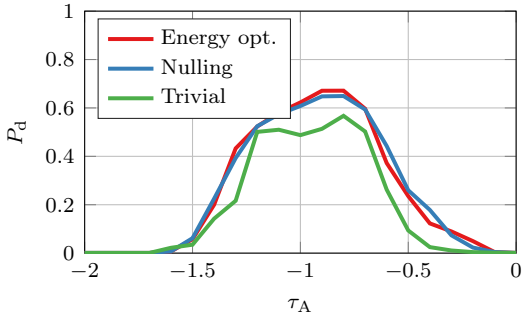
- From this limited analysis, it seems there is no pattern in when an attack performs better than another. This is likely due to the fact that the attacker does not know the phase of the authentic signal, therefore nulling and energy optimal attacks are not able to properly "delete" the authentic signal. As a consequence, they perform similarly to the trivial attack.

In Fig. 3.15 four receiver operating characteristic (ROC) are represented, one for each metric. Each ROC is derived using $\tau_{\mathrm{A}} = -1$ chip, that is the instant in which the probability of detection is, in general, the highest (as can be noted from Figs. 3.11 to 3.14). From these plots we can only confirm that no attack seems to be more powerful than the other two.

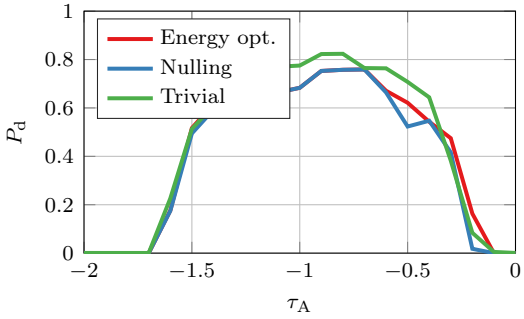


(A) $C/N_0 = 25$ dB/Hz.

(B) $C/N_0 = 35$ dB/Hz.

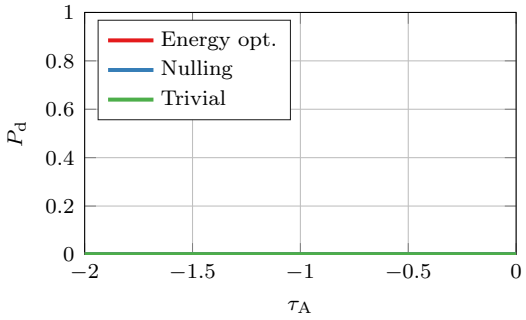


(C) $C/N_0 = 45$ dB/Hz.

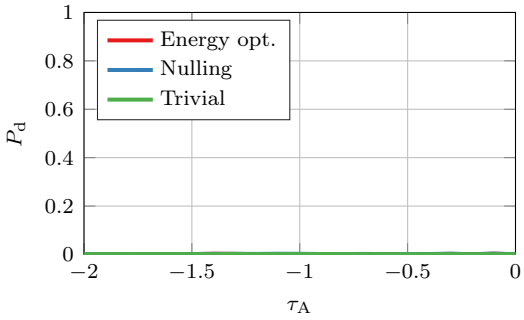


(D) $C/N_0 = 55$ dB/Hz.

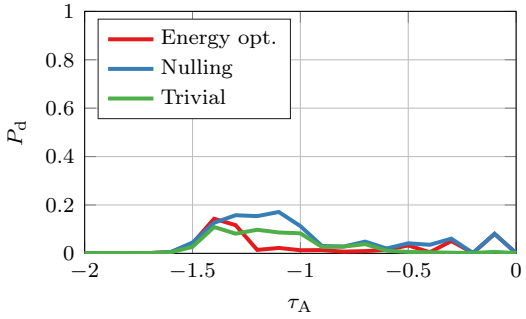
FIGURE 3.11: Probability of detection using the ratio metric as a function of τ_A for a probability of false alarm of 10^{-3}.



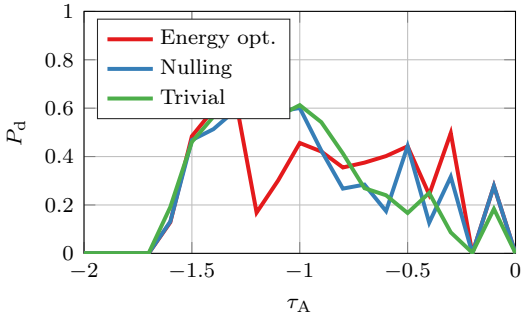
(A) $C/N_0 = 25$ dB/Hz.



(B) $C/N_0 = 35$ dB/Hz.

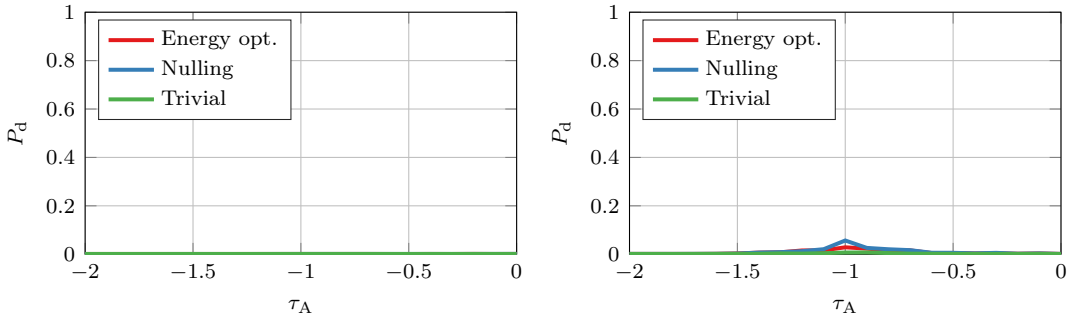


(C) $C/N_0 = 45$ dB/Hz.

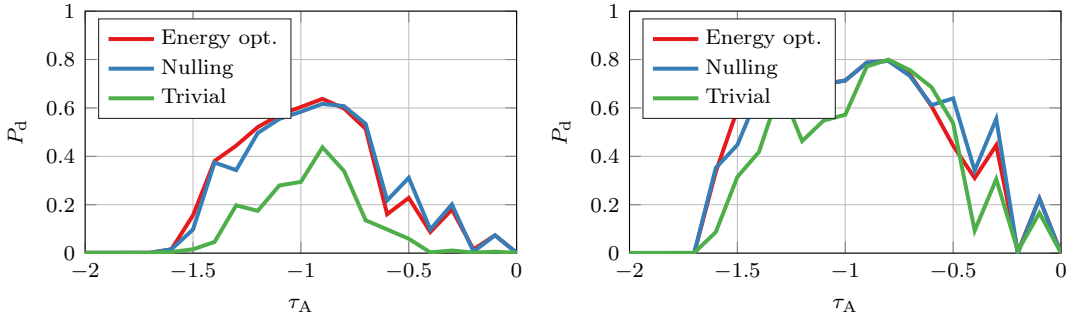


(D) $C/N_0 = 55$ dB/Hz.

FIGURE 3.12: Probability of detection using the delta metric as a function of τ_A for a probability of false alarm of 10^{-3}.

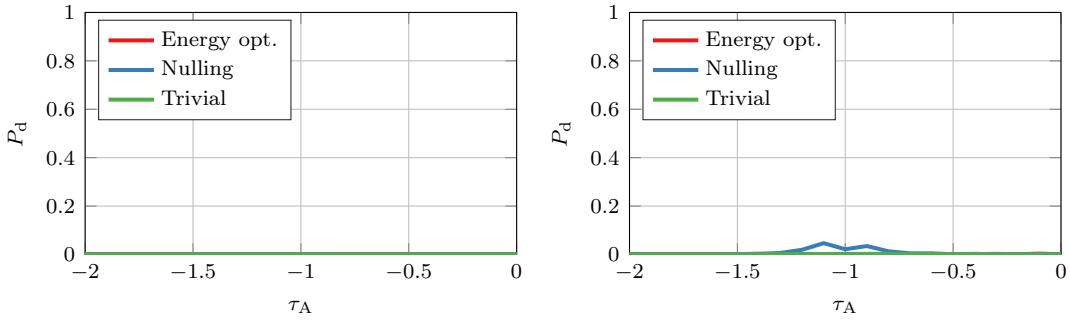


(A) $C/N_0 = 25$ dB/Hz. (B) $C/N_0 = 35$ dB/Hz.

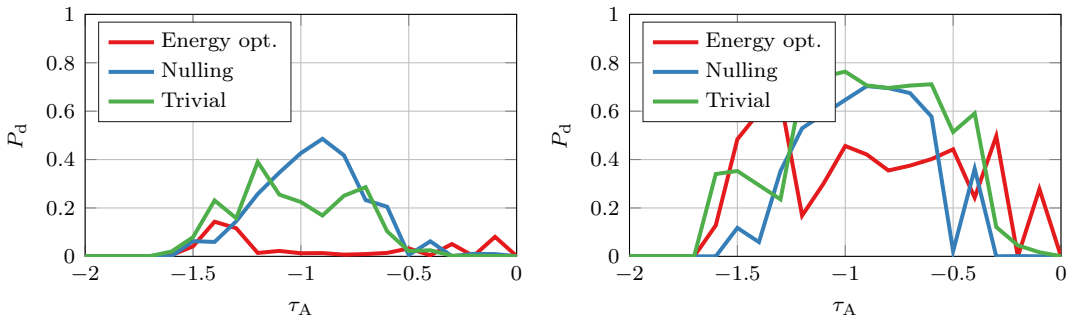


(C) $C/N_0 = 45$ dB/Hz. (D) $C/N_0 = 55$ dB/Hz.

FIGURE 3.13: Probability of detection using the asymmetric early ratio metric as a function of τ_A for a probability of false alarm of 10^{-3}.

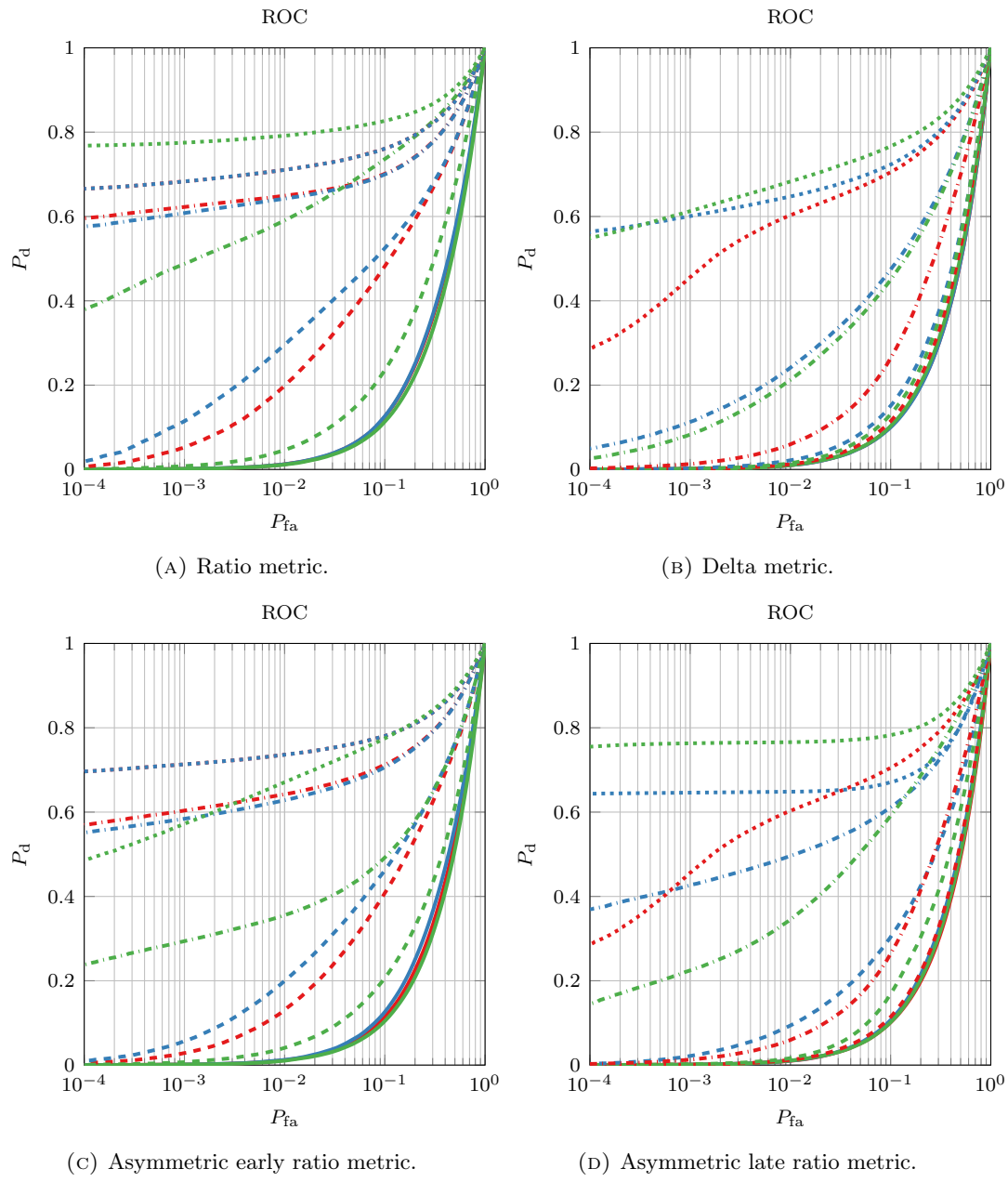


(A) $C/N_0 = 25$ dB/Hz. (B) $C/N_0 = 35$ dB/Hz.



(C) $C/N_0 = 45$ dB/Hz. (D) $C/N_0 = 55$ dB/Hz.

FIGURE 3.14: Probability of detection using the asymmetric late ratio metric as a function of τ_A for a probability of false alarm of 10^{-3}.



(A) Ratio metric.

(B) Delta metric.

(C) Asymmetric early ratio metric.

(D) Asymmetric late ratio metric.

FIGURE 3.15: ROC for different authentic C/N_0 and $\tau_A = -1$ chip.

3.2.5 Performance of SQM Techniques Implemented in the Software Receiver

The performance assessment of the SQM techniques in the software receiver is performed using the following simulator and receiver settings:

- **Simulator**: scenario of duration 20 s, sampling frequency of $F_s = 4$ MHz, AWGN enabled with $C/N_0 = 35$, 40, 45 dB-Hz, static spoofing attack where the authentic pseudorange is delayed of $\Delta\tau = 0.1, 0.2, \ldots, 2$ chips.
- **Receiver**: SQM technique enabled (1.4 chip early-late correlator spacing for GPS and 0.5 chip for Galileo) and a desired probability of false alarm of 10^{-2}.

Each simulation outputs 20000 metric values for GPS and 5000 for Galileo.

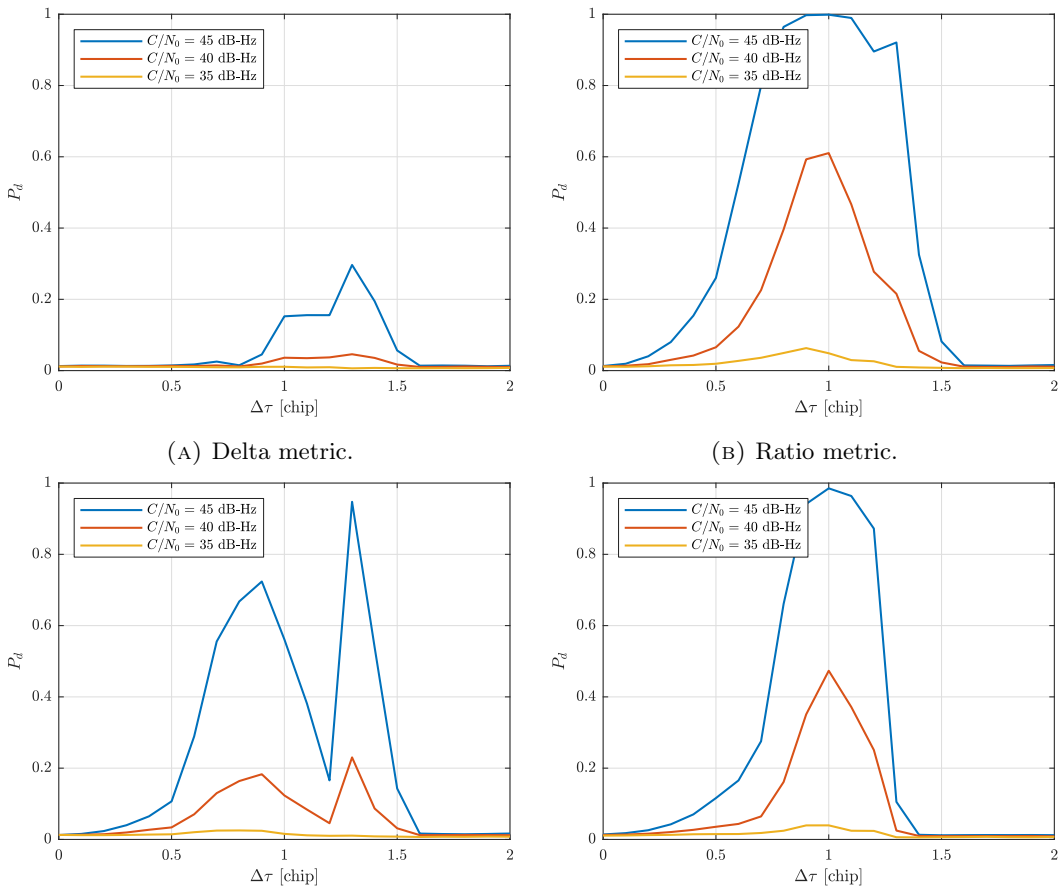
The performance of the SQM techniques is reported in Fig. 3.16 (GPS) and in Fig. 3.17 (Galileo) for all the four metrics for a single satellite. As expected, a common behavior between GPS and Galileo is that the probability of detection P_d increases with C/N_0.

For what concern the GPS scenario, the performance is different for the various metrics: the delta metric performs poorly, while the other three metrics reach a good probability of detection for at least a value of $\Delta\tau$ when $C/N_0 = 45$ dB-Hz. Moreover, as shown in Table 3.1, the empirical probability of false alarm is close to the desired one for all C/N_0 and SQM metrics.

Also for what concern the Galileo scenario, the performance is different for the various metrics; however, in this case all the four metrics reach a good probability of detection for at least a value of $\Delta\tau$ when $C/N_0 = 45$ dB-Hz. Moreover, as shown in Table 3.2, the empirical probability of false alarm is close to the desired one for all C/N_0 and SQM metrics.

TABLE 3.1: Probability of false alarm for different C/N_0 and SQM metrics in the GPS scenario.

C/N_0	Metric			
	DT	RT	AERT	ALRT
35 dB-Hz	$1.02 \cdot 10^{-2}$	$1.01 \cdot 10^{-2}$	$1.12 \cdot 10^{-2}$	$0.95 \cdot 10^{-2}$
40 dB-Hz	$1.08 \cdot 10^{-2}$	$1.05 \cdot 10^{-2}$	$1.12 \cdot 10^{-2}$	$1.14 \cdot 10^{-2}$
45 dB-Hz	$1.18 \cdot 10^{-2}$	$1.16 \cdot 10^{-2}$	$1.12 \cdot 10^{-2}$	$1.29 \cdot 10^{-2}$



(A) Delta metric.

(B) Ratio metric.

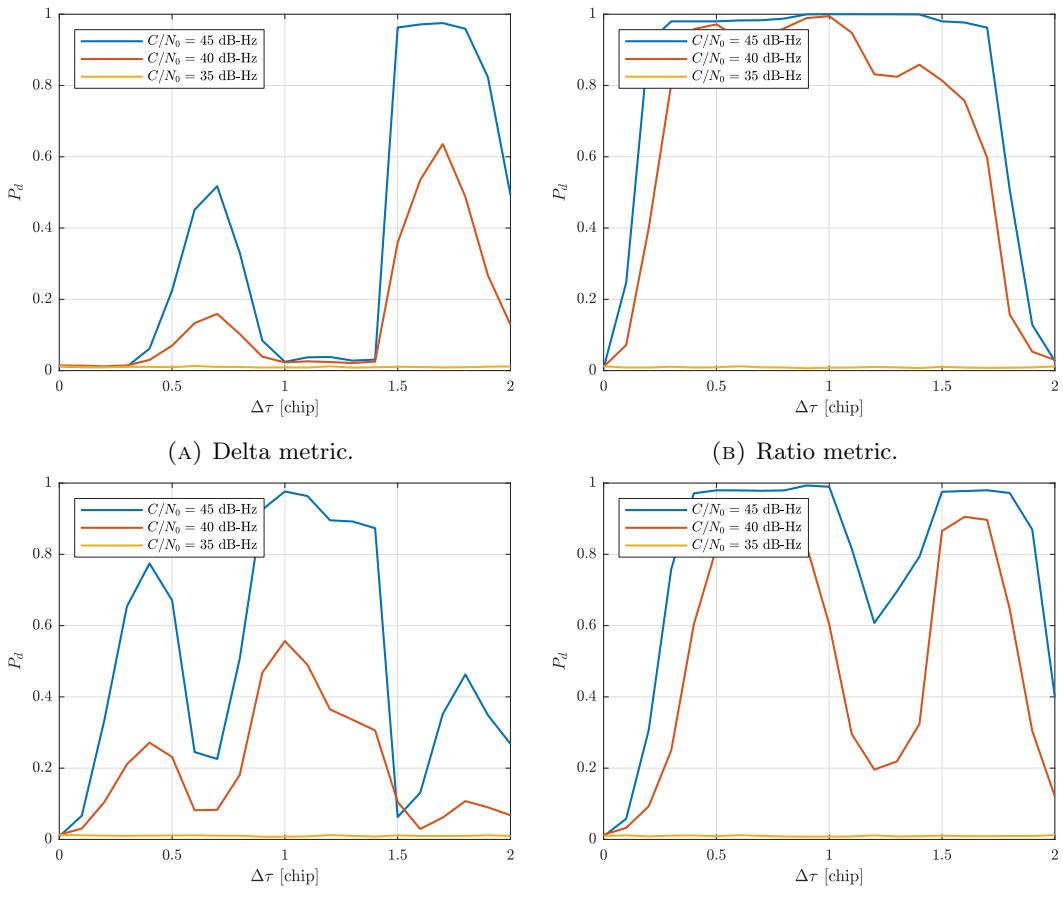
(C) Asymmetric early ratio metric.

(D) Asymmetric late ratio metric.

FIGURE 3.16: Probability of detection as a function of the difference between authentic and spoofing pseudorange for different C/N_0 in the GPS scenario.

TABLE 3.2: Probability of false alarm for different C/N_0 and SQM metrics in the Galileo scenario.

C/N_0	Metric			
	DT	RT	AERT	ALRT
35 dB-Hz	$1.2 \cdot 10^{-2}$	$1.2 \cdot 10^{-2}$	$1.24 \cdot 10^{-2}$	$0.98 \cdot 10^{-2}$
40 dB-Hz	$1.08 \cdot 10^{-2}$	$1.46 \cdot 10^{-2}$	$1.32 \cdot 10^{-2}$	$1.32 \cdot 10^{-2}$
45 dB-Hz	$0.72 \cdot 10^{-2}$	$1.26 \cdot 10^{-2}$	$0.84 \cdot 10^{-2}$	$0.86 \cdot 10^{-2}$



(A) Delta metric.

(B) Ratio metric.

(C) Asymmetric early ratio metric.

(D) Asymmetric late ratio metric.

FIGURE 3.17: Probability of detection as a function of the difference between authentic and spoofing pseudorange for different C/N_0 in the Galileo scenario.

3.3 Notch Filter Implementation in the Software Receiver

3.3.1 Algorithm Description

The implementation of the adaptive notch filter in the software receiver follows the design proposed in [11]. A brief description of the working principle of the filter follows.

The transfer function of the notch filter is given by

$$H(z) = \frac{1 - z_0 z^{-1}}{1 - k_\alpha z_0 z^{-1}}\,, \tag{3.20}$$

where k_α is the pole contraction factor, that assumes values in the range $[0, 1)$ and controls the frequency notch width ($B_{3\text{dB}} \approx \frac{(1-k_\alpha)\pi}{10T_\text{s}}$), and

$$z_0 = \mathrm{e}^{j2\pi f_0 T_\text{s}}\,, \tag{3.21}$$

with f_0 the center frequency of the notch, that is the rejected frequency, and T_s the signal sampling time. The input/output filter equations corresponding to Eq. (3.20) are

$$x_\text{r}[n] = (1 - k_\alpha)x[n] + k_\alpha z_0[n] x_\text{r}[n-1]\,, \tag{3.22}$$

$$y[n] = x[n] + z_0[n] x_\text{r}[n-1]\,, \tag{3.23}$$

where $x_\text{r}[n]$ and $y[n]$ are the output of the autoregressive (AR) unit and the final output of the filter respectively. The block diagram representation of the above notch filter is given in Fig. 3.18. Since the frequency to be rejected is unknown and varies along the time, the adaptation block is necessary to estimate z_0 at run-time.

The adaptation block is based on the principle of minimizing the instantaneous energy of the filter output and its block scheme is reported in Fig. 3.19. The input carrier signal $x[n]$ is first multiplied by $i^*[n-1]$, a delayed and complex conjugated version of the locally estimated carrier signal. The mixing gives x_B, a baseband version of the input signal, that is phase differentiated to produce an estimate of the instantaneous frequency. Then, there are the discrimination rule to produce the instantaneous frequency error, the frequency update rule and the NCO that generates the next sample of the local carrier signal $i^*[n]$.

The frequency update rule derives from the plain gradient (PG) algorithm, which consists in an iterative search of the optimum $f_0[n]$ in the form

$$f_0[n] = f_0[n-1] - \mu \cdot g[n]\,, \tag{3.24}$$

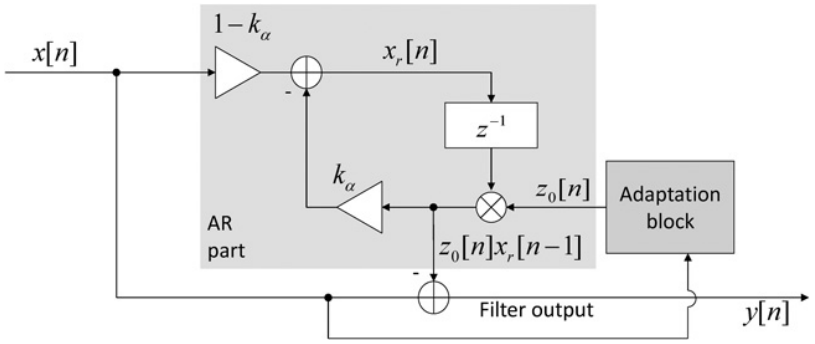


FIGURE 3.18: Structure of the adaptive notch filter [64].

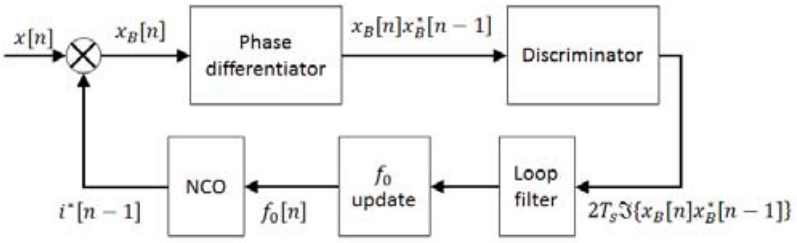


FIGURE 3.19: High-level block diagram of the standard FLL used for the adaptation block [11].

where μ is the adaptation step and $g[n]$ is the stochastic gradient of the cost function to be minimized. In particular, the adaptation step can be properly determined using the modified controlled-root formulation, as a function of the well-known loop bandwidth [65], while the stochastic gradient corresponds to the opposite of the discriminator output:

$$g[n] = -2T_\mathrm{s}\,\mathrm{Im}\left\{x_\mathrm{B}[n]x_\mathrm{B}^*[n-1]\right\}\,, \tag{3.25}$$

where $\mathrm{Im}\{\cdot\}$ indicates the imaginary part.

3.3.2 Validation

The validation of the implementation of the notch filter in the software receiver is performed using the following simulator and receiver settings:

- **Simulator**: scenario of duration 17 s, sampling frequency of $F_\mathrm{s} = 4$ MHz, $C/N_0 = 45$ dB-Hz, deterministic step jamming mode with 1 ms between frequency steps, and jamming bandwidth of 4 MHz ($f_\mathrm{c} - 2\,\mathrm{MHz} \leq f_\mathrm{J} \leq f_\mathrm{c} + 2\,\mathrm{MHz}$, with f_J jamming frequency and f_c carrier frequency).
- **Receiver**: first order frequency locked loop block for tracking the jamming frequency (loop bandwidth of $B_n = 1$ MHz) and pole contraction factor of the notch filter of $k_\alpha = 0.95$.

The time between frequency steps has been chosen an order of magnitude below the 0.01 s that the SDR of our testbed is capable of reproducing (from an hardware point of view), as proved by an experiment about the compatibility between the software simulator developed by our research group and our SDR described in Appendix C.

The performance of the FLL is well represented in Fig. 3.20 where the frequency generated by the simulator and the frequency estimated by the FLL are shown for 2 ms of signal. As we can see, the tracked frequency reaches the true frequency in about 0.2 ms.

On the other hand, the performance of the notch filter itself for two SVs are shown in Fig. 3.21 in terms of mean C/N_0 discrepancy, defined as:

$$\Delta C/N_0 = \frac{1}{N}\sum_{i=1}^{N}(C/N_0(i))_\mathrm{clean} - \frac{1}{N}\sum_{i=1}^{N}(C/N_0(i))_\mathrm{jamm}\,, \tag{3.26}$$

where N is the number of computed C/N_0 during the generated scenario ($N = 170$ in these simulations), $(C/N_0(i))_\mathrm{jamm}$ is the i-th estimated C/N_0 of the jammed signal, and $(C/N_0(i))_\mathrm{clean}$ is the i-th estimated C/N_0 of the clean signal. The mean C/N_0

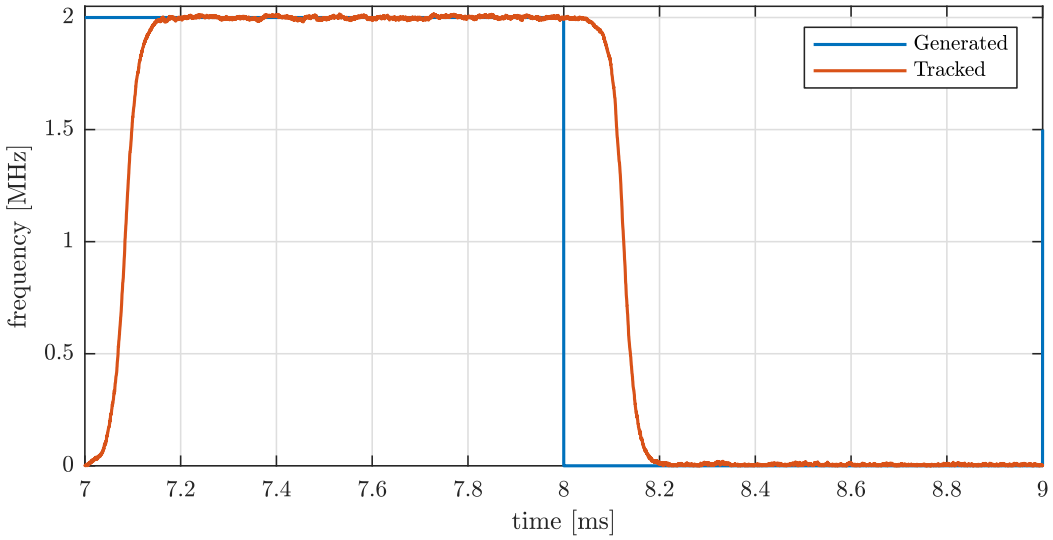


FIGURE 3.20: Frequency generated by the simulator and frequency tracked by the FLL of the notch filter for a frequency step of 2 MHz.

discrepancy is plotted as a function of the jamming to signal ratio (J/S), which is defined as the ratio between the jamming power and the signal power of a certain satellite at the receiver antenna. The result is shown for different satellites and for both notch-filtered and non-filtered signals. We can notice that the non-filtered signals are not acquired for J/S above 22 or 24 dB. Instead, for low J/S the filtered signals perform worse than the non-filtered ones, while for high J/S they are still acquired and tracked with a C/N_0 from 4 to 8 dB worse than that of the clean signal. Moreover, we can notice that, even if the two SVs have the same C/N_0 at the receiver, they show different results as the jamming power increases. One possible explanation is that the two signals have a different Doppler frequency, therefore the random hopping jamming signal impacts the two SVs in a different way, and this could lead to a significant difference between the carrier-to-noise ratios.

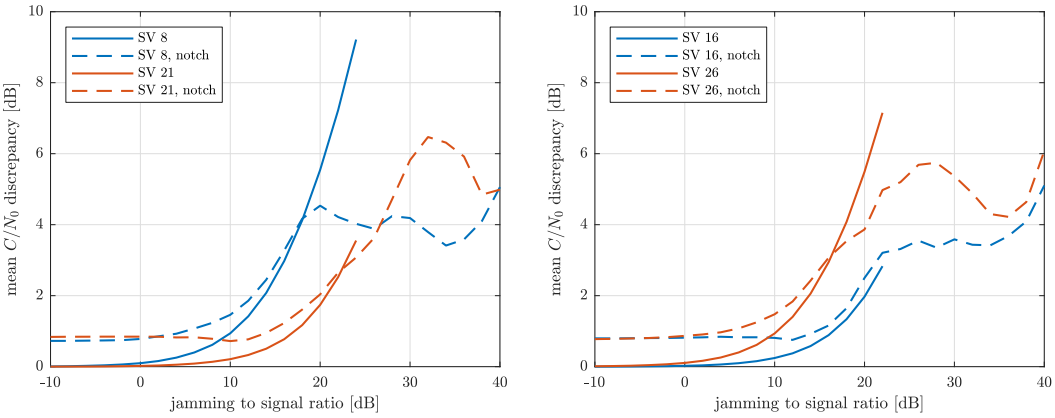


FIGURE 3.21: Mean C/N_0 discrepancy between the signal without filter and the signal with filter as a function of the jamming to signal ratio. The solid lines are for the non-filtered signals, the dashed line for the notch-filtered ones. The different colors are for the different satellites.

Another measure of performance of the notch filter is the root mean squared error (RMSE) of Doppler frequency and code delay estimates, defined as:

$$\mathrm{RMSE}_{f_\mathrm{D}} = \sqrt{\frac{1}{M}\sum_{i=1}^{M}\left[(f_\mathrm{D}(i))_\mathrm{jamm} - (f_\mathrm{D}(i))_\mathrm{clean}\right]^2}, \tag{3.27}$$

$$\mathrm{RMSE}_{\tau} = \sqrt{\frac{1}{M}\sum_{i=1}^{M}\left[(\tau(i))_\mathrm{jamm} - (\tau(i))_\mathrm{clean}\right]^2}, \tag{3.28}$$

where M is the number of computed Doppler frequencies/code delays during the generated scenario ($M = 17000$ in these simulations), $(f_\mathrm{D}(i))_\mathrm{jamm}$ is the i-th Doppler frequency of the jammed signal, $(f_\mathrm{D}(i))_\mathrm{clean}$ is the i-th Doppler frequency of the clean signal, $(\tau(i))_\mathrm{jamm}$ is the i-th code delay of the jammed signal, and $(\tau(i))_\mathrm{clean}$ is the i-th code delay of the clean signal. The results are shown in Fig. 3.22 and Fig. 3.23, respectively for Doppler frequency and code delay. For what concern the RMSE of Doppler frequency, it reflects the results of the mean C/N_0 discrepancy. However, the RMSE of the code delay has a different trend: for $J/S < 5\,\mathrm{dB}$ it is constant, then it decreases for $5\,\mathrm{dB} \leq J/S < 14\,\mathrm{dB}$, then it keeps increasing. In the first interval the filter does not correctly identify the jamming frequency and so it deletes the signal around the central frequency; as the J/S increases over 5 dB, the filter becomes increasingly effective in tracking the jamming frequency, deleting the corresponding jamming signal; finally, in the last interval the RMSE increases again due to the increasing jamming power.

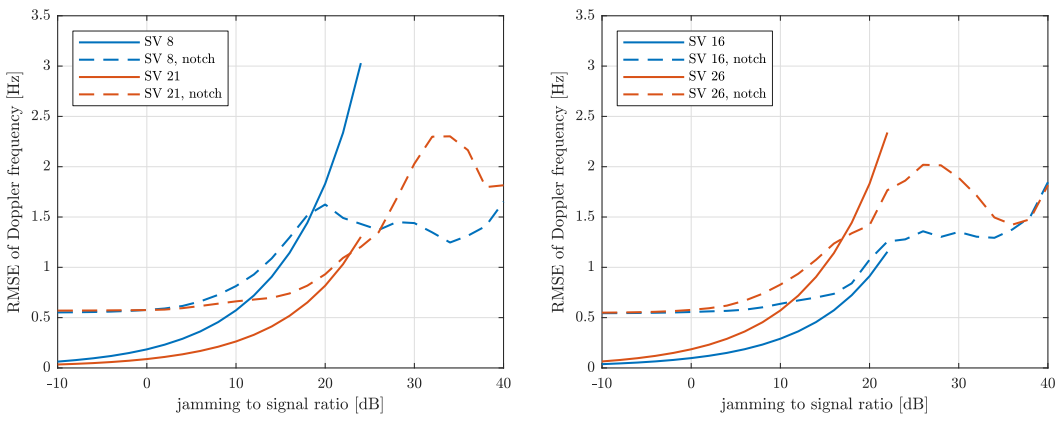


FIGURE 3.22: RMSE of Doppler frequency estimate as a function of the jamming to signal ratio. The solid lines are for the non-filtered signals, the dashed line for the notch-filtered ones. The different colors are for the different satellites.

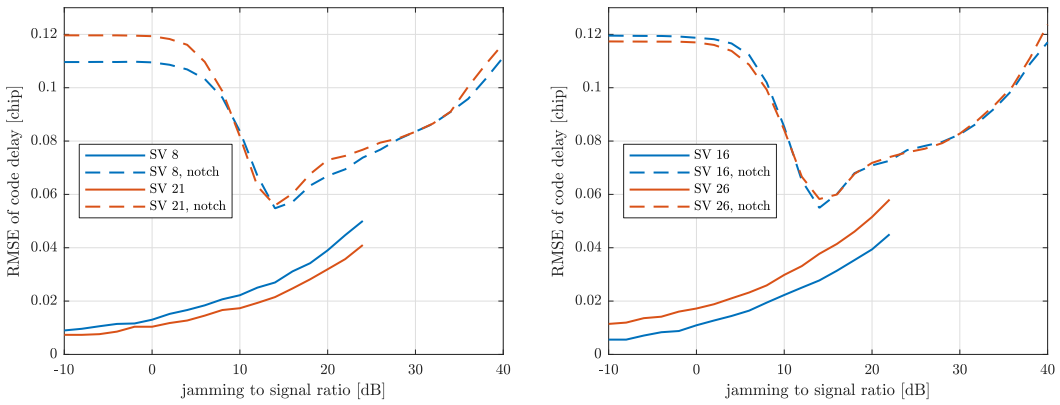


FIGURE 3.23: RMSE of code delay estimate as a function of the jamming to signal ratio. The solid lines are for the non-filtered signals, the dashed line for the notch-filtered ones. The different colors are for the different satellites.

Chapter 4

Detection of GNSS Spoofing by a Receiver in Space

4.1 Introduction

Satellites play a relevant role in several areas, such as communication, early warning systems, global broadcasting, meteorology, navigation, reconnaissance, remote sensing, and surveillance. Their services cover almost every sector, from mobile cellular communication to telemedicine, and as a consequence any interference with them could have a serious impact on the final user. Their services are a strategic asset for any country, therefore they are privileged targets for possible attacks. For this reason, new requirements are emerging aiming at optimizing physical and mechanical constraints, cost, consumption, performance, robustness, and assurance. They mainly refer to the need of reducing mass, dimensions, costs, and power consumption, performing positioning in limited visibility conditions and by leveraging multi constellation, performing positioning with very low signal power (e.g., geostationary orbit scenario or lunar missions), interoperability between different GNSSs, enhancing trust and robustness, given that intentional and unintentional interferences can easily reach space vehicle eventually compromising the onboard PVT service.

Discussions of cyber threats to critical national infrastructure often overlook the vulnerability of satellites and other space assets to cyberattack [66]. This represents a significant failing due to the society's substantial and ever increasing reliance on satellite technologies as already pointed out. Apart from in some high-end space-based systems, vulnerabilities at the junction of space-based or space-derived capability with cybersecurity cause major national, regional, and international security concerns, yet are going unaddressed. To understand this non-traditional evolving security threat it is necessary to analyse the intersection between cyber and space security. Cybersecurity and space security are inevitably linked. In this context, technologies in satellites and other space assets born from a broad international supply base and consequently require regular security upgrades. These upgrades by means of remote connections could serve to make space assets vulnerable to cyberattacks. Nowadays, satellites are normally used to provide internet services and GNSS technologies which are increasingly embedded in almost all critical infrastructure.

As a matter of fact, from a security perspective, much attention has been given to ground applications, whereas few requirements are considered for the protection and enhancement of robustness of space based GNSS receivers, that is the scenario considered in this Chapter. GNSS systems are typically vulnerable due to the fact that they have not been designed with security provisions, and only recently some systems, e.g. the European Galileo, are introducing cryptographic authentication and integrity protection mechanisms. The common unjustified assumption is that risk of space based threats is low or even negligible. However, several examples contradicting

this conclusion can be found. In a maritime setup, space-based monitoring systems could be being jammed or spoofed by vessel operators that would want to falsify their information to conceal their illegal activities. More in general, the huge amount of data spread through satellites makes it easy to impair accuracy and reliability with a low probability of detection. Particularly, integrity checks involving large amounts of data transferred between interested parties are needed.

Therefore, now more than ever, space applications need secure GNSS services. Space systems are critical infrastructures where the position, navigation and timing are required to be robust and authenticated, and threats may come either from attackers on ground or in space. While military satellites already carry on board GNSS receivers equipped with security modules for the encrypted signal, signal authenticity and integrity will be an important feature for commercial and civil missions, too. Indeed, satellites are normally used to provide internet services and GNSS technologies which are increasingly embedded in almost all critical infrastructure.

Recently, research has focused on GNSS interference countermeasures and several works have been published [67]. However, current spoofing countermeasure techniques refer to scenarios in which the target receiver is placed on the ground, e.g., by using signals of opportunity and side information from other measurements systems. The novelty in our work is to consider GNSS receivers in space, aboard low Earth orbit (LEO), medium Earth orbit (MEO) or geostationary Earth orbit (GEO) satellites and investigate how existing and proposed spoofing countermeasures can be adapted to such receivers considering the constraints and limitations, but also the opportunities coming from the different scenario.

The rationale of the work described in this Chapter is based on the fact that the trajectory of the receiver in space is generally stable and predictable, the trajectories of GNSS satellites, and the parameters and characteristics of GNSS signals are publicly known or at least predictable, and therefore the features of the received GNSS signal can be leveraged to design consistency checks. Among them, some of the most common parameters are the carrier-to-noise ratio (C/N_0) and the received power. Indeed, the C/N_0 and the range of values of the GNSS power are partially predictable. Abnormal values can be considered as warning that there may be something wrong. Moreover, GNSS satellites follow orbits that are known to the receiver and that can be related to the current estimated receiver position. Indeed, by means of a model for orbit prediction the receiver should be able to estimate its orbit and, consequently, the expected power and the C/N_0. In this context, the purpose of this Chapter is to provide a statistical analysis and develop these consistency checks. Moreover, GNSS satellites follow visibility patterns and therefore the presence of a satellite in a space position that is not expected can be seen as a suspicious. Therefore, the receiver might compare its orbit with the PVT information and infer whether a satellite should be present in each orbit's point or not. Also in this case this consistency check is related to the received power at a given position.

The approach described in this Chapter has been implemented and tested in the frame of the ENSPACE demonstrator (H2020-GALILEO-GSA-2017, Grant Agreement Nr. 776405). The aim of the ENSPACE project is to develop innovative software suites for enhanced navigation, positioning and time in space with the following objectives: (i) become a reference product for navigation, positioning and time in space for different missions that require low cost, security and a flexible software solution, and (ii) become a reference product for existing high-grade space applications that can be added to enhance security. With this target, the main drivers have been the design and development of a product with the following cutting edge features: multi applications, multi mission, low cost, secure and robust, and fully software solution. In [68], the

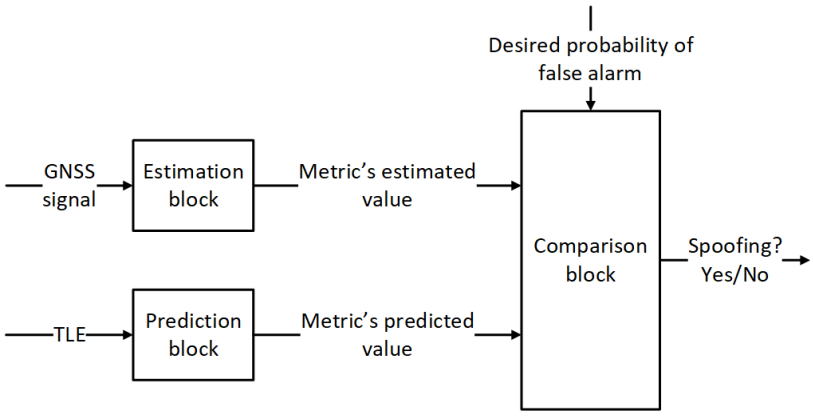


FIGURE 4.1: General block scheme considered for the consistency checks.

implementation of the snapshot processing technique, that is one of the processing modes supported by the ENSPACE demonstrator, has been presented.

The Chapter is organized as follows. Section 4.2 provides the statistical analysis and the design scheme for each consistency metric check. In Section 4.3, the fusion technique used to merge the soft outputs of the consistency checks is presented. Section 4.4 shows the results obtained by means of simulations. Finally, Section 4.5 concludes the Chapter and discuss some future perspective.

4.2 Consistency Checks Scheme

First of all, it is worth noting that even if these checks cannot be considered as cryptographic integrity protection anti-spoofing procedures, they can be seen as flags stating that an attack may be in place. The generic block scheme considered for the consistency checks is reported in Fig. 4.1. Since the development of the algorithm for each consistency check required an estimation module and used the same orbit prediction model to compute the metric's expected value, a brief introduction on the estimation theory and the orbit prediction model, i.e., simplified general perturbations 4 (SGP4) model, used for our evaluations follows.

The aim of the estimation block is to return an estimate of a certain parameter given a number of observations. Let $\mathbf{Y}$ be a random vector of dimension N, whose components are Y_i, $i = 1, ..., N$, and $\mathbf{y}$ the vector containing the observations, y_i, $i = 1, ..., N$, the problem of parameter estimation can be formalized in the following way. It is assigned a family of probability density functions to $\mathbf{Y}$, $p_{\mathbf{Y}}(\mathbf{y}|\boldsymbol{\theta})$, parameterized by an unknown vector $\boldsymbol{\theta} \in \boldsymbol{\Theta} \subseteq \mathbb{R}^M$. In the case of discrete random variables:

$$P\left(\mathbf{Y} = \mathbf{y}|\boldsymbol{\theta}\right) = p_{\mathbf{Y}}\left(\mathbf{y}|\boldsymbol{\theta}\right) \tag{4.1}$$

The objective of parameter estimation is to use the realizations of $\mathbf{Y}$ to determine the value of $\boldsymbol{\theta}$. In particular, the true value of $\boldsymbol{\theta}$ is assumed deterministic but unknown and indicated as $\boldsymbol{\theta}_0$, defining the exact probability of $\mathbf{Y}$. Therefore, all the densities obtained varying $\boldsymbol{\theta}$ are

$$\left\{p_{\mathbf{Y}}\left(\mathbf{y}|\boldsymbol{\theta}\right)|\boldsymbol{\theta} \in \boldsymbol{\Theta}\right\} \tag{4.2}$$

It can be assumed that this set contains the exact but unknown density of $\mathbf{Y}$, which corresponds to $p_{\mathbf{Y}}\left(\mathbf{y}|\boldsymbol{\theta}_0\right)$. The objective is to identify $\boldsymbol{\theta}_0$ by exploiting the observations $y_1, \ldots, y_N$.

An estimator is a function of the random observation $\mathbf{Y}$ and with values in $\boldsymbol{\Theta}$ which maps $\mathbb{R}^N$ (measures' space) to $\mathbb{R}^m$ (space that contains $\boldsymbol{\Theta}$), and that does not depend on $\boldsymbol{\theta}$. The value assumed by the estimator as a function of the realizations $\mathbf{y}$, denoted as $\widehat{\boldsymbol{\theta}}(\mathbf{y})$, provides the estimate of $\boldsymbol{\theta}_0$. In order to compare different estimators, it is crucial to introduce a concept of distance between the deterministic vector $\boldsymbol{\theta}$ and the random vector $\widehat{\boldsymbol{\theta}}$. The mean squared error (MSE) can be used. For an estimator $\widehat{\boldsymbol{\theta}}$ and a parameter $\boldsymbol{\theta}$, it is defined as

$$\mathrm{MSE}_{\widehat{\boldsymbol{\theta}}}(\boldsymbol{\theta}) = \mathbb{E}_{\boldsymbol{\theta}}\left(\left\|\widehat{\boldsymbol{\theta}} - \boldsymbol{\theta}\right\|^2\right) = \mathrm{Tr}\left(\Sigma_{\boldsymbol{\theta}}\left(\widehat{\boldsymbol{\theta}}\right)\right) + \sum_{i=1}^{M}\left(\mathrm{Bias}_{\theta_i}\left(\widehat{\theta}_i\right)\right)^2 \tag{4.3}$$

where $\mathbb{E}(\cdot)$ is the expected value operator, $\Sigma(\cdot)$ is the covariance operator and $\mathrm{Tr}(\cdot)$ is the trace operator. The bias of the i-th component of the estimator $\widehat{\boldsymbol{\theta}}$ of $\boldsymbol{\theta}$ is defined as

$$\mathrm{Bias}_{\theta_i}\left(\widehat{\theta}_i\right) = \mathbb{E}_{\theta}\left(\widehat{\theta}_i\right) - \theta_i\,. \tag{4.4}$$

Regarding the model used for the prediction of the metrics values, it is known that for all resident space objects, North American Aerospace Defense Command (NORAD) provides the so called two-line orbital element set (TLE), that is a data format encoding a list of orbital elements for each Earth-orbiting object for a given point in time, the so called *epoch time*. New element sets are generated by NORAD on an as-needed basis rather than according to an established timeline. The update frequency depends on several factors, such as the orbit type or maneuvering capability of the satellite [69]. Generally, the mean update frequency is about 1-2 days [70]. Moreover, also the accuracy of the TLEs depends on a lot of factors, from the sensors used and amount of data collected to the type of orbit and condition of space environment. Since these factors are different for each space object, so is the accuracy [69]. In general, TLEs have an error of about 1 km at epoch time [71]. The simplified general perturbations (SGP) models aim to predict satellite position and velocity. They take as input a TLE and propagate the orbit from epoch to the time of interest. Their development began in 1960s [72] and culminated with the publication of Spacetrack Report Number 3 [73], where five propagation models are described. Among them, the SGP4 model is designed for near-Earth (period less than 225 minutes) satellites [73] and it mainly differs from the original SGP technique in the treatment of atmospheric drag [74]. Regarding the accuracy, it depends on the specific space object but, in general, the propagation error grows at about 1-3 km per day [71]. The description of the algorithm for the computation of the consistency checks now follows.

The aim of the comparison block is to compare the estimate of the chosen metric to its expected value and return a soft output as an indication on the distance between the two values. The test is based on the likelihood ratio, which expresses how many times more likely the data are under one model than the other. This is done in terms of the likelihood ratio test (LRT), that is a hypothesis test used to quantify how well two models fits a set of observations. We need to define two hypotheses

$$\begin{cases} H_0 : \widetilde{\boldsymbol{\theta}} = \boldsymbol{\theta} + \widetilde{\mathbf{w}}\,, \\ H_1 : \text{otherwise}\,, \end{cases} \tag{4.5}$$

where $\widetilde{\boldsymbol{\theta}}$ is the metrics expected value, $\widetilde{\mathbf{w}}$ is the prediction noise, H_0 is the simple null hypothesis, and H_1 is the composite alternative hypothesis. Because of H_1 being composite we need to resort the GLRT [75].

Given $p\left(\widehat{\boldsymbol{\theta}}|\boldsymbol{\theta}\right)$ the probability density function associated to a specific estimator of the estimation blocks, the likelihood function $L(\boldsymbol{\theta}|\widehat{\boldsymbol{\theta}}) = p(\widehat{\boldsymbol{\theta}}|\boldsymbol{\theta})$ is a function of $\boldsymbol{\theta}$ with $\widehat{\boldsymbol{\theta}}$ fixed to the value that is observed, i.e., the estimate. The GLRT statistic is

$$\Lambda(\widehat{\boldsymbol{\theta}}) = \frac{L(\widetilde{\boldsymbol{\theta}}|\widehat{\boldsymbol{\theta}})}{\sup\{L(\boldsymbol{\theta}|\widehat{\boldsymbol{\theta}}) : \boldsymbol{\theta} \in \boldsymbol{\Theta}\}} = \frac{L(\widetilde{\boldsymbol{\theta}}|\widehat{\boldsymbol{\theta}})}{L(\widetilde{\boldsymbol{\theta}}|\widetilde{\boldsymbol{\theta}})} = \frac{p(\widehat{\boldsymbol{\theta}}|\widetilde{\boldsymbol{\theta}})}{p(\widetilde{\boldsymbol{\theta}}|\widetilde{\boldsymbol{\theta}})}. \tag{4.6}$$

The GLRT provides the decision rule as follows: (i) if $\Lambda > c$, accept H_0, (ii) if $\Lambda \leq c$, reject H_0, with c representing a threshold chosen in order to obtain a specified probability of false alarm P_{fa}. In other terms,

$$P[\Lambda(\widehat{\boldsymbol{\theta}}) < c] = \int_{-\infty}^{c} P[\Lambda(\widehat{\boldsymbol{\theta}}) = \lambda] = P_{\text{fa}}, \tag{4.7}$$

with $P[\Lambda(\widehat{\boldsymbol{\theta}}) = \lambda]$ the PDF of $\Lambda(\widehat{\boldsymbol{\theta}})$ during the authentic scenario.

The following subsections will describe the algorithm for the design of the consistency checks.

4.2.1 Position Consistency Check

The position estimation is provided by the navigation solution considering as inputs the GNSS signals and the ephemeris. The position estimator block returns the receiver position $\widehat{r} = (\widehat{x}, \widehat{y}, \widehat{z})$ in earth-centered earth-fixed (ECEF) coordinates. The absolute receiver position can be expressed as $|\widehat{r}| = \sqrt{\widehat{x}^2 + \widehat{y}^2 + \widehat{z}^2}$.
For the estimator distribution evaluation, a Kolmogolov-Smirnov test with significance level $\alpha = 5\%$ has been selected in order to determine whether the estimated position error follow a Gaussian distribution or not. According to the test's output, it can be stated that $\widehat{x}$, $\widehat{y}$, and $\widehat{z}$ are independent Gaussian random variables with means equal to $\widetilde{x}$, $\widetilde{y}$, $\widetilde{z}$ and variances $\sigma^2_{\widehat{x}}$, $\sigma^2_{\widehat{y}}$, $\sigma^2_{\widehat{z}}$, where $\widetilde{r} = (\widetilde{x}, \widetilde{y}, \widetilde{z})$ is the predicted position, with variances $\sigma^2_{\widetilde{x}}$, $\sigma^2_{\widetilde{y}}$, $\sigma^2_{\widetilde{z}}$. Consequently, the normalized error of the estimated position can be defined as

$$\varepsilon_{\widehat{r}} = \sqrt{\left(\frac{\widehat{x} - \widetilde{x}}{\sqrt{\sigma^2_{\widehat{x}} + \sigma^2_{\widetilde{x}}}}\right)^2 + \left(\frac{\widehat{y} - \widetilde{y}}{\sqrt{\sigma^2_{\widehat{y}} + \sigma^2_{\widetilde{y}}}}\right)^2 + \left(\frac{\widehat{z} - \widetilde{z}}{\sqrt{\sigma^2_{\widehat{z}} + \sigma^2_{\widetilde{z}}}}\right)^2}, \tag{4.8}$$

and it follows a Chi distribution with parameter $k = 3$ and therefore

$$p(\varepsilon_{\widehat{r}}|\widetilde{r}) = \frac{1}{\sqrt{2}\Gamma(\frac{3}{2})}(\varepsilon_{\widehat{r}})^2 \mathrm{e}^{-\frac{(\varepsilon_{\widehat{r}})^2}{2}}. \tag{4.9}$$

It is worth noting that the values of $\sigma^2_{\widehat{x}}$, $\sigma^2_{\widehat{y}}$, $\sigma^2_{\widehat{z}}$ can be defined as requirements based on the accuracy on the receiver position.

On the other hand, the position prediction block takes as input the TLE of a space object and a desired prediction time and it outputs the expected position $\widetilde{r}$ in ECEF coordinates of the receiver by means of the SGP4 model. A more detailed characterization of the comparison block will follow later in this section however, it is worth noting that, in the comparison between the position estimate and the position prediction, the inaccuracy due to the TLE measures and SGP4 model should be considered. Indeed, there is an intrinsic error in the position prediction. Furthermore, the farer is the time considered for the position prediction, the higher is the error

introduced in the prediction. It is useful also to verify the coherence of the trajectory followed by the receiver looking at the past positioning values.

In general, for the evaluations each consistency check needs a position predictor block for the prediction of the receiver position. Therefore, all the observations discussed above should be considered in the following analysis.

4.2.2 Power Content Consistency Check

The total received power estimator block takes as input L pre-correlation samples, i.e., the samples between front-end and baseband processing blocks of a receiver, and it outputs the estimated received power $\widehat{P}_{\mathrm{rx}}$. This block assumes that the receiver has a sufficient dynamic range to avoid the need for an AGC, which is a reasonable hypothesis for a receiver located in space where power variations are slow and predictable. By following the analysis done in [76], given $x(k_i), i = 1, \ldots, L$ the front-end output samples, the estimated power is computed as

$$\widehat{P}_{\mathrm{rx}} = \frac{1}{L} \sum_{i=1}^{L} |x(k_i)|^2 \, . \tag{4.10}$$

In the case the receiver front-end is equipped with an AGC, $\widehat{P}_{\mathrm{rx}}$ can still be measured indirectly through the AGC setpoint [77].

In order to derive the probability distribution of $\widehat{P}_{\mathrm{rx}}$, the first step it to characterize the samples $x(k_i), i = 1, \ldots, L$. In particular, each received sample can be written in the following form:

$$x(k_i) = \sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) + w(k_i) \, , \tag{4.11}$$

where N_{s} is the number of visible satellites, $w(k)$ is the complex additive white Gaussian noise with zero mean and variance σ_w^2 (which is assumed to be known). Moreover, A_n is the amplitude, ϕ_n the phase, C_n the spreading code and τ_n the code delay. By substituting Eq. (4.11) into Eq. (4.10), the total received power can be calculated as

$$\begin{aligned}
\widehat{P}_{\mathrm{rx}} &= \frac{1}{L} \sum_{i=1}^{L} \left[\sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) + w(k_i) \right] \left[\sum_{m=1}^{N_{\mathrm{s}}} A_m \mathrm{e}^{-j\phi_m} C_m(k_i - \tau_m) + w^*(k_i) \right] \\
&= \frac{1}{L} \left[\sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} \sum_{m=1}^{N_{\mathrm{s}}} A_n A_m \mathrm{e}^{j(\phi_n - \phi_m)} C_n(k_i - \tau_n) C_m(k_i - \tau_m) + \sum_{i=1}^{L} |w(k_i)|^2 \right. \\
&\quad \left. + \sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) w^*(k_i) + \sum_{m=1}^{N_{\mathrm{s}}} A_m \mathrm{e}^{-j\phi_m} C_m(k_i - \tau_m) w(k_i) \right] \\
&= \frac{1}{L} \left[\sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} A_n^2 C_n^2(k_i - \tau_n) + 2 \sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} \sum_{m \neq n}^{N_{\mathrm{s}}} A_n A_m \mathrm{e}^{j(\phi_n - \phi_m)} C_n(k_i - \tau_n) C_m(k_i - \tau_m) \right. \\
&\quad \left. + \sum_{i=1}^{L} |w(k_i)|^2 + 2 \, \mathrm{Re} \left\{ \sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) w^*(k_i) \right\} \right] \\
&= \sum_{n=1}^{N_{\mathrm{s}}} A_n^2 + \frac{2}{L} \, \mathrm{Re} \left\{ \sum_{i=1}^{L} \sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) w^*(k_i) \right\} + \frac{1}{L} \sum_{i=1}^{L} |w(k_i)|^2
\end{aligned} \tag{4.12}$$

where the last operation derives from the property of orthogonality between different spreading codes. The above formula can be written as $P = P_1 + P_2$ (neglecting the subscript 'rx' and the $\widehat{\cdot}$ for simplicity), with

$$P_1 = \sum_{n=1}^{N_\mathrm{s}} A_n^2 + \frac{2}{L}\,\mathrm{Re}\left[\sum_{i=1}^{L}\sum_{n=1}^{N_\mathrm{s}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) w^*(k_i)\right]$$
$$\sim \mathcal{N}\left(\sum_{n=1}^{N_\mathrm{s}} A_n^2, \frac{n\sigma_w^2}{L}\sum_{n=1}^{N_\mathrm{s}} A_n^2\right), \tag{4.13}$$

$$P_2 = \frac{1}{L}\sum_{i=1}^{L} |w(k_i)|^2 \sim \frac{\sigma_w^2}{2L}\chi^2(2L), \tag{4.14}$$

where $\chi^2(2L)$ is a chi-squared distribution with $2L$ degree of freedom. The mean and the variance of the total distribution are

$$\mu_P = \mathbb{E}\left[P_1 + P_2\right] = \sum_{n=1}^{N_\mathrm{s}} A_n^2 + \sigma_w^2, \tag{4.15}$$

$$\sigma_P^2 = \mathrm{Var}\left[P_1 + P_2\right] = \frac{\sigma_w^4}{L} + \frac{2\sigma_w^2}{L}\sum_{n=1}^{N_\mathrm{s}} A_n^2. \tag{4.16}$$

As proposed in [76], converting the power in dBW (denoted with $\bar{\cdot}$ in the following), the total distribution can be modeled as a Gaussian distribution. In order to compute its mean and variance, the first step is to consider the conversion from linear to decibel scale as a transformation $g(P) = \log_{10}(P/P_0)$ and $P_0 = 1\,\mathrm{W}$. The second step involves expanding $g\left(\mu_P + P - \mu_P\right)$ as a Taylor series, by thinking at $g(x+h)$ where μ_P takes the role of x and $P - \mu_P$ the role of h. The resulting approximate mean and variance are:

$$\mu_{\overline{P}} \approx g(\mu_P) + \frac{\ddot{g}(\mu_P)}{2}\sigma_P^2$$
$$= 10\log_{10}\frac{\mu_P}{P_0} - \frac{\sigma_P^2}{2\mu_P^2}, \tag{4.17}$$

$$\sigma_{\overline{P}}^2 \approx \left[\dot{g}(\mu_P)\right]^2\sigma_P^2 + \frac{\left[\ddot{g}(\mu_P)\right]^2}{4}\left(\sigma_P^2\right)^2$$
$$= 100\frac{\sigma_P^2}{\mu_P^2} + \frac{\sigma_P^4}{4\mu_P^4}, \tag{4.18}$$

Finally, the PDF of total received power can be written as

$$p\left(\overline{\widehat{P}}_\mathrm{rx}|\overline{\widetilde{P}}_\mathrm{rx}\right) = \frac{1}{\sqrt{2\pi\sigma_{\overline{P}}^2}}\mathrm{e}^{-\frac{\left(\overline{\widehat{P}}_\mathrm{rx} - \mu_{\overline{P}}\right)^2}{2\sigma_{\overline{P}}^2}}, \tag{4.19}$$

where $A_n, n = 1, \ldots, N_\mathrm{s}$, that are needed to compute $\mu_{\overline{P}}$ and $\sigma_{\overline{P}}^2$, can be derived by using the orbit prediction model.

The power predictor block takes as input the receiver position and all the GNSS satellites predicted positions in ECEF coordinates and, by means of the link budget, it outputs the expected total received power.

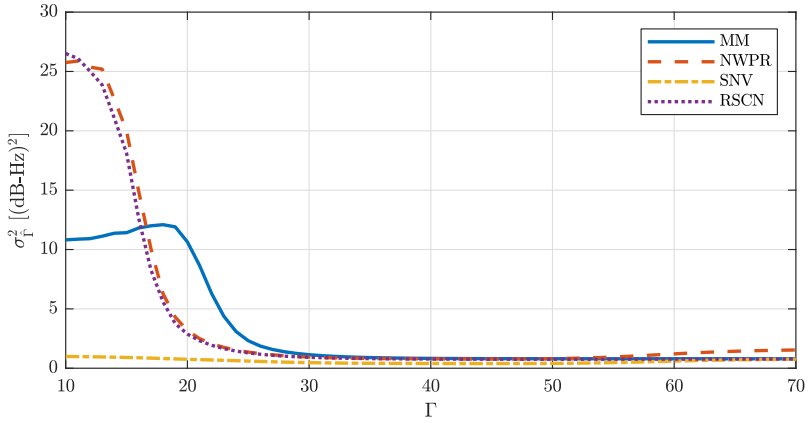


FIGURE 4.2: Variance value for the considered C/N_0 estimators.

4.2.3 C/N_0-Based Consistency Check

The C/N_0 estimator block takes as input N prompt correlator outputs and it returns its estimate. Hereafter, we denote the C/N_0 variable as Γ for notation simplicity. In [78], the authors have selected and investigated several signal-to-noise ratio (SNR) estimation algorithms and, based on their results, we considered four of them, that is real signal-complex noise (RSCN), squared signal-to-noise variance (SNV) [79], [80], moments method (MM) [79], and narrowband-wideband power ratio (NWPR) [81] (see Appendix D). The proposed estimators are biased for some Γ values. However, since the true Γ value is evaluated by the predictor block with a certain inaccuracy, the bias from the estimated value $\widehat{\Gamma}$ can be removed defining $\widehat{\Gamma}'(dB) = \widehat{\Gamma} - \text{Bias}_{\widetilde{\Gamma}}(\widehat{\Gamma})$, with $\widetilde{\Gamma}$ the predicted value and $\text{Bias}_{\widetilde{\Gamma}}(\widehat{\Gamma}) = \text{E}_{\widetilde{\Gamma}}[\widehat{\Gamma}] - \widetilde{\Gamma}$. Therefore, the choice of the C/N_0 estimator depends only on the variance that, as it can be seen in Fig. 4.2, is minimum for the SNV estimator.

According to the Kolmogolov-Smirnov test with significance level $\alpha = 5\%$, we found that $\widehat{\Gamma}'$ can be approximated with a Gaussian distribution with mean $\widetilde{\Gamma}$ and variance σ^2_{SNV} empirically calculated, so that

$$p(\widehat{\Gamma}'|\widetilde{\Gamma}) = \frac{1}{\sqrt{2\pi\sigma^2_{\text{SNV}}}} \text{e}^{-\dfrac{(\widehat{\Gamma}' - \widetilde{\Gamma})^2}{2\sigma^2_{\text{SNV}}}}. \tag{4.20}$$

The C/N_0 predictor block takes as input the receiver and a GNSS satellite predicted positions in ECEF coordinates and it outputs the expected C/N_0, $\widetilde{\Gamma}$. This block performs the same steps of the total received power predictor block using the link budget formula. Then, given a certain receiver noise spectral density N_0, $\widetilde{\Gamma} = \overline{P}_{\text{rx},i} - N_0$, where $\overline{P}_{\text{rx},i}$ is the power received from the i-th satellite.

The description of the comparison block for each consistency check is missing. The reason is that its general characterization, as already discussed, can be made more specific for each check by substituting the general PDF expression with the specific PDF of the considered check.

4.3 Fusion Technique

Each consistency check provides its own soft output that can then be combined to return a unique hard output as a flag stating that a potential threat is present. The

TABLE 4.1: Values of standard deviation used for estimated position, predicted position and estimated C/N_0.

$\sigma_{\widehat{x}}$, $\sigma_{\widehat{y}}$, $\sigma_{\widehat{z}}$	$\sigma_{\widetilde{x}}$, $\sigma_{\widetilde{y}}$, $\sigma_{\widetilde{z}}$	σ_{SNV}
10 m	1000 m [83]	1 dB-Hz

idea is to use a method based on Dempster-Shafer theory (DST) to fuse multiple detectors as done in [82].

We follow the same approach, and employ the same belief function

$$f(\Lambda, c) = \frac{1}{2^{c/\Lambda}}\,, \tag{4.21}$$

that maps the soft output of each check (the GLRT statistic Λ) and the chosen threshold c to its believable degree of evidence. Based on the inference of the combination rule of DST for the binary detection case, the combined belief function is given by

$$m = \frac{\prod_{i=1}^{N_\mathrm{D}} f(\Lambda_i, c_i)}{\prod_{i=1}^{N_\mathrm{D}} f(\Lambda_i, c_i) + \prod_{i=1}^{N_\mathrm{D}} \left(1 - f(\Lambda_i, c_i)\right)}\,, \tag{4.22}$$

where N_D represents the number of spoofing detectors and m is the combined belief function output. After the fusion, it is necessary to make a final decision to determine the signal's authenticity. The decision rule declares spoofing when $m \geq 0.5$.

4.4 Results

In order to test the proposed anti-spoofing mechanism, we considered three trajectory spoofing attacks lasting for 15 minutes: one on a LEO satellite, another one on a MEO satellite, and the last one on a GEO satellite. The spoofer starts its attack at the fifth minute aligned with the authentic trajectory and it gradually diverges to the desired orbit. Moreover, during the misalignment, the attacker increases the C/N_0 of the forged satellites over the authentic ones in order to take possession of the tracking loop. The values of the different variances that have been used are reported in Table 4.1. In Fig. 4.3 the distance d_{AS} between authentic and spoofed position is shown as a function of time.

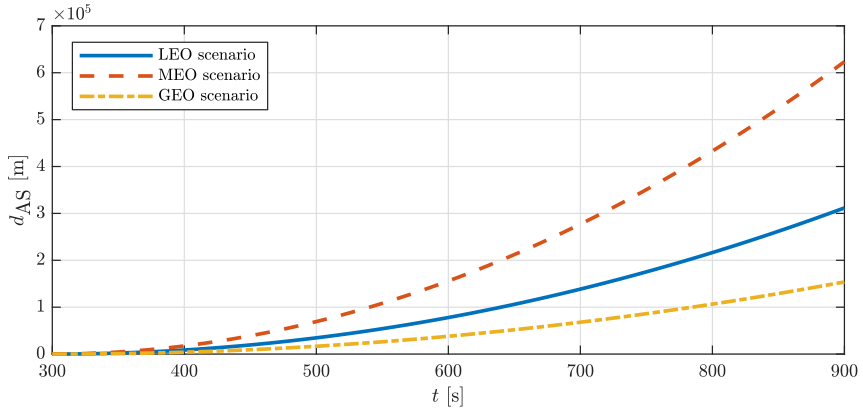


FIGURE 4.3: Distance between spoofed and authentic position as a function of time in the different scenarios.

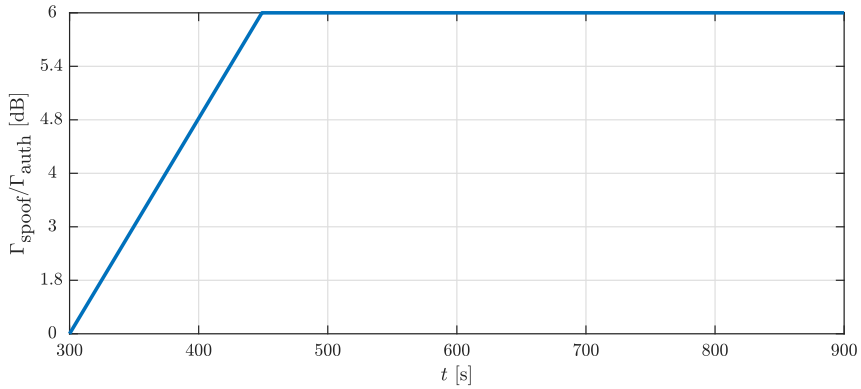


FIGURE 4.4: Ratio between spoofed and authentic C/N_0 as a function of time.

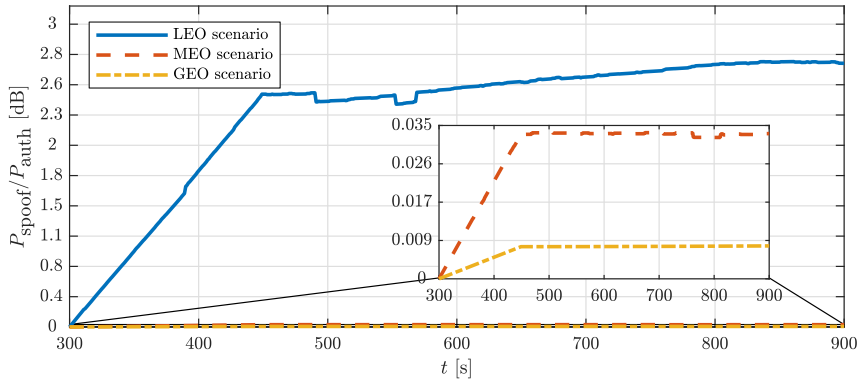


FIGURE 4.5: Ratio between spoofed and authentic pre-correlation power as a function of time.

In Fig. 4.4 the ratio $\Gamma_{\text{spoof}}/\Gamma_{\text{auth}}$ between the spoofed and the authentic C/N_0 as a function of time is reported. Since in these scenarios the spoofer imposes the same power advantage for all the spoofed satellites, the graph is shown only for a single satellite of the GPS constellation. As we can see, the C/N_0 discrepancy increases linearly in the interval $[300\,\text{s}, 450\,\text{s}]$ and it remains constant in the interval $[450\,\text{s}, 900\,\text{s}]$.

In Fig. 4.5 the ratio $P_{\text{spoof}}/P_{\text{auth}}$ between the spoofed and the authentic pre-correlation power as a function of time is reported. As we can see, the power ratio increases more or less linearly for $[300\,\text{s}, 450\,\text{s}]$ and it remains almost constant in the interval $[450\,\text{s}, 900\,\text{s}]$. The jumps and variations in the evolution of the ratio are due to C/N_0 changes of the single satellites or to the rise of a new satellite (or set of a visible satellite) in the receiver visibility cone. Moreover, we can notice that for the MEO and GEO scenarios the power ratio is much lower than that of the LEO scenario; this is due to the lower C/N_0 of the satellites visible from MEO and GEO receivers, so that the noise power is the predominant one.

The performance evaluation of the consistency checks has been carried out by fixing three target values for the false alarm probability ($P_{\text{fa}} = 10^{-1}, 10^{-2}, 10^{-3}$) and by measuring the corresponding probability of missed detection P_{md} for all the snapshots in the scenarios.

The performance of the position check is reported in Fig. 4.6 for the three different probabilities of false alarm as a function of d_{AS}. The check works very well for $d_{\text{AS}} > 2600\,\text{m}$ with $P_{\text{fa}} = 10^{-1}$, for $d_{\text{AS}} > 3400\,\text{m}$ with $P_{\text{fa}} = 10^{-2}$, and for $d_{\text{AS}} > 4000\,\text{m}$ for $P_{\text{fa}} = 10^{-3}$. Moreover, the performance of this check is scenario-independent since it

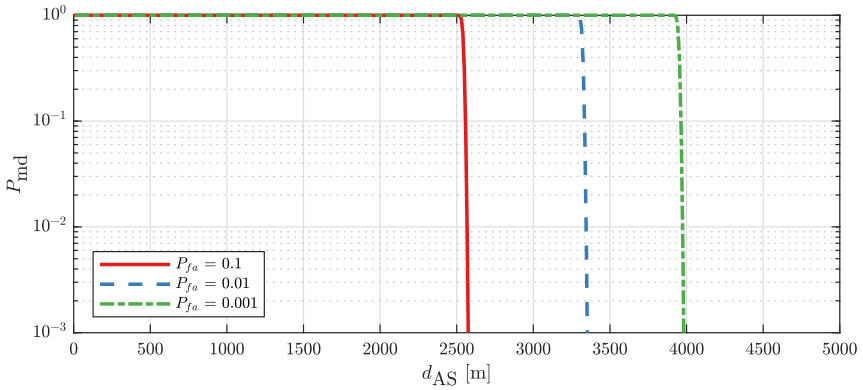


FIGURE 4.6: Probability of missed detection as a function of d_{AS} for the position check.

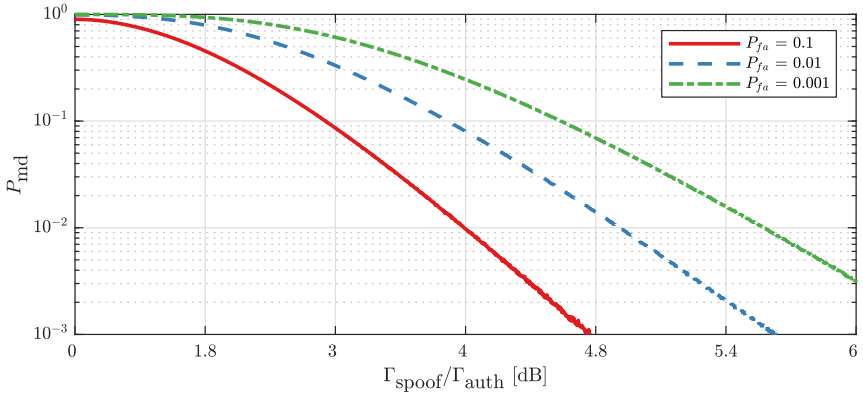


FIGURE 4.7: Probability of missed detection as a function of $\Gamma_{\text{spoof}}/\Gamma_{\text{auth}}$ for the C/N_0 check for one satellite.

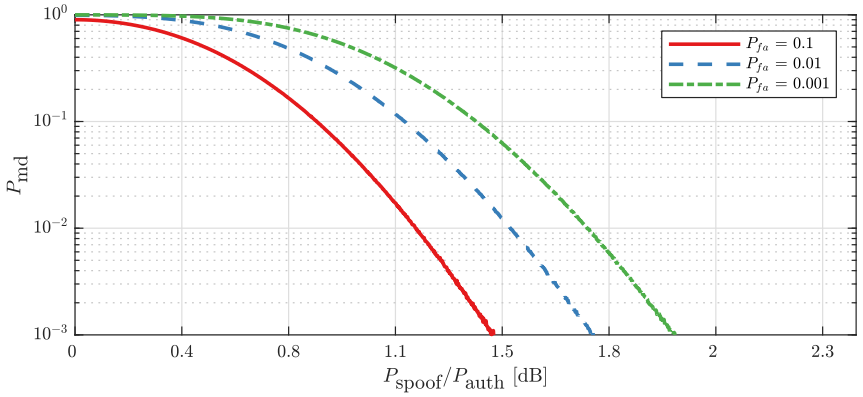


FIGURE 4.8: Probability of missed detection as a function of $P_{\text{spoof}}/P_{\text{auth}}$ for the power check.

depends only on the distance d_{AS} between authentic and spoofed position.

The performance of the C/N_0 check is reported in Fig. 4.7 for the three different probabilities of false alarm as a function of $\Gamma_{\text{spoof}}/\Gamma_{\text{auth}}$. We can see that a good P_{md} is reached when the C/N_0 discrepancy is 4 dB for $P_{\text{fa}} = 10^{-1}$, 4.9 dB for $P_{\text{fa}} = 10^{-2}$ and 5.6 dB for $P_{\text{fa}} = 10^{-3}$. Moreover, also the performance of this check is scenario-independent since it depends only on the ratio $\Gamma_{\text{spoof}}/\Gamma_{\text{auth}}$ between the spoofed and the authentic C/N_0.

The performance of the power check is reported in Fig. 4.8 for the three different probabilities of false alarm as a function of $P_{\text{spoof}}/P_{\text{auth}}$. The performance of this check are dependent on the scenario, indeed it works well only when the C/N_0 are high (from about 40 to about 55 dB-Hz, as in the case of the LEO scenario) and it does not work at all when the C/N_0 are low (from about 25 to about 40 dB-Hz for the MEO scenario, or from about 15 to about 30 dB-Hz for the GEO scenario).

The performance of the fusion check is reported in Figs. 4.9 to 4.11 for the three considered scenarios and for $P_{\text{fa}} = 10^{-2}$. We can see that P_{md} approaches acceptable values before the other checks for all the LEO and GEO scenarios, providing sensible improvements over the individual checks. On the other hand, in the MEO scenario the position check provides good performance some seconds before than the fusion check. This is because the distance between authentic and spoofed position increases quickly to the benefit of the position check, while the other two checks do not provide enough evidence to the fusion check in the same time interval.

Finally, in Table 4.2 the mapping between the desired P_{fa} of the single checks and the corresponding P_{fa} of the fusion checks derived empirically is reported. It can be observed that the latter ones are smaller than the former ones, therefore validating the usefulness of the fusion check in improving the detection performance compared to the individual checks.

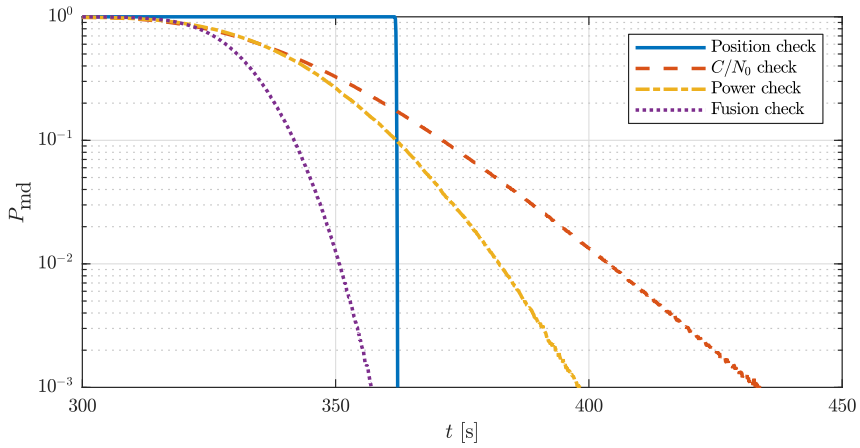


FIGURE 4.9: Probability of missed detection as a function of time for all the checks in the LEO scenario ($P_{\text{fa}} = 10^{-2}$).

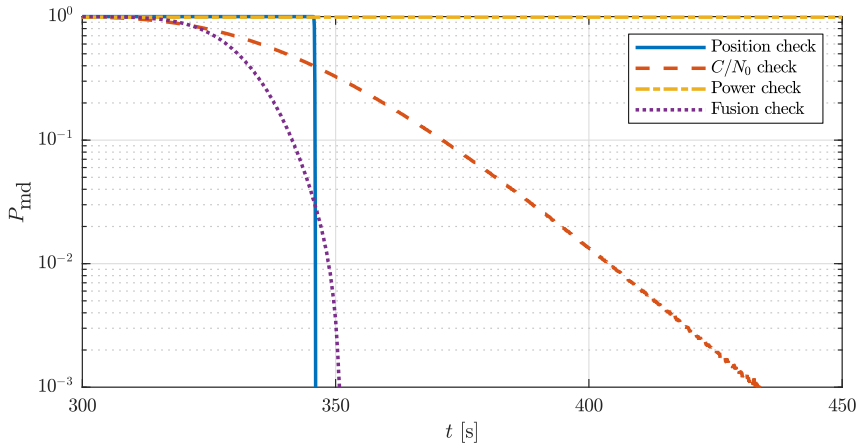


FIGURE 4.10: Probability of missed detection as a function of time for all the checks in the MEO scenario ($P_{\text{fa}} = 10^{-2}$).

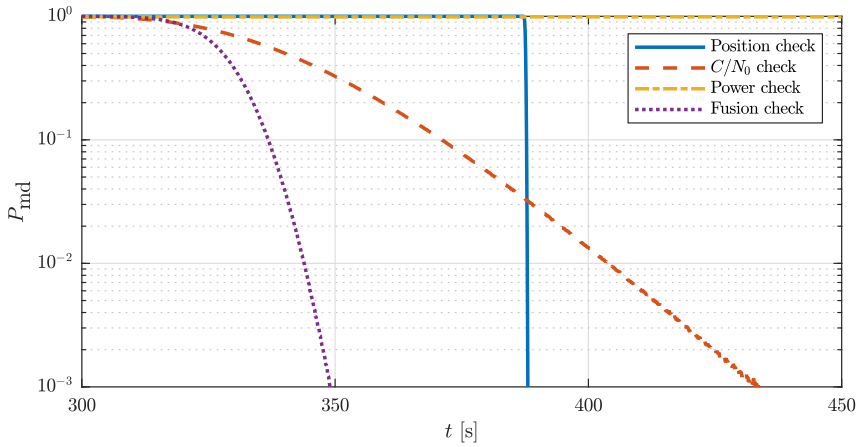


FIGURE 4.11: Probability of missed detection as a function of time for all the checks in the GEO scenario ($P_{\mathrm{fa}} = 10^{-2}$).

TABLE 4.2: Probability of false alarm for the fusion check.

P_{fa} of the single checks	10^{-1}	10^{-2}	10^{-3}
P_{fa} of the fusion check	$4.5 \cdot 10^{-2}$	$1.6 \cdot 10^{-3}$	10^{-4}

4.5 Conclusion

In the framework of securing GNSS services, much attention has been given to ground applications, whereas few requirements are considered for the protection and robustness enhancement of space based GNSS receivers, that is the scenario considered in this work.

A spoofing detection mechanism based on the consistency check of three different metrics (position, C/N_0 and total received power) has been developed. In particular, the metric value estimated from the GNSS signal and the one predicted using an orbit propagation model are compared by means of the GLRT. Then, the soft detection results of the single checks are fused together to provide a spoofing decision.

The proposed mechanism has been tested on three trajectory spoofing scenarios, for a LEO, a MEO, and a GEO satellite. Referring to a $P_{\mathrm{fa}} = 10^{-2}$, the performance of the position check is very good only when the position drift imposed by the attacker is at least 3600 m; this is due to the low precision of the orbit propagation model. On the other hand, the C/N_0 check is effective only for the satellites for which the spoofing signal is 4.9 dB more powerful than the expected authentic signal. As regards the total received power check, its usefulness is limited to the case where the C/N_0 of the forged satellites is high enough. Finally, the performance of the fusion check is in general better than that of the single checks, since the probability of missed detection assumes acceptable values earlier and the probability of false alarm is lower.

As a future work, it would be useful not only to compare the actual values with their current estimations, but also with their past estimations. Indeed, satellites move uniformly, therefore it is reasonable that the estimated values change smoothly and any discontinuity may be a sign of anomaly. Moreover, composite security requirements can be formulated that take into account different weights for orbit displacement in different directions (for example, the drift on the radial and on the cross-track directions vs that on the along-track direction).

Chapter 5

A Jamming Detection Technique for 5G and Beyond

5.1 Introduction

Security has been one of the main pillars driving the 3GPP design of the 5G of mobile communication systems. In fact, several security functionalities are available in 5G at the packet data convergence protocol (PDCP) and above layers to guarantee authentication, privacy and data integrity [84]. On the other hand, denial of service attacks in the form of radio jamming have been recently recognized as a major threat for the 5G deployment in Industry 4.0 scenarios, in particular with URLLC, which are inherently more susceptible to the interference impact of a jammer due to their stringent quality of service requirements. As an example, while we can assume that no malicious device can be activated inside a factory, it might happen that a jammer stationed outside the plant blocks the transmission of some legitimate devices inside that plant. Such attack can cause large economic losses to the factory by interrupting the production. Moreover, besides these 5G Industry 4.0 use cases, jamming detection and mitigation has been recognized as an extremely relevant topic also for sixth generation (6G) technologies [85]–[87].

Jamming attacks have been known as a threat for communication and localization systems for many years, and jammers have been extensively used in the military context to degrade the effectiveness of enemy radars. Mainly for that reason, it is very simple and inexpensive nowadays to obtain a jammer that is capable of emitting high jamming power up to several tens of Watts [88]. Furthermore, aside from simple devices that can generate narrow- or wide-bands RF interference [89], there exist much smarter but still easily available jamming devices too [90]. This last type, a.k.a. as *reactive* jammers, are inactive while no legitimate transmission is happening, and then starts generating interference as soon as they sense some transmission on the channel, making them very difficult to be detected, much more power efficient, and more effective in their jamming attack . Differently from other security aspects like authentication and privacy that can and are well managed at PDCP and above layers in 5G, jamming, as a form of malicious interference, can be handled at the physical layer. In fact, physical layer security mechanisms are expected to play an important role in 6G [91].

A fundamental difference exists between a legitimate interfering device and a jammer. A legitimate device creates interference while respecting the rules of the standard regulating communications in that band and several well-known techniques exist to deal with that type of interference. A jammer is a malicious device that intentionally attacks the system, also violating the regulatory and standardization rules, and its activity can be extremely dangerous: smart reactive jamming attacks can strongly degrade network performance even with a very limited jamming activity

[92]. For that reason, a jamming-resilient communication system needs to perform two tasks: a) detection, to understand that some network performance degradation happens because of a malicious jamming attack and not because of fading or some legitimate cellular interference, and b) mitigation, with the implementation of focused techniques to limit the impact of the attacker.

Here, we consider the problem of jamming detection in 5G-and-beyond communication systems, with particular focus on URLLC. Some work has recently been done in this framework. In [93], a detection technique has been proposed for massive MIMO base stations (BSs) exploiting pseudo-random hopping of the scheduled UEs among the pilot sequences and allowing the BS to design a jamming-resilient combiner. A more specific analysis for URLLC has been done by [94], where an advanced feedback is proposed and relays implementing promiscuous listening are used to detect rare events like a jammer. Along this direction, [95] proposes to deploy a guard node that generates and transmits a signal known at the legitimate receiver: the received signal is then post-processed to determine if a jamming attack occurred.

In this work we consider a system using OFDM and propose a novel method based on pseudo-random blanking of subcarriers to detect jamming attacks. Differently from [94], [95], our proposal does not require the deployment of additional nodes and, differently from [93], it applies also to the case of BSs with limited number of antennas, which occurs in particular with 5G deployments for Industry 4.0 indoor scenarios, for example to provide connectivity in a factory floor. Moreover, our proposal can be seamlessly embedded in the air interface design of OFDM-based technologies, including the long term evolution (LTE), 5G NR and the anticipated 6G. More specifically, we design a detector exploiting the GLRT and aiming to detect a smart jammer. Namely, we consider a jammer with one of the following objectives: a) maximize the MD probability to remain stealthy, b) minimize the SE, assuming a MBB type of traffic, and c) maximize the BLER, considering a URLLC type of traffic. The subcarrier blanking represents a loss in terms of system performance as some resources are not used for communication. Numerical results are provided to show the benefits of the proposed approach and the trade-off between the capability of detecting a jammer and the system performance, in terms of both SE and BLER.

Notation for this Chapter. $(\cdot)^{\mathrm{T}}$ denotes the transpose. $\|\mathbf{x}\|$ indicates the norm of vector $\mathbf{x}$. $|\mathcal{X}|$ denotes the cardinality of the set $\mathcal{X}$. $\overline{\mathcal{X}}$ denotes the complement of the set $\mathcal{X}$. $\mathrm{diag}(x_1, \ldots, x_N)$ denotes the diagonal matrix where $x_1, \ldots, x_N$ are the diagonal elements. $C_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$ denotes the number of k-combinations from a given set of n elements. $\mathcal{CN}(\mu, \sigma^2)$ denotes the complex Gaussian distribution with mean μ and variance σ^2. $Q(\cdot)$ denotes the Gaussian Q-function. $P[A]$ denotes the probability of event A. $\mathbb{E}[X]$ denotes the expectation of random variable (r.v.) X.

5.2 System Model

We consider a single-cell single-user uplink scenario with a UE transmitting toward a BS; both UE and BS are single-antenna. Moreover, we assume a jammer that tries to disrupt the ongoing communication by sending a malicious signal to the BS, as shown in Fig. 5.1. The considered system uses an OFDM modulation where the available radio resources can be thought as in a resource grid composed of resource elements (REs), where each RE occupies one subcarrier in frequency and one OFDM symbol in time, for a total of S subcarriers per OFDM symbol (see also Fig. 5.2).

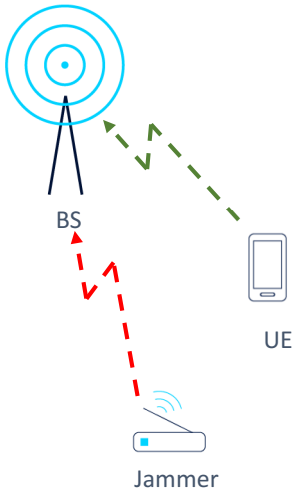


FIGURE 5.1: Representation of the considered UL scenario.

We now define the signal received by the BS on subcarrier $s \in \{1, \ldots, S\}$ at symbol $n \in \mathbb{N}$ as

$$r_s(n) = u_s(n) \cdot h_s(n) + j_s(n) \cdot g_s(n) + w_s(n)\,, \tag{5.1}$$

where $u_s(n)$ is the signal from the UE, $h_s(n)$ is the UE channel, $j_s(n)$ is the signal from the jammer, and $g_s(n)$ is the jammer channel. Moreover, $w_s(n) \sim \mathcal{CN}(0, \sigma_w^2)$ is the complex Gaussian noise with σ_w^2 as statistical power. In particular, in this Chapter we consider two types of channel:

- AWGN channel with $h_s(n) = H$ and $g_s(n) = G$, where H and G are constant for each subcarrier and OFDM symbol;
- Rayleigh channel with $h_s(n) \sim \mathcal{CN}(0, \sigma_h^2)$ and $g_s(n) \sim \mathcal{CN}(0, \sigma_g^2)$.

We can now write the corresponding signal to interference plus noise ratio (SINR) on subcarrier $s \in \{1, \ldots, S\}$ at symbol $n \in \mathbb{N}$ as

$$\mathrm{SINR}_s(n) = \frac{P_{\mathrm{UE},s}(n)\|h_s(n)\|^2}{\sigma_w^2 + P_{\mathrm{J},s}(n)\|g_s(n)\|^2}\,, \tag{5.2}$$

where $P_{\mathrm{UE},s}(n)$ is the UE power and $P_{\mathrm{J},s}(n)$ is the jammer power. We denote the respective total power per symbol as $P_{\mathrm{UE}}(n) = \sum_{s=1}^{S} P_{\mathrm{UE},s}(n)$ and $P_{\mathrm{J}}(n) = \sum_{s=1}^{S} P_{\mathrm{J},s}(n)$.

Regarding the key performance indicators (KPIs) that will be used to evaluate the damage caused by the jammer to the legitimate system, in this work we focus on SE and BLER. SE is most relevant when considering MBB type of traffic and we define it as

$$\mathrm{SE} = \mathbb{E}\left[\log_2\left(1 + \mathrm{SINR}_s(n)\right)\right]\,. \tag{5.3}$$

When considering URLLC type of traffic, performance is typically measured in terms of latency and reliability. In our study, we assume that we have small packets sent by the UE, each packet scheduled on a set of REs allocated within a limited number of OFDM symbols. Moreover, we assume that latency requirements are so strict that retransmissions are not allowed. Therefore, system performance can be evaluated just in terms of reliability, whose KPI corresponds to the BLER. For our analysis, we define a certain $\mathrm{SINR}_{\mathrm{pkt}}$ as the equivalent SINR experienced by a packet (which can be computed by using different link-to-system mapping criteria [96]), and using this we

compute the BLER from the normal approximation of the finite blocklength capacity:

$$\mathrm{BLER}_{\mathrm{pkt}} = Q\left(\left[\log_2\left(1+\mathrm{SINR}_{\mathrm{pkt}}\right) - \rho + \frac{\log_2 C}{2C}\right]\sqrt{\frac{C}{V}}\right) \tag{5.4}$$

where

$$V = \mathrm{SINR}_{\mathrm{pkt}}\frac{2+\mathrm{SINR}_{\mathrm{pkt}}}{\left(1+\mathrm{SINR}_{\mathrm{pkt}}\right)^2}\left(\log_2 \mathrm{e}\right)^2 \tag{5.5}$$

V is the channel dispersion, ρ is the packet spectral efficiency, and C is the coded packet size [97, Eq. (5)].

5.3 Defense Strategy

In this work, we propose to blank some REs in each OFDM symbol in a pseudo-random manner, such that the attacker cannot predict in advance which resources will be used for transmission and which will be blanked. In practice, there are different options to allow the legitimate devices like the UE and BS in our setup to be able to determine the sequence of blanked REs. In case of downlink (DL) the solution can be implemented purely at the BS-side, transparent to the UE, by deliberately leaving resources unoccupied. Alternatively, BS and UE can use pseudo random number generators using a secretly shared initial seed.

With our proposal, we have then two types of REs: data REs and blanked REs. The former is used for data transmission, while the latter is, indeed, left blanked and will be used for jamming detection. In particular, at each OFDM symbol n, the UE blanks a set $\mathcal{M}(n) = \{m_1(n), \ldots, m_M(n)\}$ (with cardinality $M = |\mathcal{M}(n)|$) of REs, where $m_1(n), \ldots, m_M(n)$ are chosen in a pseudo-random manner from the set $\{1, \ldots, S\}$; the remaining REs are used for data transmission. Since no data is transmitted on the blanked REs, we define the UE signal introduced in Eq. (5.1) as

$$u_s(n) = \begin{cases} d_s(n) & s \in \overline{\mathcal{M}(n)} \\ 0 & s \in \mathcal{M}(n) \end{cases}, \qquad n \in \mathbb{N}, \tag{5.6}$$

where $d_s(n)$ is the data sample sent by the UE. At the same time, the attacker transmits on a set $\mathcal{L}(n) = \{\ell_1(n), \ldots, \ell_L(n)\}$ (with cardinality $L = |\mathcal{L}(n)|$) of REs, where $\ell_1(n), \ldots, \ell_L(n)$ are chosen from the set $\{1, \ldots, S\}$ according to the jammer strategy. Note that while here we consider mainly for sake of notation M and L constant, in practice they can also be discrete random variables. Fig. 5.2 shows an example of the resource grid in such situation.

The defense strategy takes advantage of the blanked REs to detect the presence of jamming by means of statistical hypothesis testing [75]. The two hypotheses for the sequence of blanked REs are as follows:

- There is no jamming and we have just thermal noise (null hypothesis $\mathcal{H}_0$);
- There is jamming (alternative hypothesis $\mathcal{H}_1$).

The two hypotheses hold because we are in a single-cell scenario with no interference from other cells. In practice, as this proposal targets Industry 4.0 scenarios, where in many countries specific bands are now being allocated to industry players that can deploy their 5G-and-beyond network in their own campus without interference from neighboring networks [98], this idea can be extended and easily applied in such case

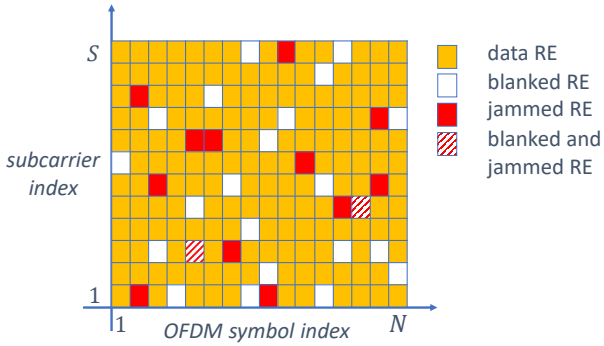


FIGURE 5.2: Example of the OFDM resource grid with blanked and jammed REs.

by considering the sharing among the deployed BSs in that same campus of the same sequence of REs to be blanked.

By denoting with N the number of OFDM symbols that will be used at the BS for jamming detection, the above hypotheses translate in the following hypothesis test:

$$\begin{cases} \mathcal{H}_0 : \mathbf{r} = \mathbf{w} \\ \mathcal{H}_1 : \mathbf{r} = \mathbf{w} + \mathbf{G}\mathbf{j} \end{cases}, \tag{5.7}$$

where $\mathbf{r} = \left[r_{m_1(1)} \cdots r_{m_M(1)} \cdots r_{m_1(N)} \cdots r_{m_M(N)}\right]^{\mathrm{T}}$, $\mathbf{w} = \left[w_{m_1(1)} \cdots w_{m_M(1)} \cdots w_{m_1(N)} \cdots w_{m_M(N)}\right]^{\mathrm{T}}$, and $\mathbf{j} = \left[j_{m_1(1)} \cdots j_{m_M(1)} \cdots j_{m_1(N)} \cdots j_{m_M(N)}\right]^{\mathrm{T}}$. These are vectors containing the samples of all the blanked REs for, respectively, received, noise, and jamming signal. Moreover, $\mathbf{G} = \mathrm{diag}(g_{m_1(1)}, \ldots, g_{m_M(1)}, \ldots, g_{m_1(N)}, \ldots, g_{m_M(N)})$ is the jammer channel matrix.

In order to proceed with the hypothesis testing process, we need to make some assumptions on the statistics of the signals involved. After defining the received jamming signal as $\tilde{\mathbf{j}} = \mathbf{G}\mathbf{j}$, we propose here a detector in the most general case where no assumption can be made about $\tilde{\mathbf{j}}$. Then, in Section 5.4, we use the derived detector for computing the MD probability in closed form in the case that $\tilde{\mathbf{j}}$ has zero-mean complex Gaussian distribution.

By assuming that the statistics of the jamming signal received by the BS are unknown, $\mathcal{H}_1$ becomes a composite alternative hypothesis and we need to resort to the GLRT [75]. The GLRT decides for $\mathcal{H}_1$ if

$$\Lambda(\mathbf{r}) = \frac{p(\mathbf{r}|\hat{\tilde{\mathbf{j}}}; \mathcal{H}_1)}{p(\mathbf{r}; \mathcal{H}_0)} > \lambda\,, \tag{5.8}$$

where $p(\mathbf{r}; \mathcal{H}_0)$ is the PDF of $\mathbf{r}$ under $\mathcal{H}_0$ and $p(\mathbf{r}|\hat{\tilde{\mathbf{j}}}; \mathcal{H}_1)$ is the PDF of $\mathbf{r}$ conditioned on $\tilde{\mathbf{j}} = \hat{\tilde{\mathbf{j}}}$ and under $\mathcal{H}_1$. Moreover, $\hat{\tilde{\mathbf{j}}}$ is the maximum likelihood estimate (MLE) of $\tilde{\mathbf{j}}$ assuming $\mathcal{H}_1$ is true, $\Lambda(\mathbf{r})$ is the test statistic, and λ is the threshold. In particular, λ is found from

$$P_{\mathrm{FA}} = P\left[\Lambda(\mathbf{r}) > \lambda; \mathcal{H}_0\right] = \int_{\{\mathbf{r}:\Lambda(\mathbf{r})>\lambda\}} p(\mathbf{r}; \mathcal{H}_0) d\mathbf{r}\,, \tag{5.9}$$

where P_{FA} is the false alarm (FA) probability, i.e., the probability of declaring jamming even if it is not present.

We now derive the threshold λ by fixing the value of P_{FA}. First of all, we need

to compute the test statistic formula, and we start by deriving the PDF of $\mathbf{r}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$. When $\mathcal{H}_0$ is true, the signal received at the BS is $\mathbf{r} = \mathbf{w}$, therefore, we have $\mathbf{r} \sim \mathcal{CN}(\mathbf{0}, \sigma_w^2\mathbf{I})$. When $\mathcal{H}_1$ is true, the received signal becomes $\mathbf{r} = \mathbf{w} + \tilde{\mathbf{j}}$, where $\tilde{\mathbf{j}}$ is an unknown vector, with resulting distribution $\mathbf{r} \sim \mathcal{CN}(\tilde{\mathbf{j}}, \sigma_w^2\mathbf{I})$. In order to derive the corresponding PDF, we need to compute the MLE of $\tilde{\mathbf{j}}$ by maximizing $p(\mathbf{r}|\tilde{\mathbf{j}}; \mathcal{H}_1)$ through the following optimization problem:

$$\hat{\mathbf{j}} = \underset{\tilde{\mathbf{j}} \in \mathbb{C}^{MN \times 1}}{\arg\max}\, p(\mathbf{r}|\tilde{\mathbf{j}}; \mathcal{H}_1)\,. \tag{5.10}$$

Under our assumptions, the solution is just $\hat{\mathbf{j}} = \mathbf{r}$, thus leading to

$$p(\mathbf{r}|\hat{\mathbf{j}}; \mathcal{H}_1) = p(\mathbf{r}|\mathbf{r}; \mathcal{H}_1) = \frac{1}{(\pi\sigma_w^2)^{MN}}\,. \tag{5.11}$$

By applying Eq. (5.11) to Eq. (5.8), the resulting decision rule is

$$\Lambda(\mathbf{r}) = \mathrm{e}^{\frac{\|\mathbf{r}\|^2}{\sigma_w^2}} > \lambda\,, \tag{5.12}$$

that, after some computations, can be rewritten as

$$\Lambda'(\mathbf{r}) = \frac{\|\mathbf{r}\|^2}{MN} > \lambda'\,, \tag{5.13}$$

with $\Lambda'(\mathbf{r}) \triangleq \frac{\sigma_w^2 \ln \Lambda(\mathbf{r})}{MN}$ being the new test statistic and $\lambda' \triangleq \frac{\sigma_w^2 \ln \lambda}{MN}$ the new threshold. This is, basically, an energy detector, which is quite an intuitive result: when we have no knowledge about the jamming signal, we can just compute the energy of the received signal on the blanked REs and compare it against a thereshold.

The test statistic distribution under $\mathcal{H}_0$ is then

$$\Lambda'(\mathbf{r}; \mathcal{H}_0) = \frac{\|\mathbf{w}\|^2}{MN} \sim \text{Gamma}\left(MN, \frac{\sigma_w^2}{MN}\right)\,, \tag{5.14}$$

where $\text{Gamma}(k, \theta)$ is the gamma distribution with shape paramenter k and scale parameter θ. From Eq. (5.9), the resulting FA probability turns out to be

$$P_{\text{FA}} = P\left[\Lambda'(\mathbf{r}; \mathcal{H}_0) > \lambda'\right] = 1 - F_{\Lambda'(\mathbf{r}; \mathcal{H}_0)}(\lambda')\,, \tag{5.15}$$

where $F_X(x)$ denotes the CDF of the r.v. X computed in x. This leads to

$$\lambda' = F^{-1}_{\Lambda'(\mathbf{r}; \mathcal{H}_0)}\left(1 - P_{\text{FA}}\right)\,, \tag{5.16}$$

which can be now used to evaluate the detection performance of this defense strategy. This is done by means of the MD probability, defined as the probability of accepting $\mathcal{H}_0$ when jamming is present. In this model, the test statistic distribution under $\mathcal{H}_1$ can be written as

$$\Lambda'(\mathbf{r}; \mathcal{H}_1) = \frac{\|\mathbf{w} + \tilde{\mathbf{j}}\|^2}{MN} \sim \frac{\sigma_w^2}{2MN}\chi^2\left(2MN, \|\tilde{\mathbf{j}}\|^2\right)\,, \tag{5.17}$$

where $\chi^2(\nu, \delta)$ is the non-central χ^2 distribution with ν degrees of freedom and non-centrality parameter δ. Eventually, we can write the MD probability as

$$P_{\text{MD}} = P\left[\Lambda'(\mathbf{r}; \mathcal{H}_1) < \lambda'\right] = 1 - F_{\Lambda'(\mathbf{r};\mathcal{H}_1)}\left(\lambda' \frac{2MN}{\sigma_w^2}\right) .$$

5.4 MD Probability with Gaussian Distributed Received Jamming Signal

We now evaluate the effectiveness of the proposed defense strategy against a jamming signal with distribution $\tilde{\mathbf{j}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{D})$, where $\mathbf{D} = \text{diag}(d_{m_1(1)}, \ldots, d_{m_M(1)}, \ldots, d_{m_1(N)}, \ldots, d_{m_M(N)})$ is the covariance matrix with diagonal elements defined as

$$d_{m_i(n)} = \begin{cases} P_{\text{J}}/L, & m_i(n) \in \mathcal{L}(n) \\ 0 & m_i(n) \in \overline{\mathcal{L}(n)} \end{cases} , \tag{5.18}$$

with P_{J} the jamming power per symbol, $i = 1, \ldots, M$, and $n = 1, \ldots, N$. In order to evaluate the performance of this type of attack against the defense mechanism, we apply the decision rule defined in Eq. (5.13) and we compute in closed form the corresponding MD probability. This result, besides for the analysis purpose, will be useful in Section 5.5 when deriving the best jammer strategy for minimizing its detectability.

For this computation, we need to take into account that the MD probability at a given time depends on the number of jammed REs that falls into the blanked ones. Therefore, first of all, we define the set $\mathcal{E} = [\mathcal{M}(1) \cap \mathcal{L}(1)] \cup \cdots \cup [\mathcal{M}(N) \cap \mathcal{L}(N)] = \{e_1, \ldots, e_E\}$ (with cardinality $E = |\mathcal{E}|$) of overlapping blanked and jammed REs. Then, by denoting with $\widetilde{\Lambda}'(\mathbf{r}, E; \mathcal{H}_1)$ the test statistic under $\mathcal{H}_1$ in Eq. (5.17) with the new assumption of Gaussian jammer, the MD probability can be computed as

$$\widetilde{P}_{\text{MD}} = \sum_{e=E_{\min}}^{E_{\max}} P\left[\widetilde{\Lambda}'(\mathbf{r}, E; \mathcal{H}_1) < \lambda' | E = e\right] P\left[E = e\right] , \tag{5.19}$$

where the law of total probability has been applied. Moreover,

$$E_{\max} = \min(MN, LN) , \tag{5.20}$$

$$E_{\min} = \begin{cases} 0 & \text{if } M + L < S \\ (M + L - S)N & \text{if } M + L \geq S \end{cases} , \tag{5.21}$$

are the minimum and maximum number of overlapping REs, given M, L, and S. We now need to derive the two factors in Eq. (5.19), i.e., the CDF of the test statistic under $\mathcal{H}_1$ and the probability mass function (PMF) of E.

Starting from the former, the test statistic distribution under $\mathcal{H}_1$, after some computations, results in

$$\widetilde{\Lambda}'(\mathbf{r}, E; \mathcal{H}_1) \sim E \cdot \mathcal{E}\left(\frac{MN}{\sigma_w^2 + \sigma_j^2}\right) + (MN - E) \cdot \mathcal{E}\left(\frac{MN}{\sigma_w^2}\right) , \tag{5.22}$$

where $\mathcal{E}(1/\beta)$ is the exponential distribution with rate parameter $1/\beta$. To derive its CDF, we take advantage of a result in [99, Eq. (9)] on the CDF of the sum of

independent exponential r.v.s:

$$P\left[\widetilde{\Lambda}'(\mathbf{r}, E; \mathcal{H}_1) < \lambda'\right] = 1 - \sum_{i=1}^{2} \sum_{j=1}^{\alpha_i} \sum_{k=0}^{j-1} \frac{\chi_{i,j}}{k!} \left(\frac{\lambda'}{\beta_{\langle i \rangle}}\right)^k \mathrm{e}^{-\frac{\lambda'}{\beta_{\langle i \rangle}}}, \tag{5.23}$$

where $\alpha_1 = E$, $\alpha_2 = MN - E$, $\beta_{\langle 1 \rangle} = \frac{\sigma_w^2 + \sigma_j^2}{MN}$, $\beta_{\langle 2 \rangle} = \frac{\sigma_w^2}{MN}$, and

$$\chi_{i,j} = \left(-\frac{1}{\beta_{\langle i \rangle}}\right)^{\omega_{i,j}} \cdot C_{\alpha_b + \omega_{i,j} - 1, \omega_{i,j}} \cdot \frac{\beta_{\langle b \rangle}^{\omega_{i,j}}}{\left(1 - \frac{\beta_{\langle b \rangle}}{\beta_{\langle i \rangle}}\right)^{\alpha_b + \omega_{i,j}}},$$

with $b \neq i$ and $\omega_{i,j} = \alpha_i - j$.

Finally, we observe that E is a hypergeometric random variable, whose PMF can be written as

$$P[E = e] = \frac{C_{(S-L)N, MN-e} C_{LN,e}}{C_{SN,MN}}, \tag{5.24}$$

where

- $C_{SN,MN}$ is the number of ways to choose MN total blanked subcarriers out of SN total subcarriers;
- $C_{(S-L)N,MN-e}$ is the number of ways to choose $MN - e$ blanked subcarriers (e overlapping subcarriers are fixed) out of $(S - L)N$ subcarriers (LN jammed subcarriers are fixed);
- $C_{LN,e}$ is the number of ways to choose e overlapping subcarriers out of LN total jammed subcarriers.

5.5 Jamming Strategies

A jammer has the two tasks of a) not being detected and b) minimize the system performance. Since expressing an optimization problem that considers both tasks at the same time is not trivial [100], we consider in this work the following three heuristic strategies in order to achieve the above objectives:

- maximize the MD probability, to remain as much undetected as possible, but still transmitting at maximum power;
- minimize the SE, to reduce the performance with MBB type of traffic;
- maximize the BLER, to disrupt a URLLC type of traffic.

Before going through all of them, it has to be pointed out that MD probability, SE, and BLER computed for the optimization problems in this section are the ones estimated by the attacker. Indeed, there are parameters that the jammer cannot exactly compute, therfore we have to make some assumptions on its knowledge of the system. While it is fair that the jammer knows or can estimate many parameters (either because defined by the standard or just because it can listen to BS and UE transmission), some variables cannot be easily tracked by the attacker, like the instantaneous channel between the UE and the BS. Therefore, in general, we assume the jammer to know the format of the transmission like the numerology, the large scale fading, and the noise statistical power at the BS. Moreover, regarding the defensive parameters, it is reasonable to assume that the jammer knows the number of blanked REs M, by

estimating it (since we consider it fixed in time), and the number of symbols N that the defense strategy uses for detection.

All these assumptions about the jammer knowledge of the system could look a bit too optimistic. On the other hand, the typical approach in security problems is to consider an attacker that can know everything that is standard defined, fixed or deterministic, because it can easily estimate those parameters by observing the transmission [101]. As a practical example, the authors in [102] created a demo implementing a jammer with SDR that can synchronize to the legitimate system and learn the necessary parameters to for instance perform an attack on specific physical resource blocks (PRBs).

5.5.1 MD Probability Maximization

A jammer transmitting at maximum power and equally distributing it among the attacked subcarriers L selected in a pseudo-random way, and that also wants to maximize the MD probability, needs to solve the following optimization problem

$$L^* = \underset{1\leq L\leq S}{\arg\max}\, \widetilde{P}_{\mathrm{MD}}(L)\,, \tag{5.25}$$

where $\widetilde{P}_{\mathrm{MD}}(L)$ has been computed in Eq. (5.19). Here we reasonably assume that λ' is known by the jammer. The above optimization problem is not trivial to solve, mainly because the function to maximize is transcendental and L is discrete and present in the bounds of the summation. However, since the objective function depends only on a single discrete variable, the attacker can solve it by performing an exhaustive search to find the optimal value.

5.5.2 SE Minimization

In this case, we assume the jammer to ignore the detectability problem and just try to minimize the system SE. Because of that, the jammer considers here an OFDM system without any blanking and needs to solve the following optimization problem:

$$\begin{aligned} \mathbf{P}_{\mathrm{J}}{}^* = \underset{\mathbf{P}_{\mathrm{J}}\in\mathbb{R}^S}{\arg\min} & \sum_{s=1}^{S} \log_2\left(1+\frac{P_{\mathrm{UE},s}E_h}{\sigma_w^2+P_{\mathrm{J},s}E_g}\right)\,, \\ \text{subject to } & \sum_{s=1}^{S} P_{\mathrm{J},s} = P_{\mathrm{J}} \end{aligned} \tag{5.26}$$

where $\mathbf{P}_{\mathrm{J}} = [P_{\mathrm{J},1}\cdots P_{\mathrm{J},S}]$, and E_h and E_g are the average UE and jammer channel energies, more specifically being $E_h = H^2$ and $E_g = G^2$ with AWGN channel, and $E_h = \sigma_h^2$ and $E_g = \sigma_g^2$ in the Rayleigh scenario. Moreover, we assume that $P_{\mathrm{UE},1}E_h = \cdots = P_{\mathrm{UE},S}E_h = \widehat{P}_{\mathrm{UE}}$.

In order to solve the optimization problem we use the method of Lagrange multipliers. First, we define the Lagrangian function as

$$\begin{aligned} \mathcal{L}\left(\mathbf{P}_{\mathrm{J}},\nu\right) = & \sum_{s=1}^{S} \log_2\left(1+\frac{\widehat{P}_{\mathrm{UE}}}{\sigma_w^2+P_{\mathrm{J},s}E_g}\right) \\ & -\nu\left(\sum_{s=1}^{S} P_{\mathrm{J},s} - P_{\mathrm{J}}\right)\,. \end{aligned} \tag{5.27}$$

Then, we solve the following system of equations:

$$\nabla_{\mathbf{P}_\mathrm{J},\nu}\mathcal{L}\left(\mathbf{P}_\mathrm{J},\nu\right)=0\,. \tag{5.28}$$

By deriving w.r.t. $P_{\mathrm{J},s}$ and w.r.t. ν, we obtain

$$\begin{cases} P_{\mathrm{J},s}=\frac{1}{2E_g}\left[-\left(\widehat{P}_\mathrm{UE}+2\sigma_w^2\right)\pm\sqrt{\widehat{P}_\mathrm{UE}^2-\frac{4\widehat{P}_\mathrm{UE}E_g}{\nu\ln 2}}\right] \\ \sum_{s=1}^{S}P_{\mathrm{J},s}=P_\mathrm{J} \end{cases}, \tag{5.29}$$

and by solving the above system we finally have

$$P_{\mathrm{J},s}=\frac{P_\mathrm{J}}{S}\,, \tag{5.30}$$

i.e., if the jammer wants to minimize the SE, it must perform a wide-band attack.

5.5.3 BLER Maximization

In this attack we still assume the jammer to ignore the detectability issue and try to minimize the system performance, which on the other hand is measured with the BLER as KPI of Eq. (5.4). A formulation of this problem is in general not straightforward at the jammer, as it would require the attacker to know how many and on which resources these packets are scheduled. So here, we consider a suboptimal approach where the jammer assumes F packets scheduled on the N OFDM symbols, each packet allocated to S/F neighbouring subcarriers with no spatial multiplexing, i.e., packets are scheduled next to each other in the frequency domain. Moreover, we still assume that the jammer transmits at full power with equal split among the attacked subcarriers, and if a packet is attacked all the subcarriers of that packet are jammed. Under these assumptions, the jammer just needs to determine how many packets to attack by solving the following optimization problem:

$$L_\mathrm{F}^*=\underset{1\le L_\mathrm{F}\le F}{\arg\max}\,L_\mathrm{F}\cdot\mathrm{BLER}_\mathrm{pkt}(P_J/L_F)\,, \tag{5.31}$$

where $\mathrm{BLER}_\mathrm{pkt}(x)$ is the BLER computed from Eq. (5.4) by considering in the SINR computation average channel energy and x as interference power.

Similarly to the MD probability maximization problem, the optimization problem of Eq. (5.31) is not trivial to solve in closed form. However, as before, since the objective function depends only on a single discrete variable, the attacker can perform an exhaustive search to find the optimal value.

5.6 Numerical Results

We consider an OFDM system with $S=300$ subcarriers, compliant to a 5G numerology with 60 kHz as subcarrier spacing for a 20 MHz bandwidth. The subcarriers are grouped into PRBs, each consisting of $S_P=12$ consecutive subcarriers, and transmission happens in slot of 14 OFDM symbols [84]. Therefore, we have $P=S/S_P=25$ PRBs per slot, and we assume the detection to be performed per slot, i.e., $N=14$. As the PRB is the smallest time-frequency resource that can be scheduled to a device, we implement a 5G standard compliant defense with blanking performed per PRB and, as a consequence, introduce M_P as the number of blanked PRBs per slot. For simplicity, we also assume the jammer to perform attacks on a PRB basis and denote with L_P

the number of jammed PRBs per slot. Basically, these are the PRB-slot version of M and L.

We introduce now some parameters to better define the considered simulation setup:

- $\mathrm{SNR}_{\mathrm{UE}}(n) = P_{\mathrm{UE}}(n)/(S \cdot \sigma_w^2)$ is the UE SNR at OFDM symbol n, where $P_{\mathrm{UE}}(n)$ is the power that the UE allocates at symbol n and evenly distributes among the data subcarriers; in our simulations we set $\mathrm{SNR}_{\mathrm{UE}} = 10\,\mathrm{dB}$;
- $\mathrm{SNR}_{\mathrm{J}}(n) = P_{\mathrm{J}}(n)/(S \cdot \sigma_w^2)$ is the jammer SNR at OFDM symbol n, where $P_{\mathrm{J}}(n)$ is the power that the jammer allocates at symbol n and evenly distributes among the jammed subcarriers.

Moreover, for the Rayleigh case, we consider a block fading model and assume different channel realizations on different PRBs. For URLLC type of traffic, we consider one packet per PRB, with $\rho = 0.48\,\mathrm{bit/s/Hz}$. Finally, we specify that all the KPIs showed in the following figures are the system KPIs, and not the ones estimated by the attacker for its optimization problems.

Let's start with the performance evaluation of the defense strategy, in terms of MD probability as a function of the FA probability, a.k.a. ROC curve. Fig. 5.3 shows the ROC for $M_P = 1, 5$, $L_P = 5, 21$ (an almost narrow- and an almost wide-band jammer), $\mathrm{SNR}_{\mathrm{J}} = 0\,\mathrm{dB}$, and for both AWGN and Rayleigh. First, we notice a huge performance improvement when using $M_P = 5$ when compared to $M_P = 1$, especially with $L_P = 21$ subcarriers and AWGN: in fact, while with $M_P = 1$ the MD is almost always above 10^{-1} for the considered range of target FA, with $M_P = 5$ the detection performance strongly improves. Moreover, we also observe that while the narrow-band jammer ($L_P = 5$) is hardly detectable, the wide-band one can be easily spotted by the proposed method even if we have small jamming power. Finally, results show that detection in a AWGN scenario is far easier when compared to detection in a more random channel like the Rayleigh considered here.

To evaluate the performance degradation with a MBB type of traffic, Fig. 5.4 shows the SE as a function of $\mathrm{SNR}_{\mathrm{J}}$ with $M_P = 5$, for the almost narrow- and almost wide-band attack, and for a system with no blanking and no jamming that provides an upper bound to the proposed method. First, we notice, as expected, a small performance loss of the proposed method against the upper bound at very low

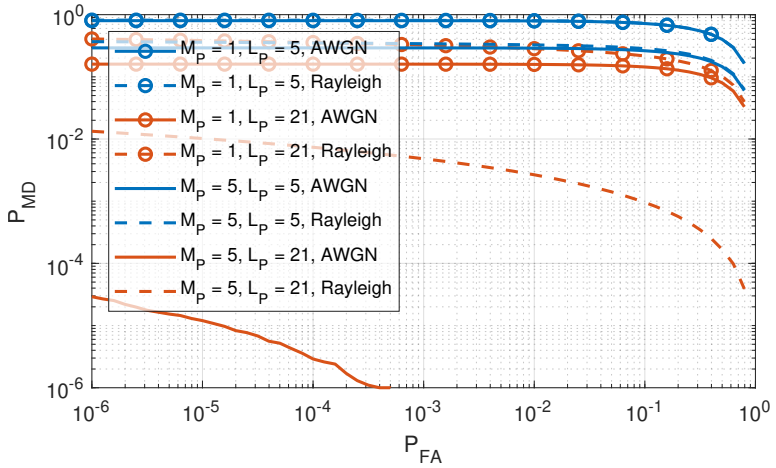


FIGURE 5.3: ROC curves for different M_P, L_P, and channel type. Here $\mathrm{SNR}_{\mathrm{J}} = 0\,\mathrm{dB}$.

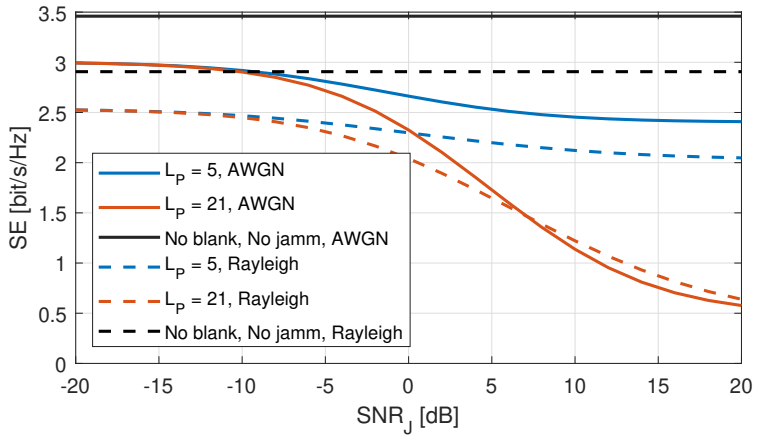


FIGURE 5.4: SE versus $\mathrm{SNR_J}$ for different L_P and channel type. Here $M_P = 5$.

jamming power because of the PRB blanking. Moreover, while the wide-band attack causes significant SE loss, especially for high $\mathrm{SNR_J}$, the narrow-band attack, that resulted in Fig. 5.3 to be more stealthy, only slightly limits the system SE. In fact, the performance degradation caused by an attack that is not fully wide-band saturates as the jammer $\mathrm{SNR_J}$ increases because of the presence of not jammed PRBs.

Concerning the URLLC type of traffic, Fig. 5.5 shows the BLER as a function of $\mathrm{SNR_J}$ for $L_P = 5, 21$ jammed PRBs and $M_P = 5$ blanked PRBs. In the AWGN channel, we observe that with limited jamming power, a narrow-band attack allows the jammer to strongly degrade the performance and at the same time avoid the blanked PRBs. But, as its power increases, the BLER reaches a saturation value, which depends on the probability of intersection between blanked and jammed PRBs, and for higher $\mathrm{SNR_J}$ it should switch to a wide-band attack. When looking at the Rayleigh case, we observe that, in general, the system performs worse than the AWGN case, apart from high values of $\mathrm{SNR_J}$ for which, however, the BLER is anyway quite high. Moreover, even in almost absence of jamming, the BLER reaches a lower value of about $3 \cdot 10^{-2}$: this can be improved by considering diversity techniques or a more robust coding rate.

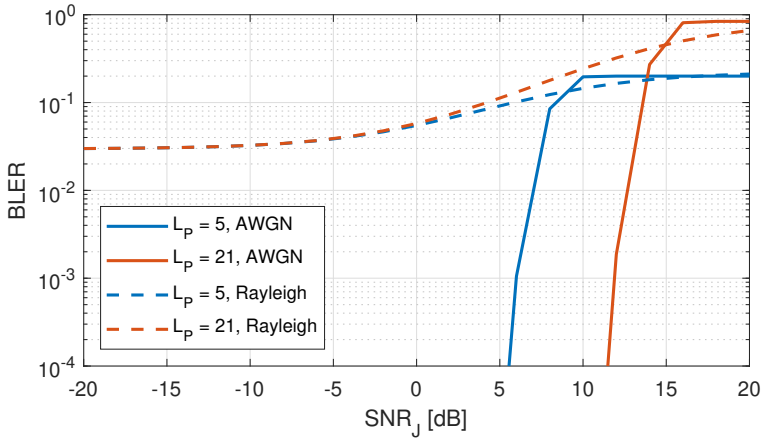


FIGURE 5.5: BLER versus $\mathrm{SNR_J}$ for different L_P and channel type. Here $M_P = 5$.

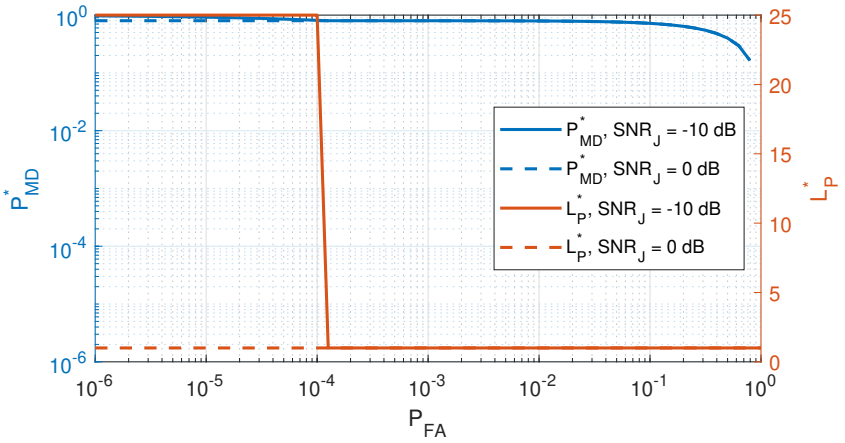


FIGURE 5.6: Optimal P_{MD} (left y-axis) and optimal L_P (right y-axis) versus P_{FA} for different SNR_{J}. Here $M_P = 5$ and AWGN is considered.

In Fig. 5.6 we evaluate the jammer strategy for MD maximization proposed in Section 5.5.1 by showing for $\text{SNR}_{\text{J}} = -10, 0\,\text{dB}$ the best MD probability achievable by the attacker and the corresponding number of jammed PRBs to achieve it. For the low power jammer, i.e., $\text{SNR}_{\text{J}} = -10\,\text{dB}$, we notice that if the defender's target FA probability is $P_{\text{FA}} \gtrsim 10^{-4}$, the best approach for the jammer is to perform a narrow-band attack; this happens because the defense tends to accept the $\mathcal{H}_1$ hypothesis more easily, and therefore the attacker tries to avoid the blanked PRBs by transmitting on a smaller number of PRBs. On the other hand, for $P_{\text{FA}} \lesssim 10^{-4}$, the jammer best strategy is a wide-band attack because, in this way, it evenly distributes its power among all the subcarriers. On the contrary, with a higher jamming power, i.e., $\text{SNR}_{\text{J}} = 0\,\text{dB}$, we see that the optimal strategy is the narrow-band attack for the entire FA probability interval that we consider.

In Section 5.5.2 we showed that the best strategy to minimize the SE is a wide-band attack, while in Fig. 5.6 we learned that, on the contrary, in many cases the narrow-band attack is the best strategy to maximize the MD, thus suggesting a trade-off between MD probability and SE. In Fig. 5.7 we evaluate this trade-off by showing the MD probability versus the SE, for different values of L_P and SNR_{J}, and for $P_{\text{FA}} = 10^{-3}$. The optimal situation for the attacker would be to achieve high P_{MD} and low SE, but, for the considered range of SNR_{J}, there is a maximum that can be achieved and, depending on its objective, the jammer needs to give up on SE reduction if it wants to increase the MD and viceversa.

Finally, Fig. 5.8 considers the BLER maximization problem of Section 5.5.3 and shows the MD probability versus the BLER, for different values of L_P and SNR_{J}, and for $P_{\text{FA}} = 10^{-3}$. These results show that if the jammer has low power, for instance with $\text{SNR}_{\text{J}} = 0\,\text{dB}$, it cannot achieve high BLER and at the same time stay undetected. On the other hand, by looking at the top-right region of the plot, we observe that a jammer with a sufficiently high power can use a narrow-band attack to achieve high BLER and high P_{MD}: for instance, with $12\,\text{dB} \lesssim \text{SNR}_{\text{J}} \lesssim 20\,\text{dB}$ and $5 \lesssim L_P \lesssim 15$, it obtains $P_{\text{MD}} > 10^{-1}$ and $\text{BLER} > 10^{-1}$.

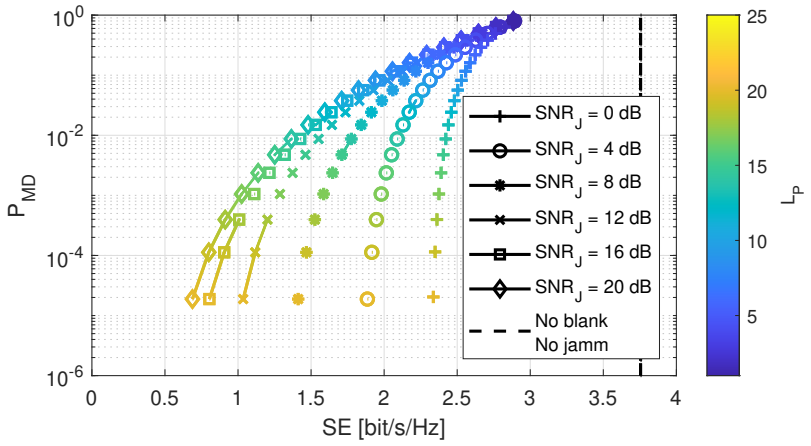


FIGURE 5.7: P_{MD} versus SE for different SNR_J. Here $P_{\text{FA}} = 10^{-3}$, $M_P = 5$, and AWGN is considered.

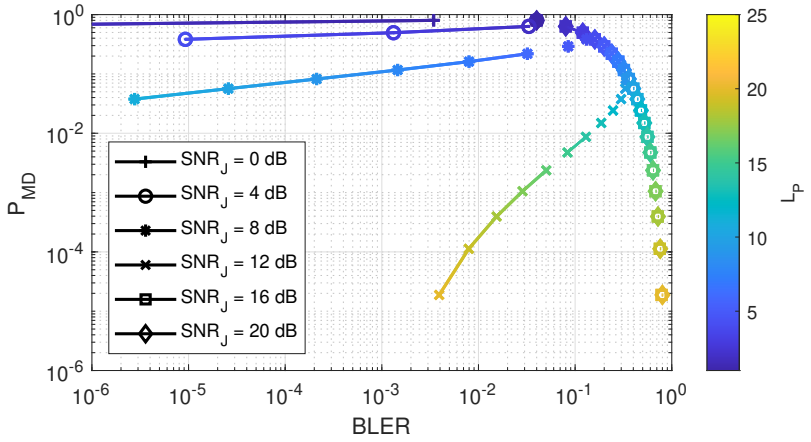


FIGURE 5.8: P_{MD} versus BLER for different SNR_J. Here $P_{\text{FA}} = 10^{-3}$, $M_P = 5$, and AWGN is considered.

5.7 Conclusions

In this Chapter, we considered the problem of jamming detection for 5G-and-beyond in Industry 4.0 scenarios, with particular focus on MBB and URLLC type of traffic. We designed a method based on pseudo-random blanking of subcarriers in an OFDM system and performing a GLRT on them that resulted to be an energy detector. We found that a wide-band jammer is far more detectable than a narrow-band one, however causing a more severe degradation to KPIs. We then considered a smart jammer following three types of strategies: remain as stealthy as possible, maximize the damage to MBB communication, and maximize the disruption of URLLC type of traffic. Results show that, while for a MBB traffic the jammer has to compromise between MD and SE, with URLLC traffic, a smart jammer with sufficiently high power can achieve good results in reaching both high values of MD probability and BLER.

Chapter 6

Jamming Resilient Indoor Factory Deployments

6.1 Introduction

In this Chapter we extend the jamming detection proposal in Chapter 5 by providing realistic performance evaluations that consider indoor factory deployments with 3GPP spatial channel model. Moreover, we propose a new detector that exploits antenna correlation at the receiver. Finally, we consider jamming mitigation techniques with frequency hopping and random scheduling of the UEs. The benefits of the proposed schemes are evaluated in terms of jamming detection probability and BLER performance with URLLC.

Notation for this Chapter. We use $(\cdot)^{\mathrm{H}}$ to denote conjugate transpose. $\|\mathbf{x}\|$ indicates the norm of vector $\mathbf{x}$. $|\cdot|$ denotes the absolute value. $[\mathbf{x}]_n$ is the n-th entry of vector $\mathbf{x}$. $F_X^{-1}(x)$ denotes the inverse of the CDF of the r.v. X evaluated at x.

6.2 System Model

We consider an industrial scenario as in Fig. 6.1 with a factory hall of dimensions $100 \times 50 \times 6$ m, and with N_{AP} APs mounted on the factory ceiling. In the whole factory we deploy a total of N_{ant} omni-directional antennas so that each AP is equipped with a square antenna array with $N_{\mathrm{ant}}^{(\mathrm{AP})} = N_{\mathrm{ant}}/N_{\mathrm{AP}}$ antennas. The following AP deployments are considered [87]:

- *Centralized deployment*: $N_{\mathrm{AP}} = 1$ AP placed at the center of the factory hall;
- *Partially distributed deployment*: $N_{\mathrm{AP}} = 4$ APs located such that the inter-AP distance (IAD) along the longest side is 50 m and the IAD along the shortest side is 25 m. An example of this deployment is reported in Fig. 6.1.
- *Fully distributed deployment*: $N_{\mathrm{AP}} = 16$ APs located such that the IAD along the longest side is 25 m and the IAD along the shortest side is 12.5 m.

We have N_{UE} UEs active and each UE is randomly dropped within the factory at an height of 1.5 m, is equipped with a single omni-directional antenna and transmits with power $P_{\mathrm{UE}} = 10\,\mathrm{dBm}$.

We assume a system operating at a central carrier frequency of $f_{\mathrm{C}} = 3.75\,\mathrm{GHz}$. Regarding the channel model, we consider the proposal in [103], where the 3GPP indoor office (InO) model is used as starting point and path-loss, shadowing, and LOS probability values are chosen on the basis of extensive measurements done in two different operational factories. In detail, this novel indoor industrial (InI) model considers different deployments, distinguishing i) elevated from clutter-embedded APs

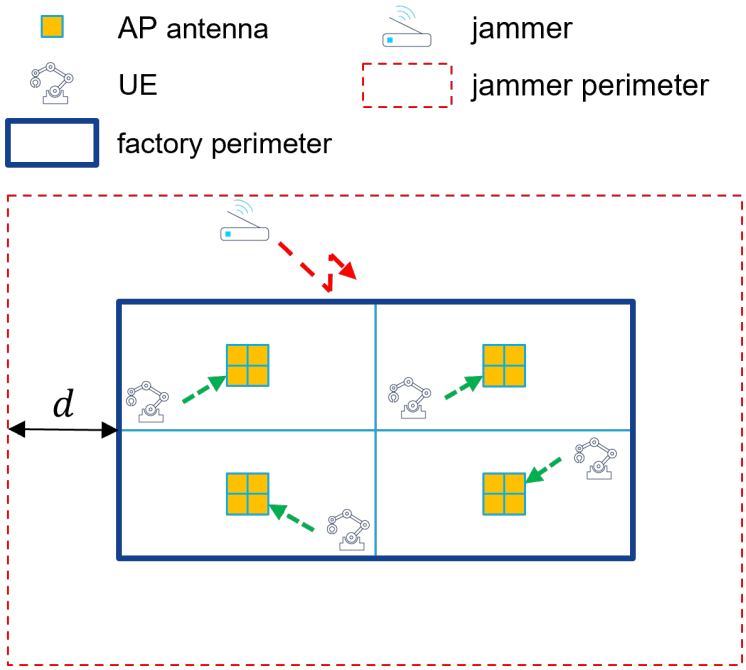


FIGURE 6.1: Representation of the considered UL scenario for the partially distributed deployment ($N_{\text{AP}} = 4$) and a total of $N_{\text{ant}} = 16$ antennas.

and ii) open production spaces from dense factory clutter, and proposing for each configuration specific values of the aforementioned large-scale fading parameters; all the details are reported in [103, Tab. 3]. In this work we focus on the dense factory clutter model with clutter-embedded APs.

6.2.1 Numerology and Resource Allocation

We adopt an OFDM modulation compliant to the 5G numerology with 60 kHz subcarrier spacing. The subcarriers are grouped into PRBs, each consisting of $N_{\text{sc}} = 12$ consecutive subcarriers over a transmission interval of $N_{\text{symb}} = 14$ OFDM symbols [84]. Therefore, each PRB consists of $N_{\text{RE}}^{(\text{PRB})} = N_{\text{sc}} \cdot N_{\text{symb}} = 168$ REs and has a bandwidth of $B_{\text{PRB}} = 720$ kHz. We consider two scenarios for our system: a total bandwidth of $B = 20$ MHz (with a total number of PRBs $N_{\text{PRB}} = 25$) with $N_{\text{UE}} = 4$ UEs, and a total bandwidth of $B = 100$ MHz ($N_{\text{PRB}} = 125$) with $N_{\text{UE}} = 20$ UEs: in both cases we set the guard band to be 10% of B. We assume URLLC traffic, such that each UE transmits a small packet of size $C = 20$ bytes in each slot, with no retransmission opportunities because of the tight latency constraint. We consider a resource allocation where interference among the active UEs is managed by allocating different UEs on different PRBs, i.e., the only interference source in the system is the jammer. The PRBs available for data transmissions are then evenly shared among the UEs, that apply equal power allocation on them. More details about the allocation of UEs to PRBs is part of the jamming mitigation strategy and will be described in Section 6.3.

6.2.2 Jammer Model

We consider an attacker stationed outside the factory at height of 1.5 m and dropped randomly within a rectangular perimeter with sides $d = 10$ m far from the factory walls (see Fig. 6.1). The jammer is equipped with a single omni-directional antenna element

that transmits with power P_{J}, ranging from 20 dBm to 60 dBm [88]. Moreover, we assume the jammer to allocate equal power on the attacked PRBs and consider both a) a wide-band jammer that attacks the whole bandwidth and b) a narrow-band jammer attacking a few PRBs but with stronger power spectral density. Finally, we assume for the jammer the same InI channel model as for the UEs inside the factory, but adding a factory wall penetration loss modelled as a Gaussian r.v. $\mathrm{PL}_{\mathrm{wall}} \sim \mathcal{N}(\mu_P, \sigma_P^2)$, with mean $\mu_P = 27.5$ dB and standard deviation $\sigma_P = 6.5$ dB [104, Tab. 7.4.3-2].

6.2.3 Imperfect CSI

We assume a TDD setup with pilot sequence length $T = 16$ [87]. Note that here we have no pilot contamination as different UEs are scheduled on different PRBs, but jamming affects channel estimation. Let $\mathbf{h}_{i,j}$ be the $(1 \times N_{\mathrm{ant}}^{(\mathrm{AP})})$-dimensional channel vector from the i-th UE to the j-th AP on a certain PRB, with $i = 1, \ldots, N_{\mathrm{UE}}$, and $j = 1, \ldots, N_{\mathrm{AP}}$. The minimum mean squared error (MMSE) estimate $[\widehat{\mathbf{h}}_{i,j}]_n$ of $[\mathbf{h}_{i,j}]_n$ can be defined as [87, Eq. (6)]:

$$[\widehat{\mathbf{h}}_{i,j}]_n = \frac{\gamma_{i,j} T}{1 + \gamma_{i,j} T} \left([\mathbf{h}_{i,j}]_n + z_i \right) , \tag{6.1}$$

where $\gamma_{i,j} = P_{\mathrm{UE},i}^{(\mathrm{PRB})} \sigma_{h_{i,j}}^2 / \sigma_w^2$ is the SNR of UE i at AP j and $z_i \sim \mathcal{CN}(0, (\sigma_w^2 + P_{\mathrm{J}}^{(\mathrm{PRB})} \sigma_{h_{\mathrm{J},j}}^2)/(P_{\mathrm{UE},i}^{(\mathrm{PRB})} T))$ is a complex Gaussian r.v. representing noise and interference on channel estimation. In particular, $P_{\mathrm{UE},i}^{(\mathrm{PRB})}$ is the power of UE i allocated to a single PRB, $\sigma_{h_{i,j}}^2$ denotes the large-scale fading attenuation between UE i and AP j, and σ_w^2 is the noise statistical power on a single PRB, computed considering a noise figure of 7 dB at the receiver. Moreover, $P_{\mathrm{J}}^{(\mathrm{PRB})}$ is the jammer power allocated to a single PRB and $\sigma_{h_{\mathrm{J},j}}^2$ is the large-scale fading attenuation between the jammer and AP j. From Eq. (6.1) we observe that channel estimation is also affected by jamming, and this is modelled through the term z_i, where the jamming power component is present.

6.2.4 Beamforming at the Receiver

At the receiver, we assume joint reception (JR), such that the signals received by the APs are combined in a central unit. Since there is no interference among the active UEs in our framework, because they are scheduled on different subbands, we adopt maximum ratio combining (MRC), that maximizes the UE SNR and is easy to implement in a distributed MIMO setup. We leave for further studies the design and evaluation of more advanced beamforming that creates nulls toward an estimated jammer channel such as in [93]. We denote with $\widehat{\mathbf{h}}_i = [\widehat{\mathbf{h}}_{i,1}, \widehat{\mathbf{h}}_{i,2}, \ldots, \widehat{\mathbf{h}}_{i,N_{\mathrm{AP}}}]$ the $(1 \times N_{\mathrm{ant}})$-dimensional vector collecting the estimated channels between the i-th UE and all the APs. The MRC beamforming is then defined as:

$$\mathbf{g}_i = \widehat{\mathbf{h}}_i^{\mathrm{H}} / \|\widehat{\mathbf{h}}_i\| . \tag{6.2}$$

6.2.5 System KPI

In order to quantify the impact of the jammer to the system, we introduce two KPIs: SINR on data transmission and BLER. We define the SINR of UE i on a certain PRB,

whose index is skipped for the sake of clarity, as

$$\mathrm{SINR}_i = \frac{|\mathbf{h}_i \mathbf{g}_i|^2 P_{\mathrm{UE},i}^{(\mathrm{PRB})}}{\sigma_w^2 + |\mathbf{h}_{\mathrm{J}} \mathbf{g}_i|^2 P_{\mathrm{J}}^{(\mathrm{PRB})}}\,, \tag{6.3}$$

where at the denominator we have the malicious interference from the jammer, with $\mathbf{h}_{\mathrm{J}}$ the $(1 \times N_{\mathrm{ant}})$-dimensional channel vector collecting the channels between the jammer and all the AP antennas.

We assume that UE i sends its packet over F_i PRBs and define $C_{\mathrm{cod},i} = F_i \cdot N_{\mathrm{RE}}^{(\mathrm{PRB})}$ as the number of REs allocated to that packet. Then, for our analysis, we use the exponential effective SINR metric (EESM) as link-to-system mapping criterion [96, Eq. (3)] to compute, as a function of the different SINRs of Eq. (6.3) experienced by a certain UE on different PRBs, a single $\mathrm{SINR}_{\mathrm{pkt}}$, that represents the equivalent SINR for the packet. We then use this $\mathrm{SINR}_{\mathrm{pkt}}$ to compute the BLER of UE i from the normal approximation of the finite blocklength capacity [97, Eq. (5)]:

$$\mathrm{BLER}_{\mathrm{pkt},i} = Q\left(\left[\log_2\left(1 + \mathrm{SINR}_{\mathrm{pkt},i}\right) - \rho_i + \frac{\log_2 \widetilde{C}_{\mathrm{cod},i}}{2\widetilde{C}_{\mathrm{cod},i}}\right]\sqrt{\frac{\widetilde{C}_{\mathrm{cod},i}}{V}}\right), \tag{6.4}$$

where V is the channel dispersion [97, Eq. (8)], $\rho_i = C/\widetilde{C}_{\mathrm{cod},i}$ is the spectral efficiency for the UE i packet, and $\widetilde{C}_{\mathrm{cod},i} = C_{\mathrm{cod},i}(1 - O)$ is the coded packet size in REs taking into account the system overhead $O = 0.25$ for control and pilots.

6.3 Defense Strategy

In this work we consider the defense strategy framework for performing jamming detection that we initially proposed in [13], where some PRBs in each slot are blanked in a pseudo-random manner, such that the attacker cannot predict in advance which resources will be used for transmission and which will be blanked. In detail, in each slot all the UEs blank a set $\mathcal{M}_P \subset \{1, \ldots, N_{\mathrm{PRB}}\}$ (with cardinality $M_P = |\mathcal{M}_P|$) of PRBs, where the set elements are chosen in a pseudo-random manner; the remaining PRBs are used for data transmission. At the same time, the attacker transmits on a set $\mathcal{L}_P \subseteq \{1, \ldots, N_{\mathrm{PRB}}\}$ (with cardinality $L_P = |\mathcal{L}_P|$) of PRBs, where the set elements are chosen according to the jammer strategy. In this work we assume that the jammer chooses the attacked PRBs pseudo-randomly and it evenly splits its power among them. Moreover, for the sake of notation, when $L_P = N_{\mathrm{PRB}}$ we refer to the attacker as a wide-band jammer, otherwise we call it narrow-band jammer.

6.3.1 Jamming Detection Strategies

The detection strategy takes advantage of the blanked PRBs to detect the presence of jamming by means of statistical hypothesis testing [75]. Moreover, we assume that jamming detection is performed by a central unit collecting the signals received from all the APs distributed in the factory hall. The two hypotheses for the sequence of blanked PRBs are as follows:

- There is no jamming and we have just thermal noise (null hypothesis $\mathcal{H}_0$);
- There is jamming (alternative hypothesis $\mathcal{H}_1$).

The above hypotheses translate to the following hypothesis test:

$$\begin{cases} \mathcal{H}_0 : \mathbf{r} = \mathbf{w} \\ \mathcal{H}_1 : \mathbf{r} = \mathbf{w} + \mathbf{j} \end{cases}, \tag{6.5}$$

where $\mathbf{r}$, $\mathbf{w}$, and $\mathbf{j}$ are $((N_{\mathrm{RE}} \cdot N_{\mathrm{ant}}) \times 1)$-dimensional vectors, with $N_{\mathrm{RE}} = M_P \cdot N_{\mathrm{RE}}^{(\mathrm{PRB})}$, containing the samples of the blanked REs of all the antennas. In particular, $\mathbf{r}$ is the total received signal by the APs, $\mathbf{w}$ is the noise vector with elements $[\mathbf{w}]_n \sim \mathcal{CN}(0, \sigma_w^2/N_{\mathrm{RE}}^{(\mathrm{PRB})})$, and $\mathbf{j}$ is the jamming signal with unknown distribution. Then, the test decides for $\mathcal{H}_1$ if

$$T(\mathbf{r}) > \delta\,, \tag{6.6}$$

where $T(\mathbf{r})$ is the test statistic and δ is the threshold, which depends on the test statistic and is function of a target FA probability P_{FA}, i.e., the probability of declaring jamming even if it is not present. Then, in Section 6.4 we will evaluate the effectiveness of the proposed detection technique against a Gaussian jammer in terms of MD probability P_{MD}, i.e., the probability of declaring no-jamming even if it is present. Note that with Eq. (6.5) we perform jamming detection in each slot: however, the proposed scheme can be applied, depending on the use case, also to multiple slots for improved performance. Regarding the test statistic, we now propose two options.

6.3.1.1 GLRT

This test defines the test statistic simply as [13]

$$T_{\mathrm{GLRT}} = \frac{\|\mathbf{r}\|^2}{N_{\mathrm{RE}} \cdot N_{\mathrm{ant}}}\,, \tag{6.7}$$

which is an energy detector. The threshold for this detector is derived as

$$\delta_{\mathrm{GLRT}} = F^{-1}_{T_{\mathrm{GLRT}}(\mathbf{r};\mathcal{H}_0)}(1 - P_{\mathrm{FA}})\,, \tag{6.8}$$

where $T_{\mathrm{GLRT}}(\mathbf{r};\mathcal{H}_0) \sim \mathrm{Gamma}\left(N_{\mathrm{RE}} \cdot N_{\mathrm{ant}}, \frac{\sigma_w^2/N_{\mathrm{RE}}^{(\mathrm{PRB})}}{N_{\mathrm{RE}} \cdot N_{\mathrm{ant}}}\right)$ is the test statistic distribution under $\mathcal{H}_0$, with $\mathrm{Gamma}(k, \theta)$ being the gamma distribution with shape parameter k and scale parameter θ. The main advantage of this detector is the very low computational complexity, as just the received power on the blanked PRBs needs to be computed.

6.3.1.2 RLRT

Differently from the GLRT, this test exploits the channel correlations among the AP antennas. For deriving the test statistic, we follow the following procedure:

1. We denote with $\mathbf{r}_m$, $m = 1, 2, ..., N_{\mathrm{RE}}$ the column vector collecting the entries of $\mathbf{r}$ received by all antennas on RE m.
2. We define $\mathbf{R} = [\mathbf{r}_1, \ldots, \mathbf{r}_{N_{\mathrm{RE}}}]$, which is a $(N_{\mathrm{ant}} \times N_{\mathrm{RE}})$-dimensional matrix.
3. We compute the sample covariance matrix as $\mathbf{C} = \frac{1}{N_{\mathrm{RE}}}\mathbf{R}\mathbf{R}^{\mathrm{H}}$.
4. Given λ the largest eigenvalue of $\mathbf{C}$, we define the test statistic as [105]

$$T_{\mathrm{RLRT}} = \frac{\lambda}{\sigma_w^2}\,. \tag{6.9}$$

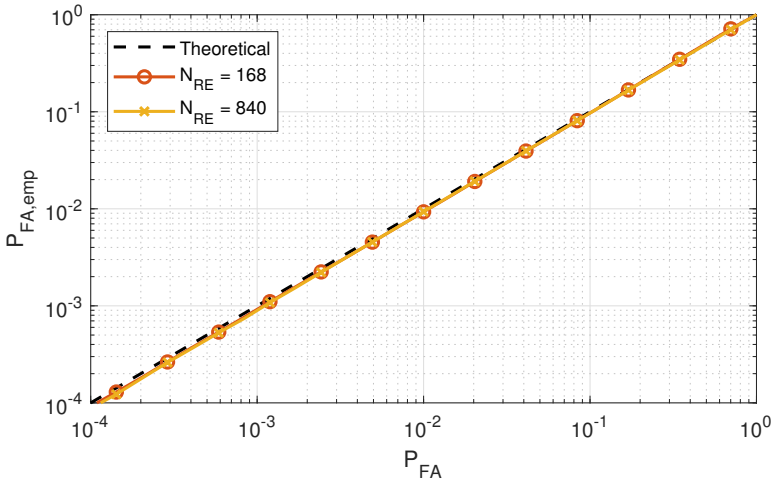


FIGURE 6.2: Empirical FA probability versus target FA probability for $N_{\text{ant}} = 16$.

The threshold for this detector is derived as

$$\delta_{\text{RLRT}} \approx \mu + \xi \cdot F_{\text{TW2}}^{-1}(1 - P_{\text{FA}}) \,, \tag{6.10}$$

where TW2 is the Tracy-Widom distribution of 2$^{\text{nd}}$ order, while μ and ξ depend on N_{ant} and N_{RE}. In particular, authors in [105] show that the approximation holds for $N_{\text{ant}}, N_{\text{RE}} \to \infty$.

When compared to the GLRT, with this detector we exploit the spatial correlation among antennas. The computational complexity increases, but is still very low as we just need to compute an eigenvalue. A second potential disadvantage is that the approximation in Eq. (6.10) creates a mismatch between empirical and target FA probabilities. Therefore, in order to evaluate the impact of this mismatch, in Fig. 6.2 we show the empirical FA probability derived in an authentic scenario, i.e., a scenario without jamming, versus the target FA probability, for a factory with $N_{\text{ant}} = 16$ antennas. Three different curves are displayed: a theoretical one, for which the two probabilities coincide, and two empirical curves corresponding to $N_{\text{RE}} = 168, 840$ (i.e., $M_P = 1, 5$). As we can see, both the empirical curves are close to the theoretical one, meaning that the approximation Eq. (6.10) holds very well even with realistic low values of N_{ant} and N_{RE}.

6.3.2 Jamming Mitigation Strategies

Alongside the above detection strategy, we consider two jamming mitigation schemes designed for narrow-band attacks: one based on user scheduling and the other one exploiting the pseudo-random blanking concept.

In Section 6.4 we will assume *sequential scheduling* as baseline, such that adjacent PRBs are allocated to each active UE. As a first mitigation strategy, we consider *random scheduling*, where PRBs are allocated to each UE in a pseudo-random way, with the constraint that still, as introduced in Section 6.2.1, a PRB is allocated to just one active UE, to guarantee orthogonality among UEs. The purpose of this approach is to counteract smart jammers that can learn allocation and, for instance, focus their attack on a specific subband that is used by just one or few UEs. With this method then the jammer cannot know in advance which UE will be scheduled on each PRB.

As a second mitigation strategy, we consider *frequency hopping*, where in each slot just a small number of PRBs is used for transmission, and that is implemented in our framework by greatly increasing the number of blanked PRBs M_P. The main objective is to lower the probability of intersection between jammed and data PRBs, so advantages of frequency hopping are expected with narrow- rather than wide-band jammers. When using a large number of blanked PRBs, the same packet needs to be transmitted on a lower number of data PRBs but with higher power per PRB, i.e., a higher packet spectral efficiency is needed in Eq. (6.4), but higher SINR is also experienced on those data PRBs: that, in fact, can be beneficial in certain interference conditions. Moreover, a large number of blanked PRBs has the benefit of performing jamming detection on more resources, thus decreasing the MD probability.

6.4 Numerical Results

In this section we show the numerical results obtained by performing Monte Carlo simulations of the above described system. In particular, we focus on the system KPIs degradation caused by the jammer and on the MD probability of the attacker. If not otherwise specified, the following parameters are used for the simulations: $N_{\text{ant}} = 64$ antennas, high power jammer with $P_{\text{J}} = 60\,\text{dBm}$, $M_P = 5$ blanked PRBs, and random scheduling of UEs.

Fig. 6.3 shows the CDF of the SINR for $N_{\text{AP}} = 1, 4, 16$, $B = 20\,\text{MHz}$, $P_{\text{J}} = 20, 60\,\text{dBm}$ (low- and high-power jammer), and $L_P = 25$ (wide-band jammer). Moreover, the SNR curves are also shown, representing a jamming free scenario. First, we notice as expected that the SINR is higher in the distributed deployments, i.e., with higher N_{AP}, because some of the AP antennas are closer to the UEs. On the other hand, with jamming the SINR gap among the deployments is reduced when compared to the jamming free scenario: that happens because some of the AP antennas are, with the distributed approaches, also closer to the jammer stationed outside the factory. Finally, we observe that, while on the median the SINR is still quite high even with a high-power jammer, on lower quantiles the SINR is strongly affected, for instance

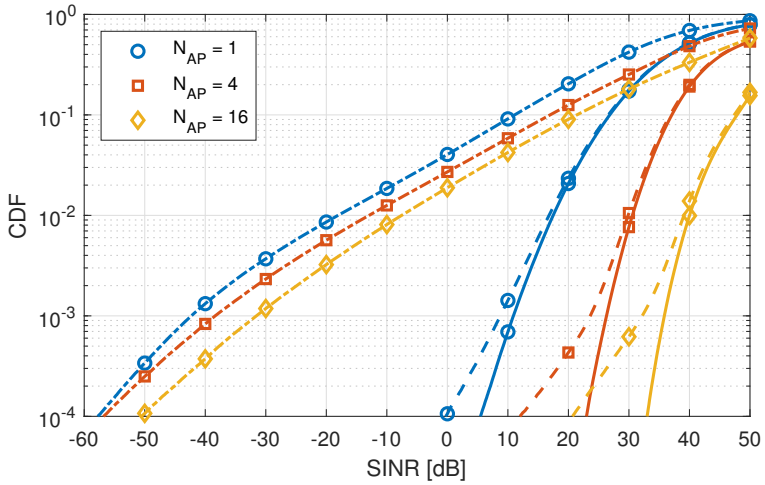


FIGURE 6.3: CDF of SINR for $B = 20\,\text{MHz}$ and $L_P = 25$. Continuous lines are without jamming, dashed lines for $P_{\text{J}} = 20\,\text{dBm}$, and dash-dotted lines for $P_{\text{J}} = 60\,\text{dBm}$.

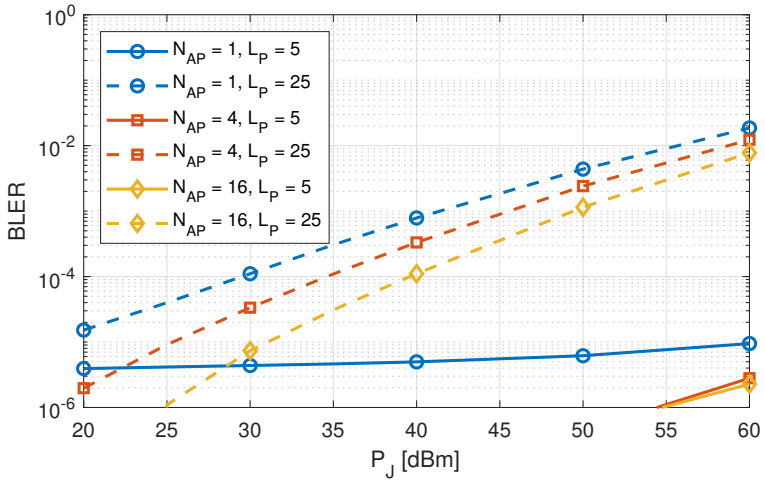


FIGURE 6.4: BLER versus P_{J} for $B = 20\,\mathrm{MHz}$.

with about 50 dB loss at the 1st percentile, i.e., considering a CDF value of 0.01, with $N_{\mathrm{AP}} = 16$.

To evaluate the performance degradation with URLLC type of traffic, Fig. 6.4 shows the BLER of Eq. (6.4) as a function of P_{J} for $N_{\mathrm{AP}} = 1, 4, 16$, $B = 20\,\mathrm{MHz}$, and $L_P = 5, 25$ (narrow- and wide-band jammer). Better BLER is achieved by the distributed deployments. Moreover, we observe that the wide-band attack is much more harmful than the narrow-band attack, and a huge BLER degradation is observed with a wide-band jammer: for instance, BLER increases with $N_{\mathrm{AP}} = 4$ from about 10^{-6} to 10^{-2} when we increase the jamming power from 20 dBm to 60 dBm.

Regarding the performance evaluation of the defense strategy, Fig. 6.5 shows the MD probability as a function of the FA probability, a.k.a. ROC curve, for $B = 20\,\mathrm{MHz}$, $L_P = 25$, and comparing GLRT against Roy's largest root test (RLRT) detectors. The first thing to notice is that the MD probability is lower, i.e., better, in the distributed approaches because AP antennas are closer to the jammer. Then, MD probability is slightly lower with the RLRT detector for relevant values of FA probability, confirming that exploiting spatial correlation among antennas brings benefit to the detection.

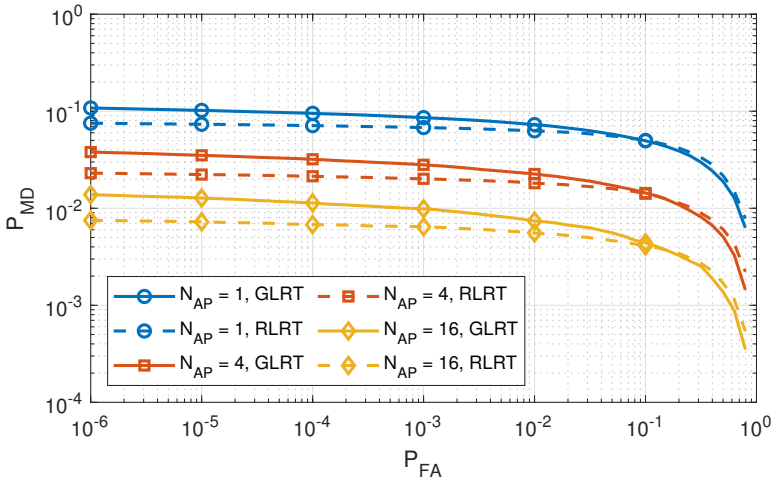


FIGURE 6.5: P_{MD} versus P_{FA} for $B = 20\,\mathrm{MHz}$ and $L_P = 25$.

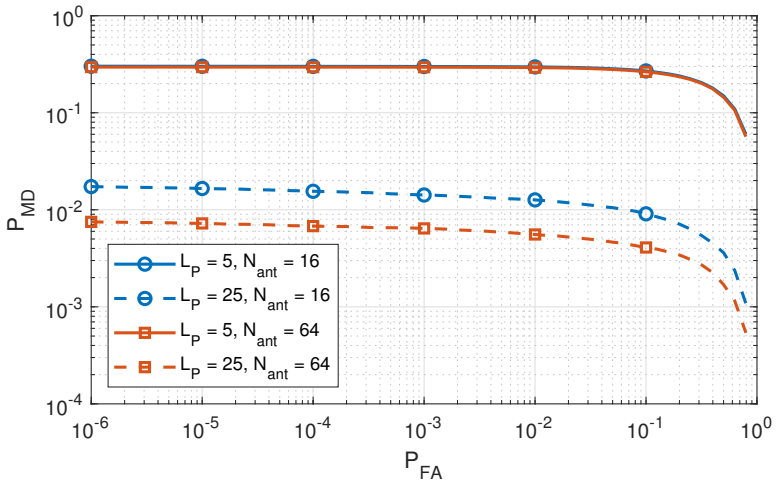


FIGURE 6.6: P_{MD} versus P_{FA} for $N_{\text{AP}} = 16$, $B = 20\,\text{MHz}$, and RLRT detector.

In Fig. 6.6 we show the ROC curve for $N_{\text{AP}} = 16$, $B = 20\,\text{MHz}$, $N_{\text{ant}} = 16, 64$, $L_P = 5, 25$, and RLRT detector. Lower MD probability is achieved with more AP antennas. On the other hand, in the narrow-band case MD probability is high and similar for different number of antennas, because limited by the probability of intersection between blanked and jammed PRBs.

As last result regarding the detection performance, in Fig. 6.7 we report the ROC curve for $N_{\text{AP}} = 16$, $B = 100\,\text{MHz}$, $M_P = 5, 85$, $L_P = 5, 25, 125$ (very narrow-band, narrow-band and wide-band jammer), and RLRT detector. In this case, thanks to the larger number of available PRBs, a massive blanking approach can be implemented and, indeed, MD probability is lower with more blanked PRBs. Moreover, with massive blanking MD probability is similar across the different jamming strategies, thus allowing to better detect narrow-band jammers.

Regarding the comparison among the different mitigation strategies with a wide-band jammer, Fig. 6.8 shows BLER as a function of P_{J} for $N_{\text{AP}} = 1$, $B = 100\,\text{MHz}$, random and sequential scheduling, $M_P = 5, 85$, and $L_P = 125$. First, we observe

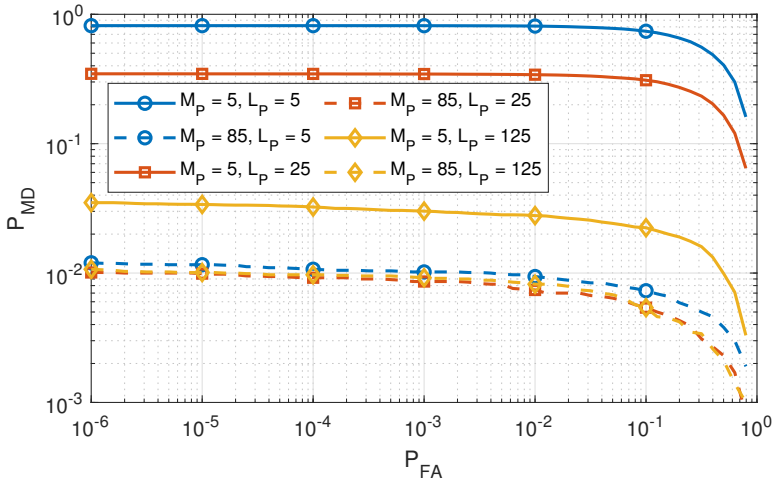


FIGURE 6.7: P_{MD} versus P_{FA} for $N_{\text{AP}} = 16$, $B = 100\,\text{MHz}$, and RLRT detector.

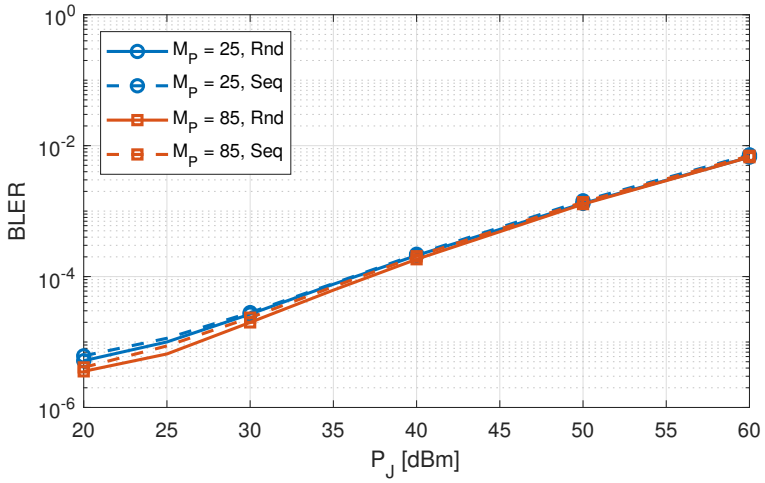


FIGURE 6.8: BLER versus P_{J} for $N_{\text{AP}} = 1$, $B = 100\,\text{MHz}$, and $L_P = 125$.

that the scheduling-based mitigation works although just a very small improvement is achieved by random scheduling when compared to the sequential one. Then, similar BLER is obtained by using the full bandwidth (small M_P) and frequency hopping (large M_P): with a wide-band jammer and the considered parameters, the increase in SINR with frequency hopping just compensates the reduced bandwidth.

Regarding the comparison among the different mitigation strategies, we consider Fig. 6.9, which reports BLER as a function of P_{J} for for $N_{\text{AP}} = 1$, $B = 100\,\text{MHz}$, random and sequential scheduling, $M_P = 25, 85, 105$, and $L_P = 25$. First, we notice that the scheduling-based mitigation works, although just a very small improvement is achieved by random scheduling when compared to the sequential one. Then, we observe a trade-off when applying frequency hopping: small M_P (large bandwidth for data transmission) provides better performance in most ranges, but frequency hopping (large M_P) starts obtaining better performance when the jamming power is low, under whose conditions lower BLER can also be achieved by the system. In other words, these results tell that frequency hopping becomes helpful as a jamming mitigation

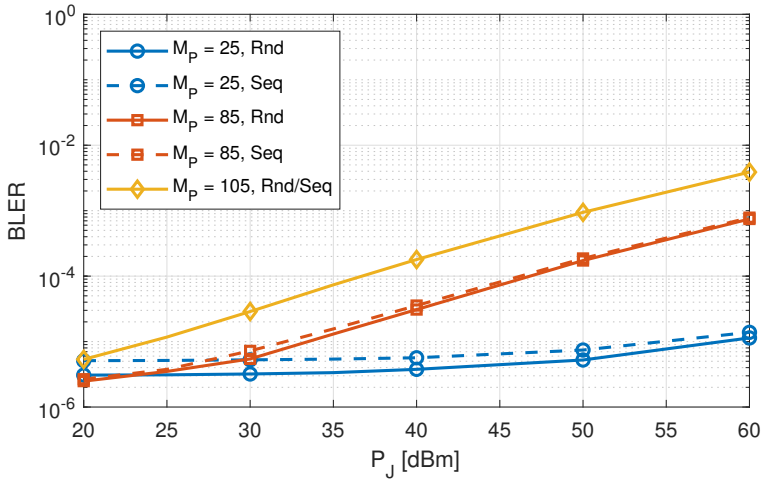


FIGURE 6.9: BLER versus P_{J} for $N_{\text{AP}} = 1$, $B = 100\,\text{MHz}$, and $L_P = 25$.

scheme mainly when reliability requirements with URLLC are stricter, otherwise the increase in SINR is not sufficient to even compensate for the reduced bandwidth.

6.5 Conclusions

In this Chapter we considered the problem of jamming attacks in 5G-and-beyond indoor factory deployments. We a) provided extensive simulations in a realistic scenario of a factory hall with 3GPP spatial channel model and a jammer stationed outside the plant, b) proposed and compared two detectors based on pseudo random blanking of subcarriers, and c) evaluated random scheduling and frequency hopping as jamming mitigation strategies. Numerical results show that a high-power jammer can strongly degrade BLER with URLLC. As promising countermeasures, a distributed deployment is more jamming resilient than a centralized one, and the RLRT detector is capable to provide good jamming detection performance by exploiting channel correlations among the deployed antennas. Finally, frequency hopping is beneficial in mitigating jamming attacks only with narrow-band jammers and with more strict reliability requirements.

Chapter 7

Conclusions

This Thesis investigated several aspects related to the security of GNSS signals and URLLC networks, ranging from techniques implemented in a security-oriented GNSS software package and detection of GNSS spoofing by a receiver in space to detection of jamming for 5G and beyond in Industry 4.0 scenarios. As GNSS systems and 5G networks are composed of different domains, the same should hold for the adopted security countermeasures: protection mechanisms can be implemented at the data level or the signal level. Designing multiple security mechanism on different domains is beneficial, but the purpose of each countermeasure shall be well defined, pursuing separation between domains. Therefore in designing a protection mechanism the purpose and target should be unambiguous: data level techniques (e.g., cryptographic techniques) should aim at protecting the authenticity of the message, while signal level techniques, which are the focus of this Thesis, should ensure the authenticity of the received signal, despite the distortion effects of the propagation environment.

In Chapter 3 we investigated an anti-spoofing and an anti-jamming technique, both implemented and tested in the software GNSS receiver developed. In particular, starting from the latter, we have seen that a notch filter being able to track the jamming frequency could be very useful in mitigating DoS attacks against GNSS receiver, without massively interfering with the authentic signal. On the other hand, in order to detect the subtle spoofing attacks, we considered the SQM techniques, which turned out to have poor performance against the proposed attacks and, in general, depending on the metric used and on the C/N_0 of the authentic signal. This is a small hint for justifying the investigation of numerous solutions, exploiting different tools and acting at different levels of the receiver architecture. However, as a first step for a improving the SQM techniques, a possibility could be to fuse the outputs of the different metrics, similarly to the approach used in Chapter 4 for the detection of spoofing by a receiver in space. In this case, the receiver is a satellite that is able to retrieve the value of three different metrics from two different sources: the GNSS signal and an orbit propagation model; by comparing the two values, we get a soft detection result. Finally, we fuse the soft outputs for all the consistency checks to get a unique spoofing flag, and the results show that the fusion can be beneficial.

Switching to the framework of mobile network communications, jamming attacks can severely degrade system performance, and therefore both detection and mitigation mechanisms are needed for becoming aware of the presence of a jammer and limiting its impact on the system. In Chapter 5 we considered the problem of jamming detection for 5G and beyond in Industry 4.0 scenarios and designed a method based on pseudo-random blanking of subcarriers in an OFDM system. We then considered a smart jammer following three types of strategies: remain as stealthy as possible, maximize the damage to MBB communication, and maximize the disruption of URLLC type of traffic. Results showed that, while for a MBB traffic the jammer has to compromise between MD and SE, with URLLC traffic, a smart jammer with sufficiently high power

can achieve good results in reaching both high values of MD probability and BLER. Then, as an extension to this work, in Chapter 6 we implemented a jammer for an indoor factory deployment with a more realistic 3GPP spatial channel model. On this scenario we tested the same jamming detector proposed above together with a detector exploiting also the channel correlation among antennas; the latter showed better performance in detecting the jammer. Given the industrial scenario, to estimate the jamming impact we focused on the performance of URLLC type of traffic, which turned out to be more jamming resilient using a decentralized deployment for APs. Potential future works related to this Chapter could include a) improvements in the defense strategy considering MIMO and the data REs, and b) performance evaluations in a 3GPP compliant Industry 4.0 scenario. Potential future works related to these two Chapters could include a) improvements in the defense strategy considering MIMO and the data REs, and b) more advanced mitigation schemes exploiting MIMO and multi-connectivity.

Far from being an extensive overview of all physical layer security aspects related to wireless communications, the effort of this Thesis has focused on tackling the challenge of securing GNSS and 5G networks from multiple points of view and with diverse tools. With the rapid growth of the market for both positioning and mobile services, the pool of feasible solutions worth exploring is envisioned to grow as well. Hopefully this work will be the first step to a broader investigation, which will ultimately result in comprehensive security solutions, integrating various security measures and increasing the resilience of the current communication systems.

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

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

where T_{s} is the sampling time interval and f_{IF} is the 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 $\tau, \phi, f_{\mathrm{D}}$ 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 AWGN [106]. 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 [106]

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

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 [106]

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

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

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

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

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

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

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

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

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

An Experiment about Compatibility between GNSS Software Simulator and SDR

C.1 Capabilities of current SDR front-ends in generating random walk frequency hopping jamming

One of the features of the GNSS simulator developed by our research group is the capability to generate jamming signals that are able to disrupt the authentic GNSS signal. Different jamming mode are implemented, but the one which interests this document is the random walk frequency hopping jamming.

In this type of jamming that I implemented, every T_r (time step of the random walk) the jammer generates a new frequency as

$$f_n = f_{n-1} + w_n, \quad \text{with i.i.d } w_n \sim \mathcal{N}(0, \sigma_f), \tag{C.1}$$

where n denotes the time (in steps) and $f_0 = f_\mathrm{J}$ is the starting jamming frequency decided by the attacker. The jamming frequencies at the sampling times within the interval $[nT_\mathrm{r}, (n+1)T_\mathrm{r}]$ are linearly interpolated between f_n and f_{n+1}. Finally, σ_f is set as a fraction of the selected jamming bandwidth B_J, that we set as $\sigma_f = B_\mathrm{J}/6$.

The aim of this document is to report the capabilities of the SDR (Nuand BladeRF x40 Rev.2) in generating the jamming signal described above. In order to test the capabilities of the SDR, the frequency hopping jamming signal is generated with our software GNSS simulator, then it is modulated with the SDR and finally it is sent

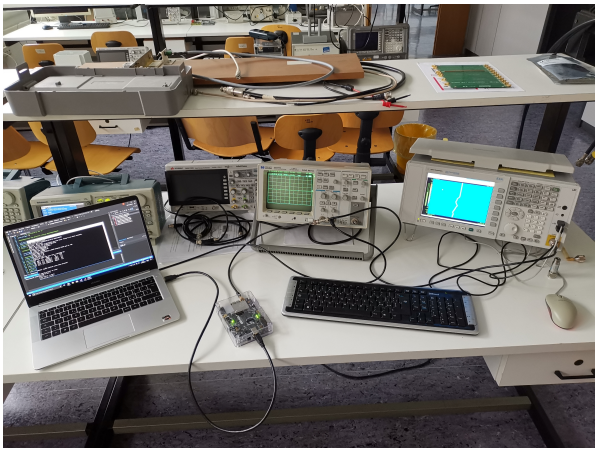
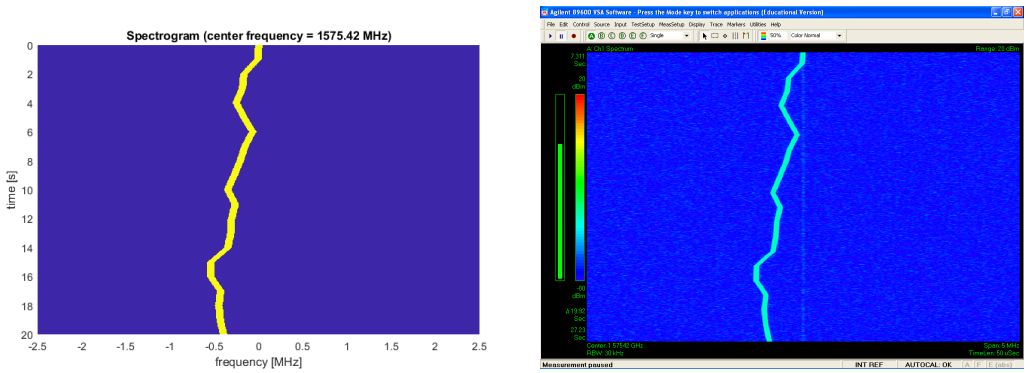


FIGURE C.1: Setup used for the tests.

to a spectrum analyzer (Agilent N9010A). The overall setup is shown in Fig. C.1, where also an oscilloscope is present between the SDR and the spectrum analyzer. The oscilloscope serves to see the time behavior of the signal and to be sure that the signal generated by the SDR is weak enough not to damage the spectrum analyzer.

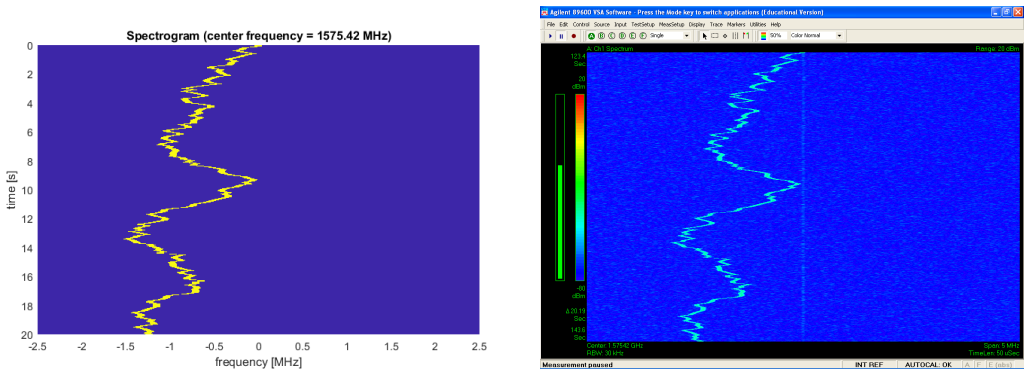
The test of the SDR is done by comparing the spectrogram outputted by the spectrum analyzer and a pseudo-spectrogram created using the theoretical jamming frequencies values generated by the simulator. In particular, several tests has been performed using different values of T_r (1 s, 0.1 s, 0.01 s and 0.001 s) and $B_\mathrm{J} = 0.5$ MHz. The results are reported in Figs. C.2 to C.5. All the figures show the spectrograms of the jamming signal in a scenario with duration 20 seconds and $f_\mathrm{J} = 1575.42$ MHz (center frequency of the L1 band). Moreover, the frequency span of the spectrogram is 5 MHz with center frequency 1575.42 MHz. The GNSS signal is voluntarily not simulated in order to make as visible as possible the jamming signal.

From the results we can see that the SDR is capable of reproducing accurately the frequencies imposed by the simulator up to a time step as low as $T_\mathrm{r} = 0.01$ s. Instead, for $T_\mathrm{r} = 0.001$ s, the hopping frequencies are different between the two spectrograms, although the general evolution is similar. Therefore, the SDR is capable to follow the simulated frequencies starting from values of T_r between 0.01 s and 0.001 s.



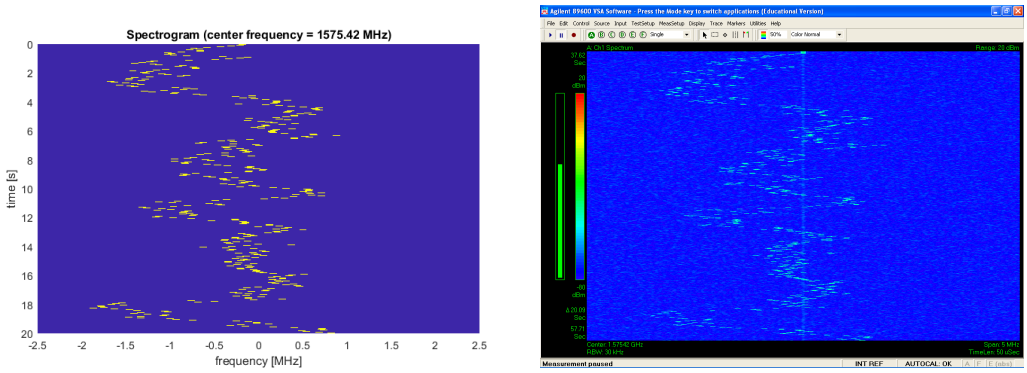
(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.2: Spectrograms of the jamming signal with $T_\mathrm{r} = 1$ s.



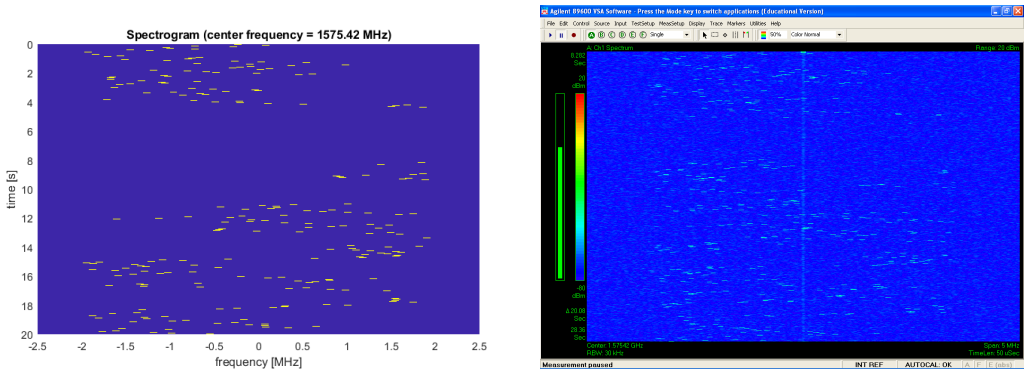
(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.3: Spectrograms of the jamming signal with $T_\mathrm{r} = 0.1$ s.



(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.4: Spectrograms of the jamming signal with $T_r = 0.01$ s.



(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.5: Spectrograms of the jamming signal with $T_r = 0.001$ s.

C.2 Capabilities of current SDR front-ends in generating deterministic step frequency hopping jamming

In order to further test the capabilities of the SDR, another type of jamming signal has been introduced in the software GNSS simulator, that is called frequency hopping jamming with deterministic step.

In this type of jamming, every T_s (time step) the jammer generates a new frequency as

$$f_n = \begin{cases} f_{n-2} + f_s & \text{if } (f_{n-2} - f_{n-4} = f_s) \vee \left(f_{n-2} < -\frac{B_J}{2} + f_s\right), \\ f_{n-2} - f_s & \text{if } (f_{n-2} - f_{n-4} = -f_s) \vee \left(f_{n-2} > \frac{B_J}{2} - f_s\right), \\ 0 & \text{otherwise.} \end{cases} \tag{C.2}$$

where n denotes the time (in steps), B_J is the jamming bandwidth, f_s is the frequency step, $f_0 = f_J$ is the starting jamming frequency decided by the attacker and $f_{-2} = f_J - f_s$. The jamming frequencies at the sampling times within the interval $[nT_s, (n+1)T_s]$ are kept constant at f_n.

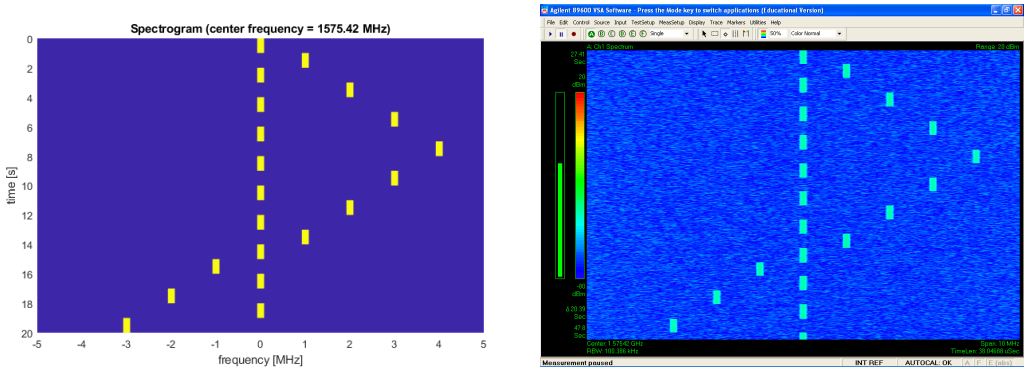
The test of the SDR is done with the same setup as the previous type of jamming. In particular, several tests has been performed using different values of T_s (1 s, 0.5 s, 0.1 s, 0.05 s and 0.01 s), $f_s = 1$ MHz and $B_J = 8$ MHz. The results are reported in Figs. C.6 to C.10. All the figures show the spectrograms of the jamming signal in a scenario with duration 20 seconds and $f_J = 1575.42$ MHz (center frequency of the L1 band). Moreover, the frequency span of the spectrogram is 10 MHz with center

frequency 1575.42 MHz. The GNSS signal is voluntarily not simulated in order to make as visible as possible the jamming signal.

Despite the presence of evident noise floor, from Figure C.6 we can see that the SDR is capable of reproducing accurately the frequencies imposed by the simulator and the transitions between one frequency and another for all the frequency's hops, up to jumps of 4 MHz.

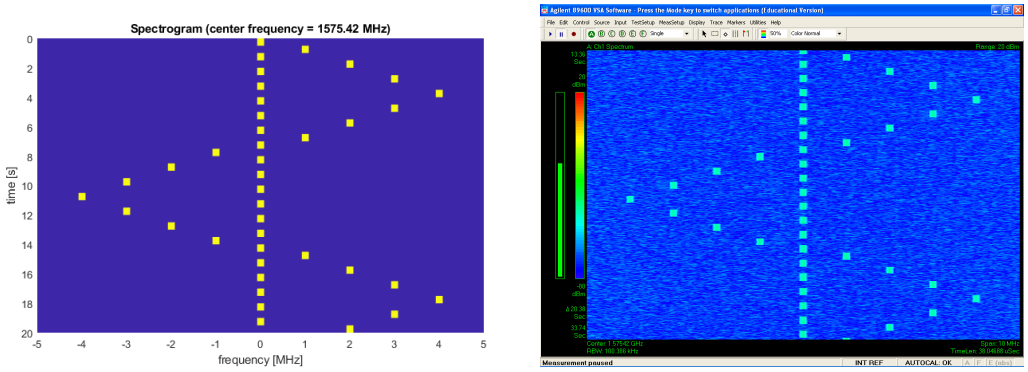
However, by comparing the performance of the SDR for different values of time step, it can be noted that it is capable of reproducing jamming signals for $T_s \geq 0.1\,s$, while for lower values there are some completely missing frequency steps. Moreover, since the time resolution of the spectrogram is $\sim 38\,\mu s$, it can be said that these missing frequencies are SDR's fault.

Therefore, after these additional tests, the SDR capability results deriving from the random hopping jamming test have to be updated. In particular, the SDR is capable to follow the simulated frequency jumps for time steps T_s greater than a value included between 0.1 s and 0.05 s.



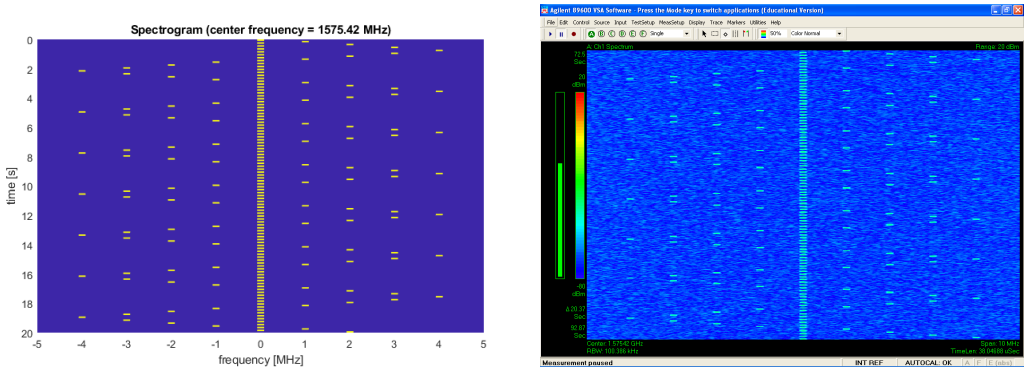
(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.6: Spectrograms of the jamming signal with $T_s = 1$ s.



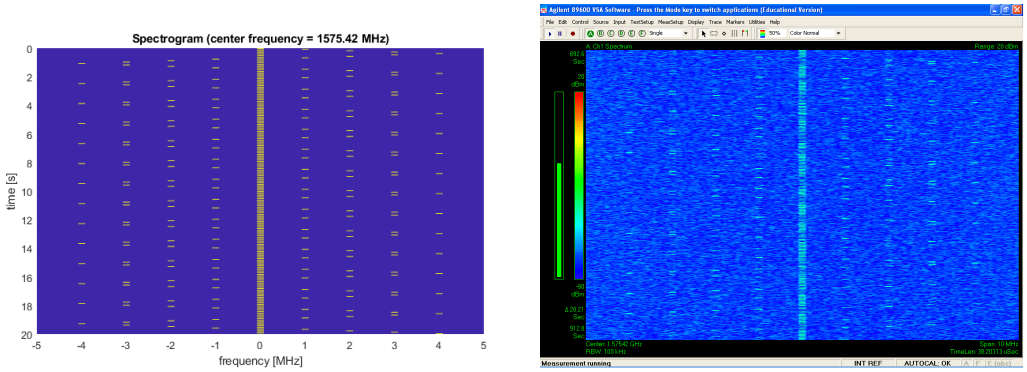
(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.7: Spectrograms of the jamming signal with $T_s = 0.5$ s.



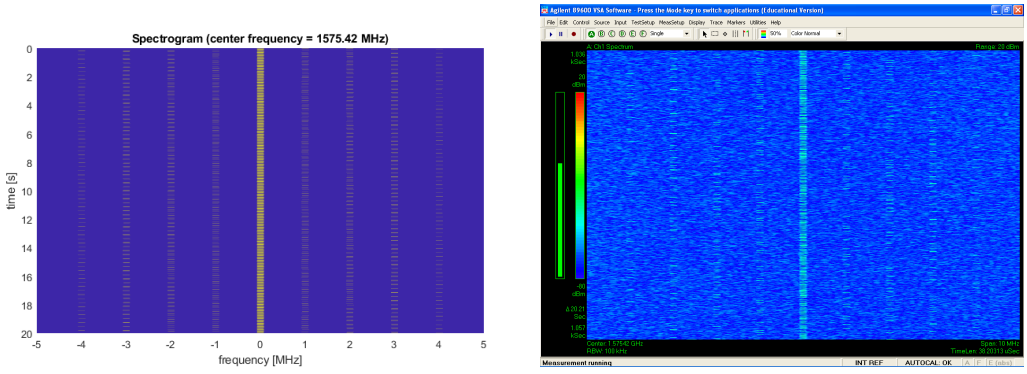
(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.8: Spectrograms of the jamming signal with $T_s = 0.1$ s.



(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.9: Spectrograms of the jamming signal with $T_s = 0.05$ s.



(A) Theoretical. (B) From spectrum analyzer.

FIGURE C.10: Spectrograms of the jamming signal with $T_s = 0.01$ s.

Appendix D

C/N_0 Estimators

The content of this appendix is based on the overview of C/N_0 estimators done in [107]. I introduce $r_{\mathrm{C}}[n] = \sqrt{P_{\mathrm{d}}}D[n] + \sqrt{P_{\mathrm{n}}}\eta[n], n = 1, \ldots, N$ as the signal samples at the correlator output, where P_{d} is the power associated to the data and P_{n} is the noise power. The SNR related to $r_{\mathrm{C}}[n]$ is then defined as

$$\lambda_{\mathrm{C}} = P_{\mathrm{d}}/P_{\mathrm{n}} \tag{D.1}$$

and the corresponding C/N_0 as

$$C/N_0\,(\mathrm{dB}) = 10\log_{10}\left(\lambda_{\mathrm{C}} \cdot B_{\mathrm{eqn}}\right) \tag{D.2}$$

where $B_{\mathrm{eqn}} = 1/T_{\mathrm{int}}$ represents the normalized equivalent noise bandwidth of the system, with T_{int} the coherence integration time of the tracking loop. The following four C/N_0 estimators are considered, where $\widehat{\cdot}$ denotes the estimated value.

Squared signal-to-noise variance (SNV) It is based on the first absolute moment and the second moment of the signal samples, developed for BPSK modulations. Its equations can be written as

$$\widehat{P}_{\mathrm{d}} = \left[\frac{1}{N}\sum_{v=1}^{N}\left|\mathrm{Re}\{r_{\mathrm{C}}[v]\}\right|\right]^2 , \tag{D.3}$$

$$\widehat{P}_{\mathrm{tot}} = \frac{1}{N}\sum_{v=1}^{N}\left|r_{\mathrm{C}}[v]\right|^2 , \tag{D.4}$$

$$\widehat{P}_{\mathrm{n}} = \widehat{P}_{\mathrm{tot}} - \widehat{P}_{\mathrm{d}} , \tag{D.5}$$

$$\widehat{\lambda}_{\mathrm{C}} = \frac{\widehat{P}_{\mathrm{d}}}{\widehat{P}_{\mathrm{n}}} = \frac{\widehat{P}_{\mathrm{d}}}{\widehat{P}_{\mathrm{tot}} - \widehat{P}_{\mathrm{d}}} , \tag{D.6}$$

where $\widehat{P}_{\mathrm{tot}}$ is the estimated total power of the signal $r_{\mathrm{C}}[n]$.

Moments method (MM) It employs the second- and fourth-order moments for the separate estimation of carrier strength and noise strength. Using the theoretical formulation of the second- and fourth-order moments of the received constellation in noise ($M_2 \triangleq \mathbb{E}\left[\left|r_{\mathrm{C}}[n]\right|^2\right]$ and $M_4 \triangleq \mathbb{E}\left[\left|r_{\mathrm{C}}[n]\right|^4\right]$), respectively), we have

$$P_{\mathrm{d}}(M_2, M_4) = \sqrt{2M_2^2 - M_4} , \tag{D.7}$$

$$P_{\mathrm{n}}(M_2, M_4) = M_2 - P_{\mathrm{d}} . \tag{D.8}$$

The statistical moments M_2 and M_4 can be estimated by their respective time averages

$$\widehat{M_2} = \frac{1}{N}\sum_{v=1}^{N} |r_{\mathrm{C}}[v]|^2 \,, \tag{D.9}$$

$$\widehat{M_4} = \frac{1}{N}\sum_{v=1}^{N} |r_{\mathrm{C}}[v]|^4 \,, \tag{D.10}$$

so that

$$\widehat{\lambda}_{\mathrm{C}} = \frac{P_{\mathrm{d}}(\widehat{M_2}, \widehat{M_4})}{P_{\mathrm{n}}(\widehat{M_2}, \widehat{M_4})} \,. \tag{D.11}$$

Real signal-complex noise (RSCN) A simple method that exploits the fact that the navigation data are transmitted on the in-phase channel, but also a quadrature channel is available after the carrier wipe-off, where just noise should be theoretically observed. Its equations can be written as

$$\widehat{P}_{\mathrm{n}} = \frac{2}{N}\sum_{v=1}^{N} |\mathrm{Im}\{r_{\mathrm{C}}[v]\}|^2 \,, \tag{D.12}$$

$$\widehat{P}_{\mathrm{tot}} = \frac{1}{N}\sum_{v=1}^{N} |r_{\mathrm{C}}[v]|^2 \,, \tag{D.13}$$

$$\widehat{P}_{\mathrm{d}} = \widehat{P}_{\mathrm{tot}} - \widehat{P}_{\mathrm{n}} \,, \tag{D.14}$$

$$\widehat{\lambda}_{\mathrm{C}} = \frac{\widehat{P}_{\mathrm{d}}}{\widehat{P}_{\mathrm{n}}} = \frac{\widehat{P}_{\mathrm{tot}} - \widehat{P}_{\mathrm{n}}}{\widehat{P}_{\mathrm{n}}} \,. \tag{D.15}$$

Narrowband-wideband power ratio (NWPR) method Such a method involves the evaluation of the total power of the process $r_{\mathrm{C}}[n]$ over two different noise bandwidths: a wideband power measurement taken over the noise bandwidth $1/T_{\mathrm{int}}$

$$\mathrm{WBP}_k \triangleq \sum_{m=1}^{M} |r_{\mathrm{C}}[kM+m]|^2 \,, \qquad k = 0, 1, \ldots, \left(\frac{N}{M} - 1\right) \,, \tag{D.16}$$

and a narrowband power measurement taken over the noise bandwidth $1/(MT_{\mathrm{int}})$

$$\begin{aligned} \mathrm{NBP}_k \triangleq & \left(\sum_{m=1}^{M} \mathrm{Re}\{r_{\mathrm{C}}[kM+m]\}\right)^2 \\ & + \left(\sum_{m=1}^{M} \mathrm{Im}\{r_{\mathrm{C}}[kM+m]\}\right)^2 \,, \qquad k = 0, 1, \ldots, \left(\frac{N}{M} - 1\right) \,, \end{aligned} \tag{D.17}$$

where $M = T_{\mathrm{bit}}/T_{\mathrm{int}}$ and T_{bit} is the navigation bit duration. The ratio between the narrowband to wideband power at discrete time k gives an estimate of the noise power

$$\mathrm{NP}_k = \frac{\mathrm{NBP}_k}{\mathrm{WBP}_k} \,. \tag{D.18}$$

An expression for the C/N_0 is given by

$$\widehat{C/N_0}(\mathrm{dB}) = 10\log_{10}\left(\frac{1}{T_{\mathrm{int}}}\frac{\widehat{\mu}_{\mathrm{NP}} - 1}{M - \widehat{\mu}_{\mathrm{NP}}}\right) \,, \tag{D.19}$$

where

$$\widehat{\mu}_{\mathrm{NP}} = \frac{M}{N} \sum_{k=0}^{N/M-1} \mathrm{NP}_k \,. \tag{D.20}$$

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. P. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attacks," in *Proc. 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, USA, Sep. 2011, pp. 2608–2618.

[3] F. Dovis, *GNSS Interference Threats and Countermeasures*. Norwood, MA, USA: 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, pp. 14–19, Jan./Feb. 2009.

[5] M. Wildemeersch, E. C. Pons, A. Rabbachin, and J. F. Guasch, "Impact study of unintentional interference on GNSS receivers," European Commission, Joint Research Centre, JRC Scientific and Technical Reports, Tech. Rep., 2010.

[6] M. Pini, B. Motella, L. Pilos, *et al.*, "Robust on-board ship equipment: The TRITON project," in *Proc. 10th International Symposium Information on Ships (ISIS)*, Hamburg, Germany, Sep. 2014.

[7] UT News. "UT Austin researchers successfully spoof an $80 million yacht at sea." (2013), [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] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[9] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[10] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, 2016.

[11] M. T. Gamba and E. Falletti, "Performance analysis of FLL schemes to track swept jammers in an adaptive notch filter," in *Proc. 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2018.

[12] L. Chiarello, A. V. Guglielmi, N. Laurenti, F. Bernardi, F. Longhi, and S. Fantinato, "Detection of GNSS spoofing by a receiver in space via fusion of consistency metrics," in *Proc. IEEE International Conference on Communications (ICC)*, Virtual Conference, Jun. 2020.

[13] L. Chiarello, P. Baracca, K. Upadhya, S. R. Khosravirad, and T. Wild, "Jamming detection with subcarrier blanking for 5G and beyond in Industry 4.0 scenarios," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Virtual Conference, Sep. 2021.

[14] L. Chiarello, P. Baracca, K. Upadhya, S. R. Khosravirad, S. Mandelli, and T. Wild, "Jamming resilient indoor factory deployments: Design and performance evaluation," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Austin, TX, USA, Apr. 2022, forthcoming.

[15] J. S. Subirana, J. J. Zornoza, and M. Hernàndez-Pajares. "GNSS data processing. volume 1: Fundamentals and algorithms." (2013), [Online]. Available: `https://gage.upc.edu/sites/default/files/TEACHING_MATERIAL/GNSS_Book/ESA_GNSS-Book_TM-23_Vol_Ip.pdf` (visited on 01/10/2022).

[16] P. Teunissen and O. Montenbruck, *Springer handbook of global navigation satellite systems*. New York, NY, USA: Springer, 2017.

[17] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS–Global navigation satellite systems: GPS, GLONASS, Galileo, and more*. New York, NY, USA: 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*. New York, NY, USA: McGraw-Hill Professional, 2008.

[19] R. Landry Jr and A. Renard, "Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers," in *Proc. 4th St.Petersburg International Conference on Integrated Navigation Systems (ICINS)*, St-Petersburg, Russia, May 1997.

[20] B. Motella, A. T. Balaeib, L. L. Prestic, M. Leonardid, and A. Dempsterb, "Characterization of radar interference sources in the Galileo E6 band," *J Aerosp Sci Technol Syst, Aerotecnica Missili Spazio*, vol. 1, no. 88, pp. 42–53, 2016.

[21] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers – Analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation)," in *Proc. 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, USA, Sep. 2011, pp. 430–435.

[22] R. Mitch, R. Dougherty, M. Psiaki, *et al.*, "Know your enemy: Signal characteristics of civil GPS jammers," *GPS world*, vol. 23, no. 1, pp. 64–71, 2012.

[23] Exelis Inc. "The threat of GPS jamming." (2015), [Online]. Available: `https://rntfnd.org/wp-content/uploads/Exelis-GPS-Vulnerability-Assessment-February2014.pdf` (visited on 12/25/2021).

[24] E. D. Kaplan and C. Hegarty, *Understanding GPS/GNSS: principles and applications*. Artech house, 2017.

[25] Nu-Trek Inc. "Anti-jam RF front ends and anti-jam solutions." (2015), [Online]. Available: `http://www.nu-trek.com/` (visited on 12/25/2021).

[26] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[27] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS receivers from jamming and interference," *Proc. IEEE*, vol. 104, no. 6, pp. 1327–1338, Jun. 2016.

[28] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proc. the IEEE*, vol. 104, no. 6, pp. 1207–1220, Jun. 2016.

[29] M. G. Amin, X. Wang, Y. D. Zhang, F. Ahmad, and E. Aboutanios, "Sparse arrays and sampling for interference mitigation and DOA estimation in GNSS," *Proc. IEEE*, vol. 104, no. 6, pp. 1302–1317, Jun. 2016.

[30] A. G. Dempster and E. Cetin, "Interference localization for satellite navigation systems," *Proc. IEEE*, vol. 104, no. 6, pp. 1318–1326, Jun. 2016.

[31] J. A. Volpe, "Vulnerability assessment of the transportation infrastructure relying on the global positioning system," U.S. Dept. Transportation, Tech. Rep., 2001.

[32] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, Portland, OR, USA, Sep. 2001, pp. 1542–1552.

[33] 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 *Proc. 21st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, 2008, pp. 2314–2325.

[34] C. Günther, "A survey of spoofing and counter-measures," *NAVIGATION, J. Inst. Navig*, vol. 61, no. 3, pp. 159–177, 2014.

[35] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Apr. 2016.

[36] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.

[37] 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, no. 127072, Jul. 2012.

[38] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th international technical meeting of the satellite division of the institute of navigation (ION GNSS)*, Long Beach, CA, USA, 2005, pp. 1285–1290.

[39] 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 *Proc. 24th International Technical Meeting of the Satellite Division of The institute of navigation (ION GNSS)*, Portland, OR, USA, Sep. 2011, pp. 2646–2656.

[40] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proc. Institute of Navigation - International Technical Meeting (ITM)*, San Diego, CA, USA, Jan. 2010, pp. 698–712.

[41] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symposium on Research in Security and Privacy*, May 2000, pp. 56–73.

[42] G. Caparra, S. Sturaro, N. Laurenti, C. Wullems, and R. T. Ioannides, "A novel navigation message authentication scheme for GNSS open service," in *Proc. 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Portland, OR, USA, Sep. 2016, pp. 2938–2947.

[43] J. T. Curran and C. O'Driscoll, "Message authentication, channel coding & anti-spoofing," in *Proc. 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Portland, OR, USA, Sep. 2016, pp. 2948–2959.

[44] J. T. Curran, M. Paonni, and J. Bishop, "Securing the open-service: A candidate navigation message authentication scheme for Galileo E1 OS," in *Proc. European Navigation Conference (ENC)*, Rotterdam, The Netherlands, Apr. 2014.

[45] I. Fernández-Hernández, "GNSS authentication: Design parameters and service concepts," in *Proc. European Navigation Conference (ENC)*, Rotterdam, The Netherlands, Apr. 2014.

[46] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service," in *Proc. 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Tampa, FL, USA, Sep. 2014, pp. 2810–2827.

[47] P. Walker, C. Rijmen, I. Fernandez-Hernandez, *et al.*, "Galileo open service authentication: A complete service design and provision analysis," in *Proc. 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Tampa, FL, USA, Sep. 2015, pp. 3383–3396.

[48] J. T. Curran and M. Paonni, "Securing GNSS: An end-to-end feasibility analysis for the Galileo open-service," in *Proc. 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Tampa, FL, USA, Sep. 2014, pp. 2828–2842.

[49] M. Canale, S. Fantinato, and O. Pozzobon, "Performance comparison of different data authentication solutions for the Galileo CS," in *Proc. 7th ESA Workshop Satellite Navig. Technol. Eur. Workshop on GNSS Signals Signal Processing (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2014.

[50] I. Fernández-Hernández, J. Simón, R. Blasi, C. Payne, T. Miquel, and J. Boyero, "The Galileo commercial service: Current status and prospects," in *Proc. European Navigation Conference (ENC)*, Rotterdam, The Netherlands, Apr. 2014.

[51] I. Rodríguez, G. Tobías, D. Calle, *et al.*, "Preparing for the Galileo commercial service – Proof of concept and demonstrator development," pp. 3399–3410, Sep. 2014.

[52] 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.

[53] G. Caparra, N. Laurenti, R. Ioannides, and M. Crisci, "Improving secure code estimation and replay attack and detection on GNSS signals," in *Proc. 7th ESA Workshop Satellite Navig. Technol. Eur. Workshop on GNSS Signals Signal Processing (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2014.

[54] L. Scott, "Proving location using GPS location signatures: Why it is needed and a way to do it," in *Proc. 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Nashville, TN, USA, Sep. 2013, pp. 2880–2892.

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

[56] O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *Proc. 5th ESA Workshop Satellite Navig. Technol. Eur. Workshop on GNSS Signals Signal Processing (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2010.

[57] O. Pozzobon, G. Gamba, M. Canale, and S. Fantinato, "Supersonic GNSS authentication codes," in *Proc. 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Tampa, FL, USA, Sep. 2014, pp. 2862–2869.

[58] O. Pozzobon, G. Gamba, M. Canale, and S. Fantinato, "From data schemes to supersonic codes. GNSS authentication for modernized signals," *Inside GNSS*, vol. 10, no. 1, pp. 55–64, Jan./Feb. 2015.

[59] A. Garcia-Pena, D. Salos, O. Julien, L. Ries, and T. Grelier, "Analysis of the use of CSK for future GNSS signals," in *Proc. 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Nashville, TN, USA, Sep. 2013, pp. 1461–1479.

[60] A. J. G. Peña, M. Aubault-Roudier, L. Ries, M.-L. Boucheret, C. Poulliat, and O. Julien, "Code shift keying: Prospects for improving GNSS signal designs," *Inside GNSS*, vol. 10, no. 6, pp. 52–62, Nov./Dec. 2015.

[61] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Exploiting side-information for resilient gnss positioning in mobile phones," in *Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 1515–1524.

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

[63] L. Chiarello, "Security evaluation of GNSS signal quality monitoring techniques against optimal spoofing attacks," M.S. thesis, University of Padua, Pauva, Italy, 2018.

[64] D. Borio, "Loop analysis of adaptive notch filters," *IET Signal Processing*, vol. 10, no. 6, pp. 659–669, 2016.

[65] S. Stephens and J. Thomas, "Controlled-root formulation for digital phase-locked loops," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 31, no. 1, pp. 78–95, 1995.

[66] D. Livingstone and P. Lewis, *Space, the Final Frontier for Cybersecurity?* Chatham House, London: The Royal Institute of International Affairs, Sep. 2016.

[67] L. Xiao, P.-C. Ma, X.-M. Tang, and G.-F. Sun, "GNSS receiver anti-spoofing techniques: A review and future prospects," in *Proc. 5th International Conference on Electronics, Communications and Networks (CECNet)*, vol. 382, Singapore, 2016, pp. 59–68.

[68] S. Fantinato, G. Da Broi, F. Bernardi, *et al.*, "Emerging applications of snapshot navigation in space," in *Proc. 9th ESA Workshop Satellite Navig. Technol. Eur. Workshop on GNSS Signals Signal Processing (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2018.

[69] T. S. Kelso. "More frequently asked questions." (2018), [Online]. Available: `https://celestrak.com/columns/v04n05` (visited on 09/05/2018).

[70] T. S. Kelso. "Master tle index." (2018), [Online]. Available: `https://celestrak.com/NORAD/elements/master.php` (visited on 09/05/2018).

[71] D. A. Vallado, P. Crawford, R. Hujsak, and T. Kelso, "Revisiting spacetrack report# 3: Rev 2," in *Proc. AIAA/AAS Astrodynamics Specialist Conference and Exhibit*, Keystone, CO, USA, Aug. 2006.

[72] M. Lane, "The development of an artificial satellite theory using a power-law atmospheric density representation," in *2nd Aerospace Sciences Meeting*, 1965, p. 35.

[73] F. R. Hoots, "Spacetrack report no. 3, models for propagation of norad element sets," *http://www. itc. nl/-bakker/orbit. html*, 1980.

[74] D.
Proc. 63rd International Astronautical Congress, Naples, Italy, 2012.

[75] S. M. Kay, *Fundamentals of statistical signal processing: detection theory*. Prentice Hall, 1993.

[76] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[77] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (agc)," *NAVIGATION, J. Inst. Navig*, vol. 59, no. 4, pp. 281–290, 2012.

[78] E. Falletti, M. Pini, and L. Lo Presti, "Low complexity carrier-to-noise ratio estimators for GNSS digital receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 1, pp. 420–437, 2011.

[79] D. R. Pauluzzi and N. C. Beaulieu, "A comparison of snr estimation techniques for the AWGN channel," *IEEE Transactions on Communications*, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.

[80] N. C. Beaulieu, A. S. Toms, and D. R. Pauluzzi, "Comparison of four SNR estimators for QPSK modulations," *IEEE Communications Letters*, vol. 4, no. 2, pp. 43–45, Feb. 2000.

[81] J. J. Spilker Jr, P. Axelrad, B. W. Parkinson, and P. Enge, *Global Positioning System: Theory and Applications, Vol. 1*. American Institute of Aeronautics and Astronautics, 1996, pp. 329–407.

[82] H. Tao, H. Li, and M. Lu, "A method of detections' fusion for GNSS anti-spoofing," *Sensors*, vol. 16, no. 12, p. 2187, 2016.

[83] S. Aida and M. Kirschner, "Accuracy assessment of SGP4 orbit information conversion into osculating elements," in *Proc. 6th European Conference on Space Debris*, Darmstadt, Germany, 2013, pp. 22–25.

[84] E. Dahlman, S. Parkvall, and J. Skold, *5G NR: the next generation wireless access technology*. Academic Press, 2018.

[85] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57 063–57 074, 2020.

[86] G. Berardinelli *et al.*, "Extreme communication in 6G: Vision and challenges for 'in-X' subnetworks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2516–2535, 2021.

[87] M. Alonzo *et al.*, "Cell-free and user-centric massive MIMO architectures for reliable communications in indoor factory environments," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1390–1404, 2021.

[88] "Jammer-store." (2021), [Online]. Available: `http://www.jammer-store.com`.

[89] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[90] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" In *Proc. ACM Conference on Wireless Network Security (WiSec)*, Hamburg, Germany, Jun. 2011.

[91] A. Chorti *et al.*, *Context-aware security for 6G wireless: The role of physical layer security*, https://arxiv.org/abs/2101.01536, Jan. 2021.

[92] C. Orakcal and D. Starobinski, "Rate adaptation in unlicensed bands under smart jamming attacks," in *Proc. ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Stockholm, Sweden, Jun. 2012.

[93] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.

[94] V. N. Swamy *et al.*, "Monitoring under-modeled rare events for URLLC," in *Proc. IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Cannes, France, Jul. 2019.

[95] P. Zhang and S. Sun, "One node to guard all: Jamming-resistant and low-latency communication for IoT," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, UAE, Dec. 2018.

[96] K. Brueninghaus *et al.*, "Link performance models for system level simulations of broadband radio access systems," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Berlin, Germany, Sep. 2005.

[97] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[98] Bundesnetzagentur, *Verwaltungsvorschrift für Frequenzzuteilungen für lokale Frequenznutzungen im Frequenzbereich 3.700-3.800 MHz (VV Lokales Breitband)*, Nov. 2019.

[99] T. V. K. Chaitanya and E. G. Larsson, "Optimal power allocation for hybrid ARQ with chase combining in i.i.d. rayleigh fading channels," *IEEE Transactions on Communications*, vol. 61, no. 5, pp. 1835–1846, May 2013.

[100] G. T. Amariucai and S. Wei, "Jamming games in fast-fading wireless channels," in *Proc. IEEE Global Telecommunications Conference (GLOBCOM)*, New Orleans, LA, USA), Nov. 2008.

[101] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[102] F. Girke, F. Kurtz, N. Dorsch, and C. Wietfeld, "Towards resilient 5G: Lessons learned from experimental evaluations of LTE uplink jamming," in *Proc. 2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China, May 2018, pp. 1–6.

[103] R1-1813177, "Scenarios, frequencies and new field measurement results from two operational factory halls at 3.5 GHz for various antenna configurations," Nokia, Tech. Rep., Nov. 2018.

[104] 3rd Generation Partnership Project (3GPP), "Study on channel model for frequencies from 0.5 to 100 GHz," Tech. Rep., TR 38.901, Jun. 2018.

[105] B. Nadler, F. Penna, and R. Garello, "Performance of eigenvalue-based signal detectors with known and unknown noise level," in *Proc. IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jun. 2011.

[106] J. Leclère, R. J. Landry, and C. Botteron, "How does one compute the noise power to simulate real and complex GNSS signals?" *Inside GNSS*, pp. 29–33, Jul./Aug. 2016.

[107] E. Falletti, M. Pini, and L. Lo Presti, "Carrier-to-noise algorithms," *Inside GNSS*, pp. 20–27, Jan./Feb. 2010.