Faculty of Information Technology and
Communication Sciences

Department of Telecommunications
and Systems Engineering

Double Doctoral Degree Programme

Interference Management and System Optimization with GNSS and non-GNSS Signals for Enhanced Navigation

AUTHOR Rubén Morales Ferré

SUPERVISORS Prof. Elena Simona Lohan
Prof. Gonzalo Seco Granados

November 2022

RUBÉN MORALES FERRÉ

Interference Management and System Optimization with GNSS and non-GNSS Signals for Enhanced Navigation

UAB Universitat Autònoma de Barcelona

PhD programme in Electronic and Telecommunication Engineering

Tampere University

Doctoral Programme of Computing and Electrical Engineering

ACADEMIC DISSERTATION
To be presented, with the permission of
the Faculty of Information Technology and Communication Sciences
of Tampere University, and of the Department of Telecommunications and Systems
Engineering of Universitat Autònoma de Barcelona
for public discussion in the TB109
of the Tietotalo, Korkeakoulunkatu 1, 33720, Tampere,
on 15 November 2022 at 9 o'clock.

ACADEMIC DISSERTATION
Tampere University, Faculty of Information Technology and Communication Sciences
Finland
Universitat Autònoma de Barcelona, Department of Telecommunications and Systems Engineering
Spain

Responsible supervisor and Custos	Professor Elena Simona Lohan Tampere University Finland	
Supervisors	Professor Elena Simona Lohan Tampere University Finland	Professor Gonzalo Seco Granados Universitat Autónoma de Barcelona Spain
Pre-examiners	Professor Gaetano Giunta University of Rome Tre Italy	Professor Christophe Macabiau Ecole Nationale de l’Aviation Civile France
Opponents	Professor Christophe Macabiau Ecole Nationale de l’Aviation Civile France	Dr. Beatrice Motella Links Foundation Italy
	Professor Paul Groves University College London United Kingdom	

ISBN 978-952-03-2581-7 (print)
ISBN 978-952-03-2582-4 (pdf)
http://urn.fi/URN:ISBN:978-952-03-2582-4

PunaMusta Oy – Yliopistopaino
Joensuu 2022

Preface

The work presented in this thesis was carried out during the years 2018-2022 in both the Department of Electrical Engineering at Tampere University (TAU) and in the Department of Telecommunications and Systems Engineering at the Universitat Autonoma de Barcelona (UAB). In the signal processing for wireless positioning (TLTPOS) group and the signal processing for communications and navigation (SPCOMNAV) group, respectively. The work presented in this thesis is done under the cooperation agreement for a double Ph.D. degree between TAU and UAB. Several individuals and organizations have made this thesis possible, and they deserve special mention and words of appreciation.

In the first place, I would like to express my sincere gratitude to my thesis supervisors Prof. Elena Simona Lohan and Prof. Gonzalo Seco Granados for giving me this invaluable opportunity, and for their constant support, encouragement, and instruction. I feel grateful for allowing me to learn from two of the most outstanding and knowledgeable researchers I have had the opportunity to meet. I would like to extend my gratitude to Dr. Philipp Richter for his support and guidance, especially at the beginning of this thesis. Furthermore, I also would like to thank MSc. Wenbo Wang and Dr. Yi Lu for their support and fruitful discussions. Lastly, I would like to thank MSc. Matias Turunen for his invaluable support while setting up the laboratory experiments.

Furthermore, I would like to thank my colleagues with whom I have spent countless good moments, especially I would like to thank Pablo, Sel, Vesa, Sahan, Islam, and Niloofar. I would also like to thank the SPCOMNAV research group, especially Prof. José A. López Salcedo, Daniel Egea, Sergi Locubiche, and the former members

Vicente Lucas, David Gómez, Alejandro Pérez, and José A. Del Peral for their support during my time in UAB.

Next, I would also like to highly appreciate the pre-examiners of this dissertation, Prof. Christophe Macabiau, and Prof. Gaetano Giunta, which have contributed to improving the quality of this manuscript with their invaluable feedback.

I would also like to thank Prof. Christophe Macabiau, Beatrice Motella, and Prof. Paul Groves for agreeing to act as opponents during the defense of this thesis.

I would also like to acknowledge the financial support received from Tampere University Doctoral School and for being awarded by the Rector's grant. In addition, I would also like to thank the Academy of Finland, the European Commission, the European Space Agency, and the TEK100/JAES foundations for their financial support through numerous projects.

I would like to extend my warmest gratitude to all my dear friends in Tampere (and Oulu) Jose, Carlos, Carmen, Alberto, Laura, Carlos C., Anastasia, Sergio, Emanuele, Irene, Pablo, Elena, Amir, Pavel, Maja, Angela, Lucie, and Roman for supporting me and share this wonderful journey in Finland close to me.

Lastly but not less important, I would like to express my most sincere gratitude to my parents Carmen and Manuel, and my sister Carla for their unconditional support and love. Finally, my last words go to Ziomara, for her constant and unlimited support and for being my compass.

Abstract

In the last few decades, Global Navigation Satellite System (GNSS) has become an indispensable element in our society. Currently, GNSS is used in a wide variety of sectors and situations, some of them offering critical services, such as transportation, telecommunications, and finances. For this reason, and combined with the relative ease an attack on the GNSS wireless signals can be performed nowadays with an Software Defined Radio (SDR) transmitter, GNSS has become more and more a target of wireless attacks of diverse nature and motivations. Nowadays, anyone can buy an interference device (also known as a jammer device) for a few euros. These devices are legal to be bought in many countries, especially online. But at the same time, they are illegal to be used. These devices can interfere with signals in specific frequency bands, used for services such as GNSS. An outage in the GNSS service at a specific location area (which can be even a few km^2) could end up in disastrous consequences, such as an economical loss or even putting lives at risk, since many critical services rely on GNSS for their correct functioning.

Fundamentally, this thesis focuses on developing new methods and algorithms for interference management in GNSS. The main focus is on interference detection and classification, but discussions are also made about interference localization and mitigation. The detection and classification algorithms analyzed in this thesis are chosen from the point of view of the aviation domain, in which additional constraints (e.g., antenna placement, number of antennas, vibrations due to movement, etc.) need to be taken into account. The selected detection and classification methods are applied at the pre-correlation level, based on the raw received signal. They apply specific signal transforms in the digital domain (e.g., time-frequency transfor-

mations) to the received signal. With such algorithms, interferences can be detected at a level as low as 0 dB Jamming-to-Signal Ratio (JSR). The interference classification combines transformed signals with previously trained signals Convolutional Neural Network (CNN) and/or Support Vector Machine (SVM) to determine the type of interference signal among the studied ones. The accuracy of such a classification methodology is above 90%. Knowing which signal causes interference we can better optimize which mitigation and localization algorithm we should use to obtain the best mitigation results.

Furthermore, this thesis also studies alternative positioning methods, starting from the premise that GNSS may not always be available and/or we are certain that we can not rely on it due to some reason such as high or unmitigated interferences. Therefore, if one needs to get a Position Velocity and Time (PVT) solution, one would have to rely on alternative signals that could offer positioning features, such as the cellular network signals (i.e. 4G, 5G, and further releases) and/or satellite positioning based on Low Earth Orbit (LEO) satellites. Those systems use presumably different frequency bands, which makes it more unlikely that they will be jammed at the same time as the GNSS signal. In this sense, positioning based on LEO satellites is studied in this thesis from the point of view of feasibility and expected performance.

Resum

En les últimes dècades, els sistemes globals de navegació per satèl·lit –comunament anomenats GNSS per les seves sigles en anglès- s'han convertit en un element indispensable en la nostra societat. En l'actualitat, GNSS és usat en una àmplia varietat de sectors i situacions, algunes d'elles oferint serveis crítics, com pot ser el transport, telecomunicacions, i finances. Per aquesta raó, i combinat amb la relativa facilitat que avui dia un atac es pot efectuar amb simplement un transmissor basat en ràdio definida per software -SDR per les seves sigles en anglès- GNSS s'ha convertit en un dels principals objectius quant a atacs de diversa naturalesa i motivació. Avui dia, pràcticament qualsevol persona pot comprar dispositius amb els quals generar interferències (coneguts com a dispositius jamming) per molt pocs euros. En l'actualitat, aquests dispositius es poden comprar legalment en molts països. Encara que el seu ús és normalment il·legal. Aquests dispositius poden interferir greument en certes bandes freqüencials, com en aquest cas les usades pels sistemes de navegació per satèl·lit. La falta de disponibilitat en el servei ofert pels sistemes de navegació (la falta de servei es pot estendre a diversos km^2)) podria acabar en conseqüències desastroses, com per exemple una pèrdua econòmica o posant en perill vides humanes. Alguns serveis crítics per a la humanitat basen el seu correcte funcionament en els sistemes de navegació per satèl·lit.

Fonamentalment, aquesta tesi s'enfoca en el desenvolupament d'algorismes i nous mètodes per a la gestió d'interferències en GNSS. L'enfocament principal és en la detecció i classificació d'interferències, encara que també es tracten temes sobre localització i mitigació d'interferències. Els algorismes de detecció i classificació analitzats en aquesta tesi van ser triats des del punt de vista del sector de l'aviació, en el qual

restriccions addicionals (per exemple, la posició i orientació de les antenes, numero total d'antenes, vibracions a causa del moviment, etc.) són necessàries de tenir-les en compte. Els algoritmes de detenció i classificació seleccionats en aquesta tesi són aplicats a nivell de pre-correlació, els quals es basen en el senyal rebut en cru (abans del seu processament en el domini digital). Aquests algorismes apliquen processament en el domini digital al senyal rebut (per exemple, transformacions en temps-freqüència). Amb els algorismes analitzats, interferències a tan baixa potència com 0 dB respecte al senyal desitjat poden ser detectades. Els algorismes de classificació d'interferències combinen els senyals rebuts amb xarxes neuronals convolucionals -CNN per les seves sigles en anglès- i màquines de vectors de suport -SVM per les seves sigles en anglès- per a determinar el tipus de senyal interferent d'entre totes les estudiades. La precisió dels algorismes de classificació en aquest estudi és superior al 90% en tots dos casos. Sabent el tipus de senyal interferent, els algorismes de mitigació i/o localització poden ser optimitzats per a obtenir els millors resultats.

A més a més, aquesta tesi també estudia l'ús de mètodes alternatius de posicionament, partint de la premissa que el servei ofert pels actuals sistemes de navegació per satèl·lit no està disponible i/o no podem confiar en ells a causa de la certesa que estan sofrint un atac. Per tant, davant la necessitat d'obtenir la solució de posició, velocitat, i temps (PVT), s'ha de trobar un sistema alternatiu que ofereixi similars característiques, com per exemple les xarxes cel·lulars (4G, 5G o futurs llançaments) i/o constel·lacions de satèl·lits situats en orbita baixa -LEO per les seves sigles en anglès-. Aquests sistemes de satèl·lit en òrbita baixa probablement usaven diferents bandes freqüencials, la qual cosa els fa menys probables de ser bloquejats alhora que els actuals sistemes de GNSS. En aquest sentit, posicionament basat en satèl·lits en orbita baixa LEO són estudiats, concretament des del punt de vista de la seva viabilitat i el rendiment esperat.

Resumen

En las últimas décadas, los sistemas globales de navegación por satélite –comúnmente llamados GNSS por sus siglas en inglés- se han convertido en un elemento indispensable en nuestra sociedad. En la actualidad, GNSS es usado en una amplia variedad de sectores y situaciones, algunas de ellas ofreciendo servicios críticos, como puede ser el transporte, telecomunicaciones, y finanzas. Por esta razón, y combinado con la relativa facilidad que hoy en día un ataque se puede efectuar con simplemente un transmisor basado en radio definida por software -SDR por sus siglas en inglés- GNSS se ha convertido en uno de los principales objetivos en cuanto a ataques de diversa naturaleza y motivación. Hoy en día, prácticamente cualquier persona puede comprar dispositivos con los que generar interferencias (conocidos como dispositivos jamming) por muy pocos euros. En la actualidad, estos dispositivos se pueden comprar legalmente en muchos países. Aunque a su vez, su uso es normalmente ilegal. Estos dispositivos pueden interferir gravemente en ciertas bandas frecuenciales, como en este caso las usadas por los sistemas de navegación por satélite. La falta de disponibilidad en el servicio ofrecido por los sistemas de navegación (cuya falta de servicio se puede extender a varios km^2)) podría terminar en consecuencias desastrosas, como por ejemplo una pérdida económica o poniendo en serio peligro vidas humanas. Algunos servicios críticos para la humanidad basan su correcto funcionamiento en los sistemas de navegación por satélite.

Fundamentalmente, esta tesis se enfoca en el desarrollo de algoritmos y nuevos métodos para la gestión de interferencias en GNSS. El enfoque principal es en la detección y clasificación de interferencias, aunque también se tratan temas sobre localización y mitigación de interferencias. Los algoritmos de detección y clasifi-

cación analizados en esta tesis fueron escogidos desde el punto de vista del sector de la aviación, en el cual restricciones adicionales (por ejemplo, la posición y orientación de las antenas, numero total de antenas, vibraciones debido al movimiento, etc.) son necesarias de tenerlas en cuenta. Los algoritmos de detención y clasificación seleccionados en esta tesis son aplicados a nivel de pre-correlación, los cuales se basan en la señal recibida en crudo (antes de su procesado en el dominio digital). Estos algoritmos aplican procesado en el dominio digital a la señal recibida (por ejemplo, transformaciones en tiempo-frecuencia). Con los algoritmos analizados, interferencias a tan baja potencia como 0 dB con respecto a la señal deseada pueden ser detectadas. Los algoritmos de clasificación de interferencias combinan las señales recibidas con redes neuronales convolucionales -CNN por sus siglas en inglés- y máquinas de vectores de soporte -SVM por sus siglas en inglés- para determinar el tipo de señal interferente de entre todas las estudiadas. La precisión de los algoritmos de clasificación en este estudio es superior al 90% en ambos casos. Sabiendo el tipo de señal interferente, los algoritmos de mitigación y/o localización pueden ser optimizados para obtener los mejores resultados.

Además, esta tesis también estudia el uso de métodos alternativos de posicionamiento, partiendo de la premisa que el servicio ofrecido por los actuales sistemas de navegación por satélite no está disponible y/o no podemos confiar en ellos debido a la certeza de que están sufriendo un ataque. Por lo tanto, ante la necesidad de obtener la solución de posición, velocidad, y tiempo (PVT), se tiene que encontrar un sistema alternativo que ofrezca similares características, como por ejemplo las redes celulares (4G, 5G o futuros lanzamientos) y/o constelaciones de satélites ubicados en orbita baja -LEO por sus siglas en inglés-. Estos sistemas de satélite en órbita baja probablemente usaran diferentes bandas frecuenciales, lo cual los hace menos probables de ser bloqueados a la vez que los actuales sistemas de GNSS. En este sentido, posicionamiento basado en satélites en orbita baja LEO son estudiados, concretamente desde el punto de vista de su viabilidad y el rendimiento esperado.

Contents

List of Tables

List of Acronyms

ADC	Analog to Digital Converter
AGC	Automatic Gain Control
A-GNSS	Assisted GNSS
AltBOC	Alternative binary offset carrier
AM	Amplitude Modulated
ANF	Adaptive Notch Filter
AoA	Angle of Arrival
APNT	Alternative Positioning, Navigation, and Timing
AWGN	Additive White Gaussian Noise
BB	Broadband
BOC	Binary offset carrier
BoF	Bag of Features
BoW	Bag of Words
bpsk	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
CIA	Central Intelligence Agency
C/N_0	Carrier-to-Noise Ratio
CNN	Convolutional Neural Network
ConvNet	Convolutional Neural Network
COTS	Commercial-Off-The-Shelf
CW	Continuous Wave

DoP	Dilution of Precision
DoS	Denial-of-Service
DPE	Direct Position Estimation
DPI	Dots-Per-Inch
ECEF	Earth-Centered Earth-Fixed
EIRP	Effective Isotropic Radiated Power
EO	Earth Observation
ESA	European Space Agency
EUROCAE	European Organization for Civil Aviation Equipment
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FM	Frequency Modulated
FPD	Frequency Power Detector
GDoP	Geometric Dilution of Precision
GEO	Geostationary Earth Orbit
GLRT	Generalized Likelihood Ratio Test
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HDoP	Horizontal Dilution of Precision
HEO	High Earth Orbit
ICAO	International Civil Aviation Organization
IGSO	Inclined geosynchronous orbit

IIR	Infinite Impulse Response
IoT	Internet-of-Things
ISDA	Iterative Single Data Algorithm
ITU	International Telecommunication Union
JSR	Jamming-to-Signal Ratio
LEO	Low Earth Orbit
LNA	Low Noise Amplifier
LoS	Line of sight
MBOC	Multiplexed binary offset carrier
MCAR	Multi-Correlator output with Auto Regressive modelling
MEO	Medium Earth Orbit
NATO	North Atlantic Treaty Organization
NB	Narrow Band
NLoS	Non Line of Sight
P_{d}	Probability of Detection
PDF	Probability Density Function
PDM	Power Distortion Monitoring
PDoP	Position Dilution of Precision
P_{fa}	Probability of False Alarm
PLD	Power Law Detector
PNT	Pseudo Navigation and Timing
PRN	Pseudo Random Noise
PSD	Power Spectral Density

PVT	Position Velocity and Time
RAAN	Right Ascension of the Ascending Node
RBF	Radial Basis Function
RF	Radio Frequency
RGB	Red Green Blue
RTCA	Radio Technical Committee for Aeronautics
SAR	Search and Rescue
SDR	Software Defined Radio
SMO	Sequential Minimal Optimization
SNR	Signal-to-Noise Ratio
SoO	Signals-of-Opportunity
SoS	Sum-of-Squares
SQM	Signal Quality Monitoring
SSO	Sun-synchronous Orbit
SVD	Singular Value Decomposition
SVM	Support Vector Machine
TDoP	Time Dilution of Precision
TPD	Time Power Detector
TT&C	telemetry tracking and control
TTFF	Time To First Fix
UAV	unmanned aerial vehicles
USRP	Universal Software Radio Peripheral
UWB	Ultra-Wideband

VDoP	Vertical Dilution of Precision
VST	Vector Signal Transceiver

List of Symbols

$+$	Addition Operator
$\oplus$	Direct sum operator
$\lvert \cdot \rvert$	Absolute value
$\lvert\lvert \cdot \rvert\rvert]$	Vector norm
a	Orbit semi-major axis
α	Minimum elevation mask
A_{cover}	Satellite coverage area
b	Orbit semi-minor axis
β	Satellite off-nadir angle
BW_{Rx}	Receiver bandwidth
C_d	Drag coefficient
C_k	GNSS Ranging code
D_k	Navigation data
e	Orbit eccentricity
F	Relative spacing between satellites in adjacent planes
f_c	Carrier frequency
F_{Drag}	Drag force orbit perturbation
f_{J_k}	Jammer k-th tone frequency
F_r	Pulsed signal repetition frequency
F_{swp}	Chirp signal sweep frequency
G	Transmitter chain gain
γ	Fix or adaptive threshold
h	Satellite orbit altitude
H	Range measurement residuals matrix
H_0	Interference-free hypothesis

H_1	Interference hypothesis
$H_n(z)$	Infinite Impulse Response notch filter Z-transform
θ	Satellite Cap angle
θ_0 / θ_1	Unknown interferer parameters
i	Orbit inclination
i_{min}	Minimum orbit inclination for achieving global coverage
J	Number of short observation intervals
K	K-fold coverage
K_a	Pole contraction factor for Notch Filter
λ	Slant range
μ_r	Mean of the received signal $r(n)$
$n(\zeta)$	represents a stationary random process with zero mean and σ_ζ^2 variance
N	Number of samples
ν	Orbit true anomaly
N_0	receiver noise density
N_d	Number of days duration of an orbit in a flower constellation
$N_{minPlanes}$	Minimum number of orbits to give global coverage
N_{minSV}	Minimum number of satellites in the constellation for achieving k-fold coverage
N_{pt}	Number of petals in a flower constellation
ω	Orbit argument of periapsis
Ω	Orbit Right Ascension of the Ascending Node (RAAN)
P	total number of orbital planes in the constellation
$\mathbb{P}$	Probability function
P_c	Carrier Power
P_{J_k}	Power of the k-th jammer signal
P_{Rx}	Received signal power

P_{Tx}	Received signal power
PL	Path loss
ϕ_l	Minimum latitude within the coverage area
ϕ_u	Maximum latitude within the coverage area
Q	Measurement matrix
$r(n)$	Incoming pre-correlation samples in digital domain at the GNSS receiver
ρ	Atmospheric air density at the satellite altitude
$\Re$	Real number set
R_E	Earth radius
S	Reference area of the satellite
$s_K(t)$	Signal leaving from the k-th satellite
$\overline{\#Sat}$	Mean number of satellites in view
σ	Positive number that determines the power law
Σ_{all}	Diagonal error covariance matrix containing the error variances
T	Total number of satellites in the constellation
τ	Pulsed signal duty cycle
θ_{J_k}	Phase of the k-th jammer
T_{TPD}	Time Power Detector test statistic
T_{sweep}	Chirp signal sweep period
V_r	Relative speed between satellite and atmosphere
w^T	Normal vector to the hyper-plane
x	Vector containing the points defining the hyper-plane
(x, y, z)	3-D user position ECEF coordinates
(x_s, y_s, z_s)	3-D satellite ECEF coordinates
$z_0(n)$	notch filter's time-varying zero

Chapter 1

Introduction

1.1 Motivation and Background

In the last decades, GNSS has become a fundamental pillar of our modern society. Besides the widely known purpose of computing the receiver position and velocity (also known as PVT solution), its uses are much more than that. GNSS is used in a wide variety of sectors and services, including energy distribution (e.g., monitoring the power grid), finance (e.g., automated stock trading systems), transportation (e.g., vehicle monitoring and tracking), item tracking (e.g., goods tracking) or telecommunications (e.g., synchronization of base stations). Due to this gain in popularity in the past years, GNSS has become a target of many security attacks such as Denial-of-Service (DoS) attacks. At the same time, it has also brought a rise in the concerns about GNSS security and it increased the importance of having reliable and interference-protected GNSS. For example, the hypothetical loss of GPS service was estimated to cost the US economy more than 1 billion Dollars per day in 2019 [1]. Similarly, a five-day GNSS disruption would have an economic impact of more than 6 million Euros, with the road, maritime, and emergency service impact accounting for 88 percent of the cost [2]. In addition to potential economic damage, this relatively recent rise in GNSS security concerns can also be influenced by the current availability of inexpensive and programmable signal simulators, which can be used to carry out attacks in the GNSS frequency bands. Software-defined GPS signal simulators are already available, such as the one publicly posted on GitHub in 2015 [3]. Such software can be downloaded and run on a wide number of general purpose Commercial-Off-The-Shelf (COTS) RF generation platforms. The price of these devices is relatively low, and they are really easy to get. These devices have already been tested and it has been verified that they can effectively attack standard civil GPS receivers [4].

In the last few years, several intentional wireless attacks against GNSS have been documented. Some of these attacks were carried out under controlled circumstances and with educational / awareness-raising purposes. For example, the authors of [5] took control of a drone by forcing it to acquire counterfeit GNSS signals (i.e., jamming first the GNSS real signals) and interposing fake GNSS signals (e.g., using higher transmit powers). Once the drone acquired the counterfeit GNSS signals, the authors were able to fully control the drone position. Moreover, the drone was still showing the expected position (according to its specified original track) instead of the real one. Another example can be found in [6]. In this case, the authors took the steering control of a yacht by using a similar approach as in [5]. They forced the yacht to re-acquire the GNSS transmissions and superimposed the counterfeit signals instead of the real GNSS transmissions. By doing this, again they took control of the vehicle. On the other hand, some other attacks can be considered malicious, even though some of them might be unintentional. One example of an unintentional attack can be found in[7]. In June 2015, several planes that flew into Northeast Philadelphia Airport reported that they were losing the GPS signal in the last mile of their approach to landing. This usually happened a couple of times per day and the effect was lasting only a few minutes. After an exhaustive investigation, it seems that a driver passing by the surrounding area of the airport was using a jammer gadget inside the vehicle to disable a tracking device installed in his vehicle. This jammer device was powerful enough to disable the real GNSS transmissions in the car, but also in some hundreds of meters around the car. Besides this, most of the attacks against GNSS are mainly intentional. For example, back in 2011, the Iranian military forces captured a Central Intelligence Agency (CIA) reconnaissance drone [8] by fooling the drone's GNSS receiver and making it land in their territory. Or in 2012, it was reported that GNSS transmissions were sabotaged (supposedly by North Korea) near the border between North and South Korea [9, 10]. In 2016, a jamming attack was reported in Russia, near the Kremlin building area. It seems that in order to heavily protect the Kremlin from any possible attack relying on the use of GNSS, in the surroundings of the building one was not able to get its true position but erroneous coordinates hundreds of meters away [11]. In addition, a similar approach has been supposedly used by the Russian government in the last years in order to protect their government members when they were abroad [12, 13]. It seems they fooled the current location of the rest of the users' surroundings when the main members of the government were visiting other territories and regions to minimize possible attacks relying on GNSS. Furthermore, another documented attack against GNSS was reported by the US government in 2017. It was discovered that about 20 ships sailing in the Black Sea were incorrectly positioned [14, 15]. They were positioned by the internal GNSS receivers about 32 km away from their true position. After an exhaustive investigation, it was reported that all the ships were communicating in similar positions, even though the reported positions were not respecting the minimum security distances. After discarding any malfunctioning in the GNSS receivers, it was stated that an attack against GNSS occurred. From 2019 to nowadays, many of these attacks have been occurring more often in Europe [16, 17, 18, 19, 20, 21]. Especially noticeable are those interferences occurring near the border of Finland and Norway with Russia [16, 17, 18, 19, 20] or the jamming detected in Ukraine during the war [21].

Table 1.1 summarizes the main documented attacks in the last 10 years, providing the type of interference disrupting the GNSS transmissions, namely jammer or spoofing, the year it happened, a brief description of the attack, and references to articles/news/reports. We can observe that these attacks are becoming more and more common nowadays compared to some years ago.

As noted in the examples summarized in Table 1.1, attacks on GNSS are feasible and occur every now and then. One of the goals of this thesis has been to provide a deeper survey and analysis of the attack types in GNSS bands and to offer interference management solutions. We have adopted the terminology "interference management" as a comprehensive term for interference detection, classification, localization, and mitigation. Another objective is to provide an analysis of possible satellite-based positioning alternatives, based on LEO satellites [22, 23, 24]. The thesis goals and objectives are described in more detail in Section 1.3.

Some organizations such as International Civil Aviation Organization (ICAO), Radio Technical Committee for Aeronautics (RTCA), EUROCONTROL, and European Organization for Civil Aviation Equipment (EUROCAE) try to safeguard and mon-

Table 1.1 Examples of attacks against GNSS, including jamming and spoofing.

Interference Type	Year	Description	Ref.
Spoofing	2011	Capture of a CIA drone by the Iranian military forces.	[8]
Jamming	2012	Jamming on the Korean peninsula was carried out, supposedly, by North Korea's regime.	[9, 10]
Spoofing	2014	Capture of a drone with educational purpose	[5]
Jamming	2017	Non-availability of GPS signals near Northeast Philadelphia's Airport	[7]
Spoofing	2016	Spoofing in the Kremlin bordering area was carried out, presumably, by the Russian Government.	[11]
Spoofing	2017	The authors took the control of the steering of a yacht, driving it to any place they wanted.	[6]
Spoofing	2017	Attack in the Black Sea reported by the USA government that some ships were positioned incorrectly, over 32 km away from their true position.	[14, 15]
Jamming	2019	Jamming in the Norway Border with Russia during North Atlantic Treaty Organization (NATO) maneuvers.	[16]
Spoofing	2019	Massive worldwide Spoofing was carried out, presumably, by the Russian government.	[12, 13]
Jamming	2021	Emergency landing of long-range unmanned aerial vehicle due to dual GPS signal interference.	[17]
Jamming	2022	Disruptions in GPS services hinder air traffic in central and eastern Finland.	[18, 19, 20]
Jamming	2022	HawkEye 360 Detects GPS Jamming Along Ukraine Border Prior to Russian Invasion.	[21]

itor communications in order to detect any interference source. In addition, these organizations also characterize interferences, providing technical guidance, and proposing and recommending good practices concerning air navigation for new generation standards.

1.2 Research Questions and Methodology

The focus of this thesis lies on GNSS interference management and alternative positioning methods offering global coverage. In this regard, this thesis provides answers to the following research questions:

1. *What interference management solutions exist and which one would be more suitable for a particular GNSS application such as aviation domain?*. This research question has also been addressed in the following publications by the author [25, 26, 27].
2. *How different interference signals could be detected and/or classified based on machine learning approaches?*. This research question is also addressed by the author in [28].
3. *Is LEO satellite-based positioning a good and feasible complementary or alternative to increase robustness in situations when GNSS is strongly affected by interference? If so, what are the main advantages it can provide?* This has been addressed by the author also in [29, 30, 31, 32].
4. *Are LEO mega-constellations the answer to future global positioning using satellite systems?*. This topic has been addressed by the author in [31, 32].

This thesis can be divided into two main parts. The first part focuses on the mathematical model derivation and feature analysis of the most common jamming interference signals provoking intentional interference. In addition, it also analyzes some interference detection algorithms in the context of aviation. This first part answers the first and second research questions listed above. The main contributions to this chapter have been published in [25, 26, 27, 28, 33, 34]. The second part relies on the assumption that we have detected and/or classified the interference, and that the user knows it is suffering a wireless attack against GNSS. Therefore, this second part focuses on feasibility studies on positioning alternatives capable of offering global coverage, and which are the main metrics that describe whether they are a good candidate as an alternative to GNSS. Contributions to this part have mostly been published in [29, 30, 31, 32].

To succeed in this thesis and answer the above-mentioned research questions, a combination of analytical thinking and statistical analysis with simulations based on MATLAB and laboratory testing has been carried out. First, the problem statement was formulated via analytical models, in order to find possible solutions/ways through it. Then a proof-of-concept/initial implementation was done in MATLAB. After succeeding with the MATLAB simulations, laboratory validation tests were done with the instrumentation available in the laboratory (e.g., Universal Software Radio Peripheral (USRP), Vector Signal Transceiver (VST), Spectrum Analyzer, etc.). These tests were carried out to confirm that the initial concept was doable and working with hands-on hardware.

1.3 Scope and Outline of the Thesis

The first objective of this thesis has been to develop a good scientific understanding and mathematical models regarding potential attacking signals. An additional goal has been to analyze the performance losses when GNSS suffers intentional or unintentional interference. Related to this first objective, the thesis also emphasizes how relatively easy an intentional wireless attack can be performed on GNSS signals with the nowadays available tools. The second objective of this thesis has been to offer solutions to this GNSS security issues or at least try to find a way out of them. Therefore, this thesis investigates possible countermeasures, such as techniques to detect GNSS attacks and classify those attacks according to specific features to further mitigate their effects with signal-specific algorithms. A third objective has been to look for an alternative positioning solution in case no effective countermeasure is found. In this sense, we investigate to find alternative systems when getting a reliable PVT solution. One of the most promising was the use of LEO satellites as an alternative to the current MEO GNSS. In order to fulfill these objectives, mathematical modeling and extensive computer simulations have been carried out in order to model the LEO main features and orbit types.

This thesis is divided into two main parts. The first part comprises Chapter 2 and Chapter 3. Chapter 2 gives an overview of GNSS and background information about interferences in GNSS context. The most common interference signals are classified, modeled, and analyzed. Chapter 3 analyzes in more detail the effects produced by the interferences in GNSS signals and measures the performance of different detectors and classifiers of interferences. In addition, Chapter 3 provides numerical evaluations comprising both detection and classification, as well as simulated and laboratory GNSS data. The second part of this thesis is covered in Chapter 4. It comprises alternative or complementary positioning, based on LEO satellites. Chapter 4 analyzes the suitability of satellite constellations based on LEO satellites as an alternative to the current MEO GNSS constellations. This chapter also provides numerical results about constellation geometry, coverage, and link budget measuring the suitability of different launched or planned LEO and MEO constellations for positioning purposes.

1.4 Novelty and Author Contributions

In this section we describe the novel contributions provided in this thesis along with the main author's contributions:

1. Presenting a comprehensive state-of-the-art of the currently operative GNSS constellations, including descriptions about GNSS constellations, system architecture, frequency bands, signals transmitted by the satellites, GNSS receiver main blocks, etc., as well as a literature review and unified mathematical models about RF interference types and impairments. The contributions related to this point have been also published by the author in [25].
2. Implementation, comparison, and investigation of seven interference detection methods for jammer detection in GNSS. Four papers [25, 26, 27] have been published on this theme by the author. Papers [25, 27] mainly focus on simulated GNSS data, while papers [26] focus on real GNSS data recorded in the laboratory.
3. Presenting a novel approach for classifying interferences by treating the problem as a classification of black-and-white images, based on time-frequency analysis and image mapping of a jammed signal. The proposed method relies on machine learning to achieve its purpose. Contributions related to this topic were published in [33, 34].
4. Presenting an analysis about the feasibility of LEO constellations as complementary or an alternative to the current MEO satellite-based positioning. This contribution is also provided in the publications [29, 30, 31].
5. Analyzing and comparing different constellations deployed and planned to be launched LEO from the point of view of positioning feasibility. The different

LEO constellations were analyzed from the point of view of coverage provided, DoP, and link budget. These LEO constellations were also compared with the current MEO GNSS systems. Contributions related to this point are also addressed in [29, 30].

6. Analyzing, from the point of view of coverage considerations, the minimal LEO constellation provides global coverage with at least four satellites in view at any time; Providing mathematical models along with simulations to prove the achieved results.

1.5 Impact of the research

This thesis has been partially shaped according to the requirements faced in the different projects that contributed to the financing. For example, the H2020-funded GATEMAN (GNSS-Based Navigation Threats Management) [35] project deeply influenced the final selection of the jamming detection algorithms. GATEMAN project addressed problems arising from GNSS interferences (either jamming or spoofing) for the airspace sector. In order to mitigate the effects of GNSS interferences, GATEMAN proposes and develops techniques to tackle the interferences from two ends: i) Integrating a GNSS interference air navigation threats management for minimizing the effects of the interferences (detecting and localizing the source of interferences and mitigating the spoofer effects) and ii) Usage of 5G as an alternative mean of navigation in case of GNSS degradation during approaches, which is the most critical phase during a flight. The results obtained during the GATEMAN project proved the feasibility of the proposed methodology, being good candidate techniques for consideration in the future, although the interference localization performance needs to be evaluated with further experiments and analysis. Performance studies on the use of the 5G cm-band as an alternative to GNSS confirmed that the approach was limited to low-altitude operations (e.g., approach phase for commercial aircraft), while the mm-band was limited to close-to-ground operations (e.g., taxiing for commercial aircraft). These results were an initial analysis of the usage feasibility of 5G networks. Although so far no regulation and/or frequency allocation has been done in this sense. Therefore, our studies used regular 5G frequency allocation for aircraft applications, which may not be totally realistic in the sense that for aircraft applications there are additional regulations (i.e. limited power, frequency, bandwidth usage, etc.). The research done within GATEMAN contributed to publications [25, 26, 27, 36].

The Academy of Finland-funded ULTRA (Ubiquitous Localization, communication, and sensing infrastrucTuRe for Autonomous systems) [37] project contributed to further investigation of alternative positioning methods in addition to GNSS. ULTRA aims to create novel signal processing methodologies that allow the use of 5G technology jointly as a localization, communication, and radar system. The Academy of Finland-funded project PRISMA (Reliably connected Industrial Systems with Mobile mm-Wave Access) [37] project focused on reliably connected industrial systems with mobile mm-Wave access aided by positioning. Both ULTRA and PRISMA projects contributed to the publication [36]. In addition, the author also contributed to the development of new low-power high-accuracy signal acquisition mechanisms for satellite-based positioning and a Signals-of-Opportunity (SoO) analysis for the future LEO satellite positioning systems [29, 38].

European Space Agency (ESA)-funded FINESSE (FINgEr-printing GNSS for authEntication) project also contributed to this thesis, especially regarding the jamming signal classification. The main objectives of this project were: i) assessing the feasibility of employing RF fingerprinting for authenticating GNSS satellites and user terminals; ii) simulating and evaluating the performance of the selected radio signal identification and classification techniques, and iii) to come up with a reliable GNSS signal authentication concept based on radio-level signal classification. The main results that contribute to FINESSE can be found in [33, 34].

TEK100/JAES foundations-funded INCUBATE (INdoor navigation form CubeSat TEchnology) [39] aims to promote the usage of LEO small satellites for the precise positioning, navigation, and timing information in challenging conditions and in indoor environments. INCUBATE evaluates the feasibility of such a LEO constellation from both technical and economical points of view. Moreover, INCUBATE analyzes all three main segments in any satellite system: space, ground, and user. The main results so far can be found in [29, 30, 31]

In addition to the contributions to the different projects described above, the work done so far in this thesis has influenced and inspired many other researchers from many countries based on Google Scholar outputs. Our publication in [25], carried out within the work done in this thesis, was cited by several other authors in [40, 41, 42, 43, 44, 45, 46, 47]. As examples of research avenues opened by our research in [25], the authors in [40] focused on the direction of the arrival estimation and proposed a new algorithm to provide information to a ground control center to locate the source of the jammer. The research in [40] presents the design of the chain of algorithms and their preliminary tests in a laboratory setup The authors in [41] proposed using adaptive notch filters to suppress the jamming interference effect. The achieved results in [41] demonstrated that the proposed solution can effectively mitigate the jamming effects. The authors in [42] focused on interference based only on spoofing. They comprehensively analyzed the ability of different anti-spoofing methods at the signal level and the data level to protect from different spoofing attacks. The authors of [43] provided a survey paper on different interference localization mechanisms and provided simulations to evaluate their performance. The authors of [44] proposed a solution for GNSS drone jamming. This method is based on using drones, which position is previously known before any jamming attack, as positioning anchors. In case of non-availability of GNSS, the authors in [44] proposed using the drone position, which is perfectly known, to continue providing positioning service. In [45], the authors proposed the use of a dual frequency antenna array for robust aeronautical navigation. The authors in [46] proposed a method based on the direction of arrival of the synthetic aperture to suppress the jamming signals by estimating and producing nulls in its direction of arrival. The authors in [48] proposed an angle of arrival algorithm for the location of civil aviation interference and the use of drones for aerial surveillance and the location of the source of the interference. Finally, in [47] the authors proposed a method for accurate localization and tracking of interference using LEO satellites as sensors and drones as interference emitters. Besides the publication [25], our publication [28], in which a methodology based on machine learning and image classification is proposed, also contributed to several follow-up research works as, for example, [49, 50, 51, 52, 53, 54, 55, 56]. The authors in [49] proposed the use of a deep neural network in combination with the cross-ambiguity function (during acquisition) for the detection and classification of spoofing. The results in [49] show that complex neural networks are effectively able to capture the nature of spoofing attacks. In [50], the authors proposed the use of incremental learning (a machine learning technique that allows the introduction of new information to a previously trained network) to create jammer classifiers that can expand and expand their capabilities without the need to train the algorithm from scratch. The authors in [51] reviewed the possibilities of different machine learning algorithms to enhance GNSS performance and usability. The authors reviewed different algorithms by comparing their performance. In [53] the authors proposed to use the machine learning algorithm k-nearest to the pre-correlation GNSS interference detection of some types of jamming, such as chirp. The authors in [55] performed a similar approach to the presented in this thesis, although combining PSD, spectrogram, raw constellation, and histogram information. They compare the performances of different machine learning algorithms including SVM, Logistic Regression (LR), and Random Forest (RF). Although publication [28] contributed not only in the field GNSS, but also in fields such as RADAR [57, 58]. In [57], the authors proposed two methods to predict the appropriate jamming technique for a received threat signal using deep learning.

Finally, our publication [34] also impacted some follow-up research works in [59, 60, 61, 62, 63]. In [59], the authors proposed a multi-frequency band algorithm for detection, alerting, and reporting systems in GNSS and RADAR. The authors in [60] provided a survey of many radio frequency fingerprinting methods applicable in GNSS and they also proposed a novel methodology for spoofing detection at GNSS pre-correlation data level. In [62] the authors focused on the different preprocessing steps that can be used on the input training data and tested the results on a fixed deep learning architecture. The authors in [62] combined the information of both time and frequency domain data to achieve radio frequency signal classification. The authors in [63] provided a survey on machine learning technologies for the identification of devices in Internet-of-Things (IoT) along with the detection of compromised or falsified devices.

Furthermore, our contributions have not only influenced GNSS jamming and spoofing follow-up studies but also LEO-satellite-based positioning. Our works in [29, 30] were cited in several follow-up studies, e.g., [64, 65, 66, 67, 68, 69]. The authors in [64, 66] proposed a method for processing the Doppler shift measured from different LEO satellites to achieve positioning at the user-end. With the proposed approach no specific signaling is needed to measure the propagation delay. In [65], the authors proposed a method to combine pseudorange and Doppler shift measurements from LEO satellites for positioning purposes. The authors in [67, 68] demonstrated the feasibility of achieving positioning using real Doppler measurements received from real satellite constellations. The results in [67] showed a horizontal positioning error of 10 m by tracking the Doppler of six Starlink LEO satellites.

Chapter 2

Types and Analytical Models of Interference in Satellite-based Positioning

In this chapter we give a general overview of interferences, in particular GNSS interferences, but applicable to any other wireless system. In the first part of the chapter, we will give a general overview of GNSS, describing the system architecture and listing the main GNSS constellations currently available in the sky, including their main parameters (e.g., orbit altitudes, orbital periods, number of satellites in the constellation, etc.). Then we describe some basics about GNSS signals, showing signal examples in both time and frequency domains. Following, we describe the main stages of a typical GNSS receiver and the principal functioning purpose of each receiver stage.

In the second part of the chapter, we describe and classify most of the interference types against GNSS, comprising both the intentional and non-intentional. We also show specific interference signal types, providing mathematical models and simulation examples. In addition, we also provide explanations about how they may affect the GNSS transmissions, by for example analyzing the received GNSS spectrum. Finally, we list and describe other types of interferences, such as channel impairments, including atmospheric scintillation and multipath.

2.1 Satellite-based Positioning Systems and Their Susceptibility to Interference

In this section, we first describe currently operating satellite-based positioning systems, which are mainly based on signals broadcast by satellites in MEO. We describe the system architecture for those systems, and we also briefly describe how the signal is generated and which type of information it carries. In addition, we also explain the main blocks of a satellite-based positioning receiver. We then provide an introduction to wireless interferences in the context of satellite-based positioning, providing some examples and categorization of different types. We make an introduction to future satellite-based positioning systems, based principally on LEO constellations, and we finally discuss the particularities of these satellite systems in terms of coverage and susceptibility to interferences.

2.1.1 Currently Deployed Satellite-based Positioning Systems and System Architecture

The main system architecture for the currently deployed GNSS is described in the following lines. Any GNSS is composed basically of three segments: the space segment, the control segment, and the user segment [70]. The space segment comprises the satellites in space and the control segment deals with the management of the satellite operations. On its behalf, the user segment covers the equipment required (e.g., receivers) for using the broadcasted signals from the satellites. As we see, each segment has a specific role in the overall system.

The space segment is basically composed of satellites in the sky. These satellites are placed in a determined orbit around the Earth. The GNSS satellites are mostly placed in MEO orbits, between 19000 and 24000 km of altitude approximately, depending on the GNSS constellation. The period, which is the time it takes one satellite to perform a complete orbit cycle, is approximately between 11 hours to 14 hours (which depends again on the GNSS constellation and the chosen orbit altitude). Table 2.1 summarizes the space segment attributes for the most common GNSS constellations. With the set of satellites in orbit placed around the Earth, almost all users with a clear view of the sky have a minimum of 4 satellites-in-view from each constellation. Usually, the user has much more than 4 satellites in view, given the combination of compatible GNSS constellations, such as GPS and Galileo, which are interoperable at the system level. The satellites in the sky broadcast the ranging signals and navigation data to the user equipment, which allows measuring the pseudoranges between satellite and user, and hence determine the user position by trilateration. The communication is typically unidirectional; the user receiver is passive (it only receives the broadcast signal and does not transmit anything back, with the exception of Search and Rescue (SAR) devices which support also a return link).

Table 2.1 GNSS Space Segment comparison for the main four constellations.

	GPS	Galileo	GLONASS	BeiDou[1]
Country	USA	Europe	Russia	China
Orbital Altitude in MEO	20200 km	23222 km	19100 km	21528 km
Approximated Orbital Period	12 hours	14 hours	11 hours and 15 min	12 hours and 38 min
Active Number of Satellites in MEO	24	27	24	27
Number of Orbital planes in MEO	6	3	3	3
Inclination (deg)	55	56	64.8	55
Multiple Access Scheme	Code Division Multiple Access (CDMA)	CDMA	Frequency Division Multiple Access (FDMA)[2]	CDMA

The control segment is composed of a set of ground control stations located

---

[1] Only MEO part of BeiDou constellation is listed. Five additional Geostationary Earth Orbit (GEO) satellites form part of BeiDou constellation, but for a fair comparison with the rest of GNSS constellations , Table 2.1 focuses only on MEO.

[2] New GLONASS-K satellites are planned to use a CDMA approach, similar to the rest of GNSS constellations. their current status is uncertain.

across the Earth. Each GNSS constellation has its own ground stations. The control segment is in charge of determining and broadcasting to the satellites some crucial data such as the navigation message the satellites broadcast, accurate timing data including the navigation messages, the telemetry tracking and control (TT&C) commands, satellite ephemeris prediction, and clock parameters, keep track and correct (if needed) GPS time, etc.

Figure 2.1 shows the typical satellite constellation segments, namely space, control/ground, and user segments.

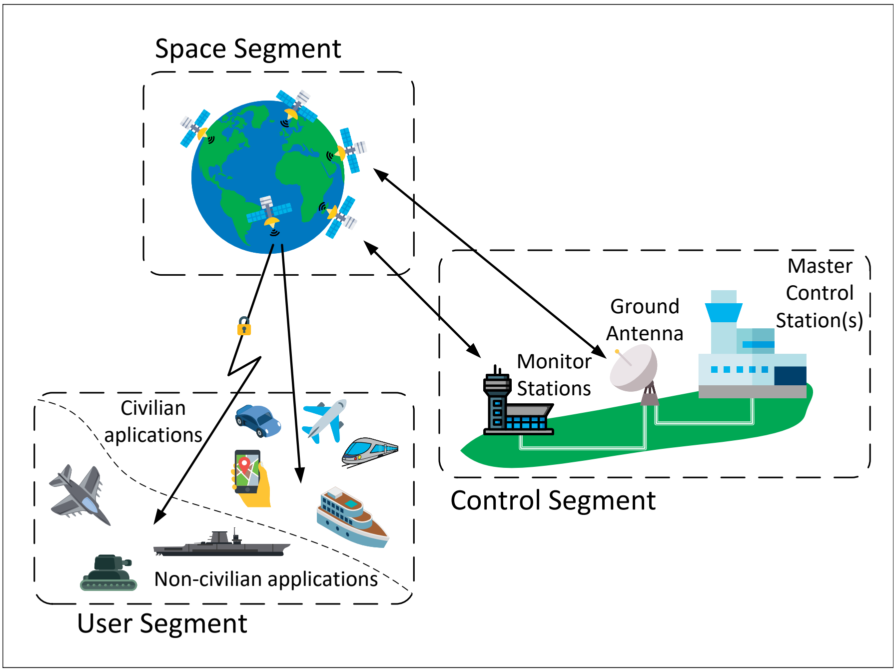


Figure 2.1 Illustrative plot representing the three main segments in GNSS architecture.

2.1.2 GNSS Signal Description

The GNSS satellites continuously transmit navigation signals in two or more frequency bands, usually in L-band (between 1 GHz and 2 GHz). These signals contain ranging codes and navigation data that allow the users to compute the signal traveling time and satellite coordinates, for then computing the user' PVT solution. The main signal components are described as follows:

- Carrier: It is a waveform (usually sinusoidal) that modifies the signal into an information-bearing signal with the purpose of transmitting the information as an electromagnetic wave. This carrier wave usually has a much higher frequency than the input signal does. The frequency bands are chosen to minimize the impact of the signal propagation channel (e.g. the attenuation due to the atmosphere) and to limit the physical size of the antennas. GNSS typically uses frequencies in the L-band frequency range, specifically between 1 GHz and 1.6 GHz. Uplink TT&C signals from ground stations are typically in S-band (between 2 GHz and 4 GHz).
- Ranging Code: Consists of a combination of 1s and 0s that allows the receiver to determine the travel time of the radio signal from the satellite to the receiver. The sequence of 1s and 0s belongs to a family of codes called Pseudo Random Noise (PRN) sequences or simply PRN codes. These codes behave statistically as white noise. This means that the PRN codes are orthogonal between them, which results in the cross-correlation (the correlation between two different PRN codes) being minimum (approximately zero), and the auto-correlation (the correlation between a certain PRN code with itself) is maximum (if both codes are perfectly aligned). This PRN code allows the same different satellites to transmit the signaling simultaneously, using the same channel without any collision in the information. Each satellite differentiates its transmission by using a different PRN code. These codes also allow precise range measurements and mitigate most of the undesired effects of reflections and interfering signals received by the antenna.
- Navigation data: It is a binary-coded message that provides information regarding the satellite, required for computing the PVT solution at the user end. The navigation data contains ephemeris information (satellite position and velocity), clock bias parameters, almanac (accuracy-reduced ephemeris data), satellite health status, and some other complementary information.

The signal leaving from the k-th satellite can be modeled in the time domain as:

$$S_k(t) = \sqrt{2P_k} \cdot (C_k(t) \oplus D_k(t)) \cos(2\pi f_c t) \tag{2.1}$$

where P_k is the carrier power, C_k is a sequence of $+1$s and -1s composing the PRN code, D_k corresponds to the navigation data bits, $\oplus$ stands for direct sum operator and $\cos(2\pi f_c t)$ is the carrier wave, where f_c is the frequency of such carrier. In Figure 2.2, we show an example of a transmitted GNSS signal using Equation (2.1) with a carrier frequency of 1.57542 GHz. We observe that the general waveform of the signal is a sinusoidal carrying the PRN code composed by ± 1.

The signal at the GNSS receiver side, in an additive Gaussian noise environment, can be written as the sum of N individual signals from Equation (2.1), plus a noise term:

$$S(t) = \sum_{k=1}^{N} \sqrt{2P_k} \cdot (C_k(t) \oplus D_k(t)) \cos(2\pi f_c t) + w(t) \tag{2.2}$$

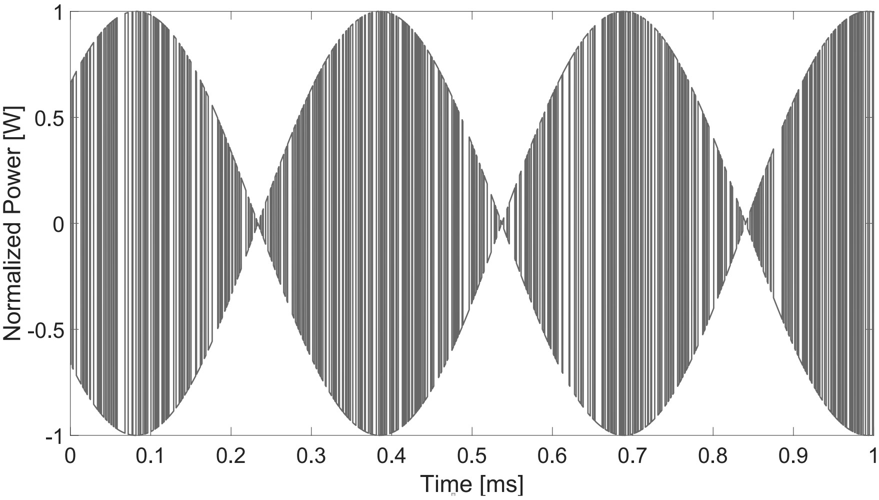


Figure 2.2 Example of GNSS signal transmission from a single satellite in the time domain.

In order to propagate the transmissions, the signal in Equation (2.1), is modulated by a specific modulation scheme, which depends on the constellation and signal design. Phase modulation is typically used in GNSS to carry the PRN code and navigation message data on the carrier frequency. The most commonly-used modulation technique for GNSS signals has been traditionally Binary Phase Shift Keying (bpsk). In bpsk, the data is either transmitted "as is" or with a 180° phase shift over successive intervals in time depending on whether the digital data to transmit is a 0 or a 1. Some other more advanced modulation schemes such as Binary offset carrier (BOC), Alternative binary offset carrier (AltBOC), or Multiplexed binary offset carrier (MBOC) also exist and are typically used as well in some specific cases.

In addition, Forward Error Correction (FEC) is employed, whereby redundant bits (more than the original information originally had) are transmitted over the channel according to some prescribed method, allowing the receiver to detect and correct some errors that may be introduced by noise, interference, or fading.

2.1.3 GNSS Receiver Main Blocks

Based on the received signal from the different satellites in the sky, the GNSS receiver determines the PVT solution. A typical GNSS receiver configuration is shown in Figure 2.2. It is composed of the following main processing blocks:

- **Antenna/s**: The antenna is the first element in any GNSS receiver chain. Its main purpose is to collect the received signals, which are transmitted by the satellites, making them usable for the further receiver blocks in the chain. Multiple antennas or antenna arrays are also possible in GNSS receivers [71]. Sometimes, the antennas are embedded in the receiver front-end, but in the case of multi-band GNSS, antennas tuned to certain frequency bands may come with their own front end.
- **Front-end**: The front-end is located just after the GNSS antenna. It is usually composed of a Low Noise Amplifier (LNA), a band-pass filter, a frequency converter (either to an intermediate frequency or directly to the baseband), and some additional filtering stages (e.g., anti-aliasing filters).
- **Analog to Digital Converter (ADC)**: The ADC converts the analog waveform to digital samples by performing an analog-to-digital conversion at a specific number of quantization bits. The signal at the output of the ADC block is the signal in the so-called pre-correlation domain, i.e., before any correlation with a PRN code replica is performed at the receiver side. Depending on the chosen number of quantization bits, the signal will be more or less degraded in terms of Signal-to-Noise Ratio (SNR). For example, by using 2-bit quantization the signal is degraded (in terms of SNR) about 1.5dB. While if using 1-bit quantization, this degradation rises to about 3.5 dB [72]. Although this degradation can be minimized depending on the ratio of the maximum quantization threshold to the input noise standard deviation level [72].
- **Acquisition Module**: The main goal of the acquisition module is to determine

which satellites are in view from the receiver position and to calculate a rough estimate of parameters needed in further blocks, namely tracking and navigation modules. These parameters typically are the index of the satellites (which satellite's ID is in view), the coarse time-delay estimate from the satellite to the receiver, and the coarse Doppler shift estimate of these satellites. These estimates will be used by the tracking module as initial values to initialize its routines. The receiver signal acquisition relies on performing correlations between the received signal and several time-shifted and frequency-shifted PRN code replicas.

- **Tracking Module**: The main objective of the tracking module is to refine the initial estimations of Doppler shift and signal delay, provided by the acquisition module, and then be continuously tracked in order to estimate any variation of these parameters. The tracking of a specific satellite only is initialized if the acquisition is successful, as some of the satellites initially considered in-view may be at very low elevation angles with respect to the user position or be in Non Line of Sight (NLoS) conditions, i.e., lack of a direct Line of sight (LoS) between the satellite and receiver due to the existence of obstacles, buildings, tunnels, trees, foliage, etc. Therefore, during the tracking process, accurate Doppler shift and time-delay estimates from each satellite in view are obtained, allowing the GNSS receiver to track the dynamics of the user. As at least four satellites are needed to get the position estimation, there should be at least four tracking channels in parallel, corresponding each satellite channel to a single satellite.
- **Navigation Module**: The focus of the navigation module is computing the PVT solution, based on the values tracked by the tracking module and combining the information coming from all the satellites in view.

Figure 2.3 shows an example of a typical GNSS receiver. The GNSS transmissions are collected by the antennas. The signal is processed in the front end. The amplified and filtered analog signal is then converted to digital samples in the ADC with a specific number of bits. This digitalized signal is then correlated by the PRN local replicas, in order to find which satellites are in view. At this stage the GNSS receiver must deal with the ambiguity of the acquisition function, caused both by the notches or low-level values and the multiple peaks appearing within ±1 chip from the main correlation peak in the correlation envelope [73, 74]. In addition, a coarse estimation of the signal delay and Doppler is carried out, which is useful for the following blocks. In the tracking block, the coarse estimation is fine-tuned, in order to find which is the actual delay and Doppler in each satellite transmission. Knowing the delay and the velocity at which the signal travels (i.e., the speed of light), we can determine the satellite distances from the receiver's perspective. And by trilaterating these distances, we can determine the user PVT solution. The PVT solution is computed in the navigation block. Finally, the PVT solution is provided to the user. As we will see later, we can perform interference detection, localization, and mitigation techniques at different stages of the GNSS receiver. For example, in the front end, we can perform some techniques on the analog signal in order to determine if interference is present. The same at the pre-correlation or post-correlation stages. Pre-correlation stands for the quantized signal obtained directly from the ADC output in which we still don't know which satellites are in view. On the contrary, the post-correlation stage stands for the individual satellite signal after the de-spreading process (multiplication by the unique satellite PRN code). Finally, during the navigation block can also be applied different techniques to cross-check if, for example, transmission is coming from a real satellite or a fake transmitter mimicking an original satellite.

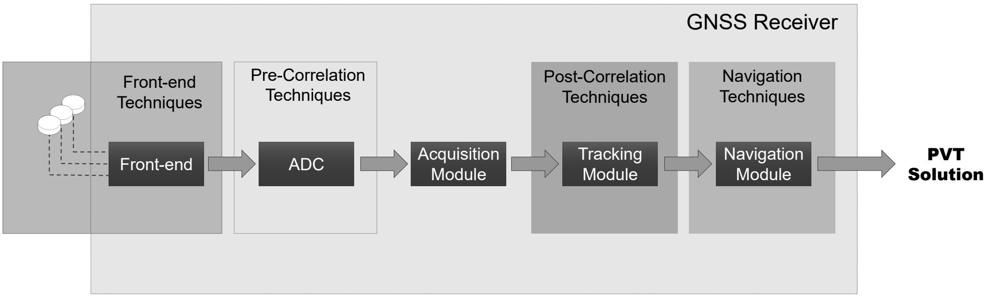
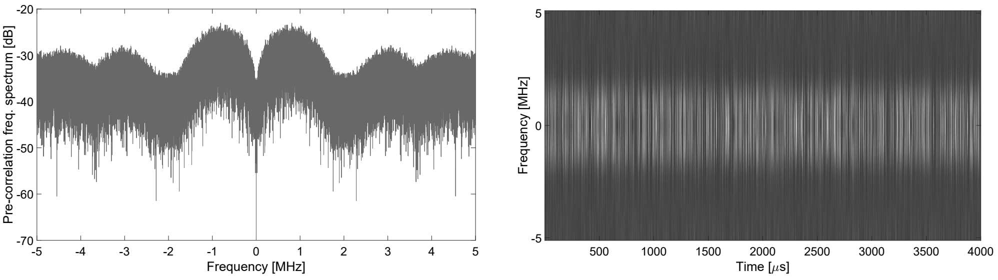


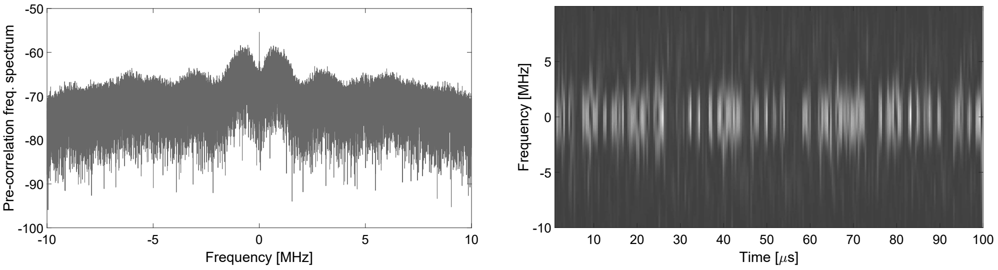
Figure 2.3 Simplified block diagram of a typical GNSS receiver.

Besides the generic GNSS receiver blocks described above, it also exists in more advanced configurations. For example, the so-called Direct Position Estimation (DPE) [75, 76], in which the receiver integrates code/carrier tracking loops and Navigation Solution in a single step. The time-delays and Doppler shifts to the visible satellites are estimated to solve geometrically and compute the PVT solution. A different approach is the one based on vector tracking loops [77, 78]. This approach combines the tracking and navigation modules into a single one, processing simultaneously all received signals from different satellites at the same time. These configurations, and some others, have advantages and drawbacks to be considered and deeply analyzed before their implementation, such as their accuracy in the PVT solution, computational load, and efficiency. Further in this thesis, we just consider the typical configuration when referring to a GNSS receiver.

Figure 2.4 shows the PSD and spectrogram for a simulated and recorded Galileo E1 signal at the receiver end with no channel applied. As we can see in Figure 2.4, the received signal suffers a huge attenuation due to the big distance it has traveled from satellite to receiver. Typically, transmitted powers are about 45 W. while typical attenuation levels due to propagation are ≥ 180 dB [79]. Typical average received power levels are ≤ -150 dBW [79], while the noise power at the receiver end is usually considered as ≥ 140 dBW [79].



(a) Simulated GNSS spectrum **(b)** Simulated GNSS spectrogram



(c) Recorded GNSS spectrum **(d)** Recorded GNSS spectrogram

Figure 2.4 Examples of Power Spectral Density (PSD) and spectrogram for a simulated and recorded Galileo E1 signal. Receiver bandwidth is set to 5 MHz for the simulated signal and 10 MHz for the recorded signal.

2.1.4 Future Satellite-based Positioning Systems

GNSS offers a continuous, global, and costless (for the end-user) PNT service outdoors, with accuracies ranging from a few meters to even sub-meter level. Despite being a successful technology for a wide number of diverse applications, the current GNSS has some weaknesses, including the following:

i) Indoor positioning is not available due to weak-signal reception [80]. As we have mentioned in Section 2.1.2, received signal power in MEO GNSS is below -150 dBW, with path loss due to signal long distance travelling higher than -180 dB. This typically makes unavailable the positioning signal from MEO satellites due to extra losses while penetrating the buildings.

ii) Performance is poor in dense-urban canyons [81, 82, 83], areas with tunnels, and locations a few meters underground due to heavy multipath reflections and huge attenuation of the signal.

iii) MEO GNSS are increasingly suffering from interferences such as coming from jammers and spoofers, as we have seen in real-case examples in Section 1.1. These interferences coming from jammers are especially harmful due to the extremely low power GNSS signals are received and the easiness a jammer can be set up.

iv) Assisted GNSS (A-GNSS) [70] can be used to overcome some of the above-mentioned weaknesses. With A-GNSS the mobile network is used to aid the user GNSS receiver and improve the GNSS availability and reduce the Time To First Fix (TTFF). The mobile network, which can continuously receive and track signals from the satellites, can process the received GNSS data and send it to the user using the mobile network [70]. The user receiver can use this data to calculate the position when the satellite signals are weak or can use this data for further error correction to improve the positioning accuracy. A-GNSS has a few downsides though. A-GNSS usually requires some sort of wireless Internet access (e.g., Wi-Fi) or internet subscription (e.g., cell phone data connection) to access the service, which often costs extra or it is not available globally (for example in low populated areas). In addition, there are also some privacy concerns, as a third-party server knows the exact user location.

For the reasons above-mentioned, in addition to the current MEO GNSS, complementary PNT solutions are needed in the near future. One of the most promising complementary methods currently under research is the so-called LEO-PNT [84, 85]. This solution is based on LEO satellites, whose altitude is between 200 km to 2000 km above the Earth. In particular, the satellites are based on small-sized or miniaturized satellites, which have low-to-moderate costs of building, launching, and maintenance. The architecture of the system will be similar to the described above for current MEO systems, which is divided into three segments: the space segment, ground segment, and user segment. In addition to continuous and global coverage, the main advantage of using LEO orbits is that due to the closer proximity to the Earth, the attenuation due to propagation is considerably lower. As a drawback, the coverage per satellite is heavily reduced due to the closest proximity to the Earth of LEO with respect MEO. For this reason, a higher number of satellites in the sky is required for covering the whole Earth. In addition, the cost of putting in orbit a whole constellation from the scratch is huge, compared with the alternatives described next. A different solution can be found in [85, 86, 87, 88], where signals from LEO satellites already in orbit (and which purpose is not positioning) are used as SoO for offering a PNT solution. The advantage of this approach is that no dedicated constellation has to be launched, which decreases considerably the costs. But typically, the accuracy one can get from this approach is much lower than with a dedicated system. Finally, a third approach is shown in [89, 90], in which a LEO system is proposed to enhance the current MEO constellation by re-broadcasting its signals. These approaches would benefit from a reduced cost with respect to launching a completely new constellation, but the satellite payload needs to be adapted in order to be able to process GNSS signals, which might be challenging and even not possible for the satellites already launched.

More details about LEO-PNT will be given in Chapter 4.

2.2 Interference Classification

We can define an RF interference as any disturbance provoked by an electronic system or device due to external electromagnetic emissions at the frequency of interest [91, 92, 93]. In Figure 2.5 we show the different frequency bands each GNSS constellations use in different colors. Galileo frequency bands are represented in blue, GPS are represented in yellow, GLONASS in red, and BeiDou in purple.

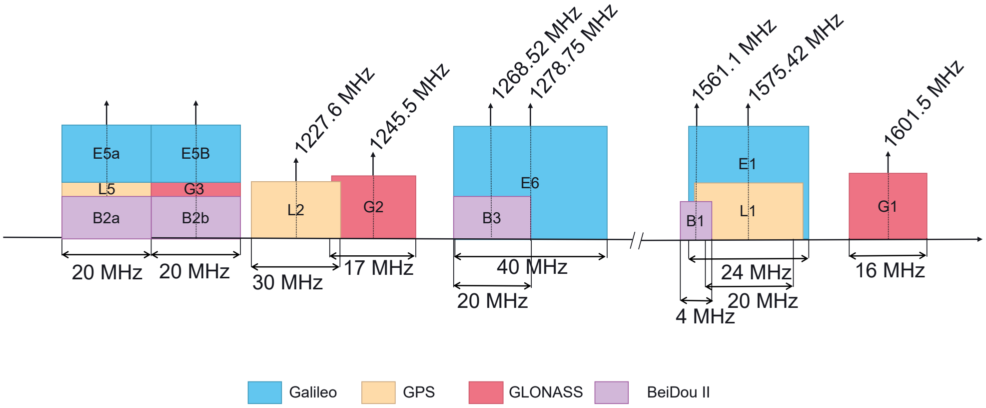


Figure 2.5 GNSS frequency bands for GPS (yellow), Galileo (blue), GLONASS (red) and BeiDou (purple).

RF interference can be classified according to different criteria (e.g., wideband/-narrowband interference, intentional/non-intentional, DoS/signal forgery, etc). In this thesis, we adopt a classification similar to the ones shown in [91, 92, 93, 94]. This classification is shown in Figure 2.6. In the first instance, we divide the interference as artificial (or human-made) and natural (or channel-based), according to if they are produced by different wireless transmitters (artificial) or the interference is provoked by wireless channel effects (natural). If we focus on the human-made interferences, we can in turn divide them according to if they were generated by a malicious transmitter or not in: intentional and unintentional interferences. Intentional interference includes jamming, spoofing, and meaconing. Jamming refers to transmitting any signal deliberately into the frequency bands of the signal of interest, usually at higher powers in comparison to the signal of interest. Spoofing refers to transmitting counterfeit GNSS signals towards the receiver with the intention of fooling the user receiver. Meaconing is a particular case of spoofing. It refers to broadcasting back the authentic GNSS signals by a malicious transmitter. As for unintentional interference, we divided them into co-channel and adjacent channel interference. Co-channel interference is provoked by emissions of a transmitter using the same channel (e.g., radio resource allocation problem or cross-talk). It includes out-of-band emissions of additional RF systems, which are commonly harmonics of broadcast systems, but also signal leakage from Ultra-Wideband (UWB) systems, personal electronic devices, and/or RF systems installed near the user receiver. Adjacent channel interference is due to a RF emission into a different channel, leaking energy into the channel under consideration (e.g., intermodulation products). Many unintentional interferences can be still modeled as a jammer. Natural (or channel-based) interference is due to interactions of the RF transmissions with the environment on the wireless channel (e.g., reflection, diffraction, refraction, scattering, scintillation, etc.). This can cause multipath propagation (i.e., delayed and attenuated copies of the same signal) or ionospheric and tropospheric delays and attenuation. Space weather effects in the ionosphere, causing scintillation, are another source of natural interference that are specific for satellite communication and navigation systems. Fading, shadowing, and Doppler effects over the wireless channel can also be seen as a form of natural interference.

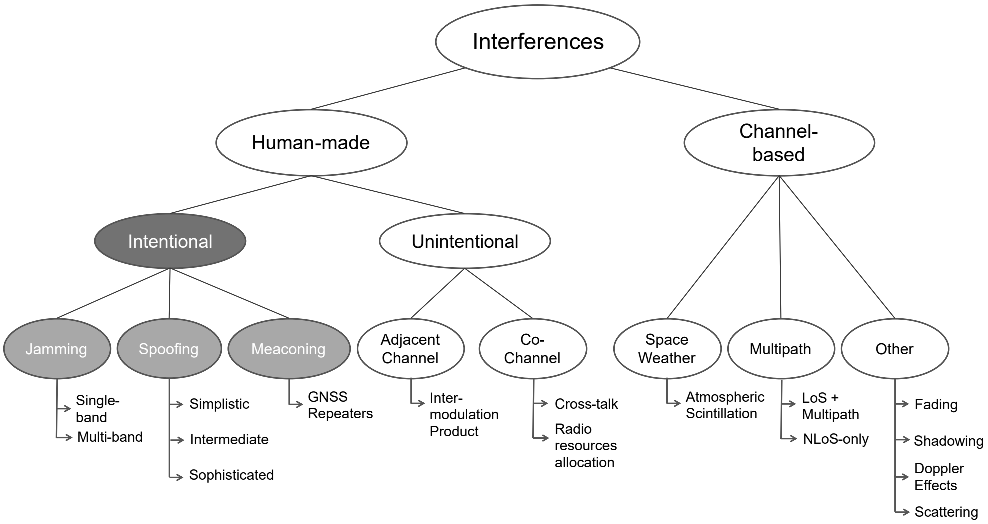


Figure 2.6 RF interference top-level classification.

2.3 Jamming Classification

According to the literature, jamming signals can be classified in different manners (e.g., according to used bandwidth, if the signal is continuous/ in burst, linear/non-linear modulation type, etc). One of the proposed methods to classify jamming signals is based on the signal type and difficulty to detect them, from lowest to highest difficulty, divided into four categories [95, 96], namely class I to class IV. We propose to include an additional class to incorporate those jammer types not fitting in the rest of the categories. In addition, Table 2.2 summarizes the different classes, jammer type, baseband signal model $j(t)$ as a function of time, and the main parameters describing these jammer types. The considered jammer classes are listed next:

1. **Class I, Continuous Wave (CW) jammers**: The simplest type of jammers and one of the most studied ones are those based on Continuous Wave (CW) modulation. CW modulations typically refer to signals with bandwidth up to 100 kHz. Class I includes the single and multi-tone Amplitude Modulated (AM) and Frequency Modulated (FM) jammer types. These signal types typically are the easiest jamming signals to detect and deal with. Table 2.2 shows the mathematical models for single-tone and multi-tone AM and FM jammers. The mathematical models are given in Equation (2.3), Equation (2.4), Equation (2.5) and Equation (2.6) for single AM-tone, multi-tone AM, single-FM tone and multi-tone FM, respectively. The mathematical models show that Class I consists of $k = 1, \ldots, K$ of single tones characterized by P_{J_k}, f_{J_k} and θ_{J_k}, which are the power at the antenna, and the corresponding frequency and phase of the k-th jammer component, respectively. FM models in Equation (2.5) and Equation (2.6) incorporates β_k into the signal model, which is the modulation index of the k-th tone.
2. **Class II, Single saw-tooth chirp jammers**: This category comprises the signals whose frequency is modulated linearly over time (linear FM signals). Saw-tooth chirp signals are also known as saw-tooth chirps, swept CW signals, or simply single chirps for the sake of brevity. This type of jammer is similar to the signals used in most radar systems, but with a different carrier frequency. The mathematical model for single chirp jammers is given in Equation (2.7) in Table 2.2. The main parameters are the jamming power P_J, the starting frequency of the sweep f_J (at time $T_{\text{sweep}} = 0$), the minimum and maximum frequency of the frequency sweep $f_{\min}$ and $f_{\max}$ and the sweep period T_{sweep}, which is the time it takes the jammer to sweep from $f_{\min}$ to $f_{\max}$. The variable $b = \pm 1$ is a flag determining if we have an up-chirp ($b = 1$) or a down-chirp ($b = -1$), θ_J denotes the initial phase of the jammer and $f_q(t) = 2\pi f_J t + \pi b \frac{(f_{\max} - f_{\min})}{T_{\text{sweep}}} t^2$ is the instantaneous frequency of the jamming signal.
3. **Class III, Multi saw-tooth chirp jammer**: It is composed of multi saw-tooth chirps, representing the weighted sum of two or more single-chirp jammers,

transmitted at the same time. These signals are modeled in Equation (2.8) in Table 2.2. The main parameters are: b_k, a flag (±1) indicating an up or down chirp; f_{J_k} the frequency of the k-th chirp and θ_{J_k}, the initial phase of k-th chirp.

4. **Class IV, Chirp signals with frequency bursts**: This class comprises chirp signals with frequency bursts. Typically the frequency bursts are used to expand the frequency band affected by the jammer. These jamming signals are also frequency modulated signals, like the ones in class II and class III, but the modulating signal takes more complex functions. The signals of class IV are described by Equation (2.9). The main parameter for a class IV jammer type is the instantaneous frequency of the jamming signal $f_q(t)$, which typically has a periodic pattern.

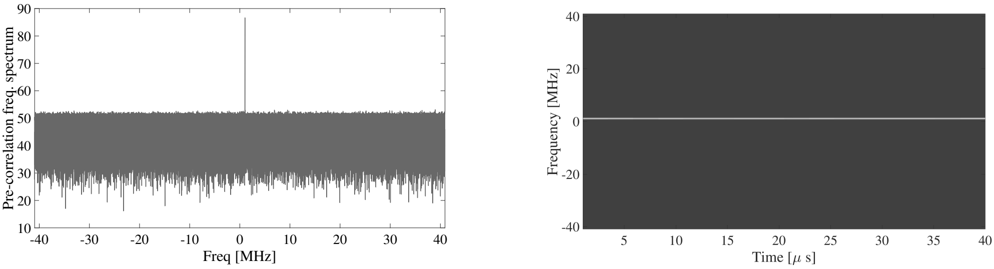
5. **Class V, Other jammer types**: This last class contains the jammer types not fitting in any of the above-mentioned categories, such as jamming signals that are active only during specific and repetitive periods of time (pulse-like jammers) with an active period of a pulse called duty cycle, or narrowband noise jammers, which just transmits random noise. The mathematical models are given in Equation (2.10) and Equation (2.11), for pulsed and narrowband noise jammers, respectively. The main parameters for the pulsed jammer model shown in Equation (2.10) are τ and f_r, which are the duty cycle and pulse repetition frequency, respectively. As for the narrowband noise jammer, $n(\zeta)$ represents a stationary random process with zero mean and σ_ζ^2 variance.

In Figure 2.7, we depict the PSD and spectrogram for a Galileo E1 signal mixed-up with three different jamming types, namely AM, chirp and pulsed jammer. In this example, the C/N_0 is set to 50 dB-Hz, and JSR is set to 40 dB. Figure 2.7a shows an example of PSD and corresponding spectrogram of a single AM-tone jamming signal at $f_{J_k} = 1.023$ MHz. Figure 2.7b shows the PSD and spectrogram of an up-chirp jammer with 0.6 MHz sweep range and $T_{\text{sweep}} = 8.64\ ms$ sweep period. Finally, in Figure 2.7c, we depict a pulse tone jammer with a duty cycle τ and pulse repetition frequency f_r set to 4.5μs and 12μs, respectively.

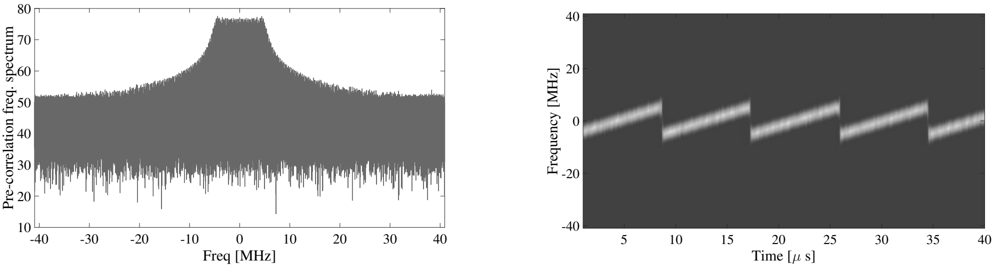
Comparing both Figure 2.4 and Figure 2.7, we can observe as the PSD in the examples shown in Figure 2.7 is not flat anymore due to the presence of a jammer.

Table 2.2 Jamming signal models. The subscripts in the case of single-component signals are dropped for clarity.

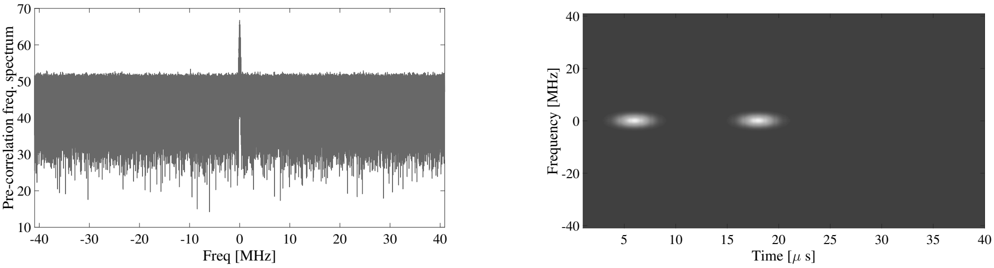
Jammer class	Jammer Type	Jammer baseband model		Parameters
Class I	Single AM Tone	$j(t)=\sqrt{P_J}\cdot\exp(j(2\pi f_J t+\theta_J))$	(2.3)	f_J, P_J, θ_J
	Multi AM Tone	$j(t)=\sum_{k=1}^{K}\sqrt{P_{J_k}}\exp(j(2\pi f_{J_k}t+\theta_{J_k}))$	(2.4)	$f_{J_k}, P_{J_k}, \theta_{J_k}$, and K, with $k=1,2,\ldots,K$
	Single FM tone	$j(t)=\sqrt{P_J}\cdot\exp(j(2\pi f_J t+\beta\cdot\sin(2\pi f_J t)))$	(2.5)	f_J, P_J, β
	Multi FM Tone	$j(t)=\sum_{k=1}^{K}\sqrt{P_{J_k}}\exp(j(2\pi f_{J_k}t+\beta_k\cdot\sin(2\pi f_{J_k}t)))$	(2.6)	$f_{J_k}, P_{J_k}, \beta_k$, and K, with $k=1,2,\ldots,K$
Class II	Single Chirp	$\begin{aligned} j(t) &= \sqrt{P_J}\cdot\exp(j(2\pi f_J t+\pi b\tfrac{(f_{\max}-f_{\min})}{T_{\text{sweep}}}t^2+\theta_J)) \\ &= \sqrt{P_J}\cdot\exp(j(f_q(t)t+\theta_J)) \end{aligned}$	(2.7)	$f_J, P_J, b, T_{\text{sweep}}, f_{\min}, f_{\max}$
Class III	Multi-Chirp	$j(t)=\sum_{k=1}^{K}\sqrt{P_{J_k}}\exp(j(2\pi f_{J_k}t+\pi b_k\frac{(f_{\max_k}-f_{\min_k})}{T_{\text{sweep}_k}}t^2+\theta_{J_k}))$	(2.8)	$f_{J_k}, P_{J_k}, b_k, T_{\text{sweep}_k}, f_{\min_k}, f_{\max_k}$, and K, with $k=1,2,\ldots,K$
Class IV	Chirp Signals with Frequency Bursts	$j(t)=\sqrt{P_J}\exp(j(f_q(t)t+\theta_J))$	(2.9)	Shape and parameters of $f_q(t), P_J, \theta_J$
Class V	Pulse Jammer	$j(t)=\sqrt{P_J}p_\tau(t)\otimes\sum_{k=1}^{K}\delta\left(t-\frac{k}{f_{r_k}}\right)\cdot\exp(j2\pi f_{J_k}t)$	(2.10)	τ, P_J, f_J, f_r, K
	Narrowba Jammer	$j(t)=\sqrt{P_J}\cos\left(2\pi f_J t+\beta\int_0^t n(\zeta)d\zeta+\theta_J\right)$	(2.11)	$P_J, f_J, \beta, \theta_J$ shape and statistics of $n(\cdot)$



(a) Single AM jammer spectrum **(b)** Single AM jammer spectrogram



(c) Single Chirp jammer spectrum **(d)** Single Chirp jammer spectrogram



(e) Pulsed jammer spectrum **(f)** Pulsed jammer spectrogram

Figure 2.7 Examples of Power Spectral Density (PSD) and spectrogram for a Galileo E1 signal (with C/N_0 set to 50 dB-Hz) in combination with various types of jammer.

2.4 Spoofing Principles

Spoofing carries out a different approach to interfere with GNSS service. In spoofing, forged/repeated GNSS signals are transmitted instead of generic modulated signals. By broadcasting false GNSS signals, a malicious user can attain two objectives: simply blocking the true GNSS signals, or also forcing the user receiver to misinterpret these transmissions as authentic signals. If the user receiver is fooled with fake signals, the obtained PVT solution might not be the real one, but the chosen one by the attacker. We can classify spoofer attacks according to the degree of complexity as [4, 97]:

a) **Simplistic spoofing attacks**: The simplest spoofing attacks can be performed by just a GNSS signal generator connected to a transmitting antenna [4]. The receiver could be fooled by just jamming the current GNSS signal reception and forced to reacquire the satellites by the fake signal, which typically has higher power. Such spoofing attacks may be quite expensive, due to the fact that it requires specific hardware (e.g., a GNSS signal generator, transmitter antenna, energy source), which can be expensive (e.g., up to hundreds of thousands of dollars) and it is not easily portable. Such attacks can be easily detected since generally they do not synchronize the spoofing signals with the current signals from the GNSS satellites in view. Therefore pseudoranges, C/N_0 and Doppler jumps can occur, and inconsistencies can be found in the signal.

b) **Intermediate spoofing attacks**: The attacks in this category combine a GNSS receiver with a digital processor and a transmitting RF front-end [4]. The spoofer is able to synchronize the frequency and align the code phase between the real and the counterfeit signals. When the signals from the satellites are tracked by the attacker receiver, it has a perfect knowledge of both the Doppler shift and the code delay of the true satellite. In principle, any GNSS receiver, properly modified, can be converted into a spoofer device. This type of spoofer is also able to adjust the signal power strength of the counterfeit signals, in order to simulate signal levels compatible with satellite transmissions. The user receiver is not able to distinguish the counterfeit signal from the genuine one, since the spoofer accurately reproduces the code phase, frequency, and navigation data bits. The navigation bit reproduction requires a procedure of bit prediction and estimation to perform the attack in real-time (since to receive a whole bit from the real satellites is required a certain amount of time). Nowadays, intermediate spoofing attacks can be performed with software and RF components easily available on the market and on the internet for a limited cost; nonetheless, a deep knowledge of GNSS signal processing is required to correctly set up the signal processing chain.

c) **Sophisticated spoofing attacks**: Sophisticated spoofing attacks consist of a coordinated and synchronized attack carried out by different spoofing devices [97]. These attacks are the most complex to implement and deploy, and the most expensive and difficult to perform and coordinate. But they are also the hardest to respond to. In these attacks, the spoofing devices act as a beamforming antenna array, simulating the different Angle of Arrival (AoA)s for different satellites. This can be accomplished either by keeping each spoofer fixed and transmitting the signals of all satellites with appropriately calculated delays compatible with the receiving antenna or by having each spoofer transmit the signal of exactly one satellite and mechanically moving the spoofer around the target receiver. Implementing sophisticated attacks based on multiple intermediate spoofers is possible, but very hard to implement. The likelihood of such an attack is particularly low, because of the technical complexity required by the implementation and the logistic problems implied by the simultaneous operation of multiple spoofing devices, especially in dynamic scenarios.

d) **Meaconing attacks**: Meaconing are a particular case of spoofing. These attacks consist of the interception and re-broadcast of true GNSS signals (by just recording and playback the real signal) with enough gain to overwhelm the true signal at the target antenna [4]. These attacks do not modify the transmitted signals, so the target receiver's PVT solution becomes the PVT solution of the attacker, with a rebroadcasting delay. Through a meaconing attack, even an encrypted GNSS signal (e.g., military GPS L2 or Galileo E6) can be affected, since by means of these attacks the authentic signals are only rebroadcast. These attacks are generally easy to implement since it only requires a few RF components to capture and re-transmit back the signal.

Table 2.3 summarizes the mathematical models of the generated signals for various types of spoofers discussed above. The provided equations refer to the signal model for one forged satellite at a time; to be effective, spoofers simultaneously produce many of these signals, one for each satellite to be mimicked. Equation (2.12) shows the signal model for a simplistic spoofer attack, where P_s is the spoofer power, mimicking the power of the authentic satellite signal; n is the index of the current data bit; d_n are the data bits generated by the spoofer; in the simplistic attack these bits are different from the true b_n data bits sent by the satellites in the sky; $c_n(t)$ is the pseudo-random code that modulates the n-th data bit, possibly including alternative modulation types such as BOC modulation, corresponding to an authentic satellite code; notice that the summation over n cover non-overlapping wave forms in time; $\tau_{\mathrm{sp},n}$ is the time delay introduced by the spoofer; it may vary with the time, although for simplicity of notation, the dependence on the time t is removed here; Δf_{sp} is the frequency shift introduced by the spoofer in the simplistic and intermediate attacks; as for τ_{sp}, it may be a function of the time; finally Ψ is the carrier phase offset for the selected satellite to be forged. Equation (2.13) shows the model for an intermediate spoofer attack where $\hat{b}_n$ is the estimated data bit (at the spoofer end) of the n-th transmitted bit of the selected satellite to forge, $\hat{\tau}$ is the spoofer estimated true code delay, $\hat{f}_D$ is the spoofer estimated true Doppler frequency shift and $\hat{\Psi}$ is the estimated carrier phase at the spoofer's end. Equation (2.14) shows the model for sophisticated spoofer attacks executed with K coordinated and synchronized transmitters, where the superscript (k) indicates the values measured or estimated by the k-th spoofer. Such quantities are the same found in Equation (2.13)), apart from the additional phase term $\Phi^{(k)}$ used to adjust the relative geometrical term among the different transmitters. Finally, in Equation (2.15) a meaconer is modeled as a simplified version of an intermediate attack when the exact signal received from a satellite is delayed with an unknown delay τ_{sp} and amplified with the spoofer amplitude $\sqrt{P_s}$.

2.5 Other Wireless Channel Impairments

Besides the intentional interference summarized above, the largest and the most difficult to deal with the source of interference are those coming from the channel. Following, we list the main sources of interference:

a) **Atmospheric effects**: The largest errors in the PVT solution are attributable to the atmosphere. Through both refraction and diffraction, the atmosphere alters the apparent speed and direction of the signal, causing an apparent extra delay [70]. The effects due to the atmosphere are typically divided into: i) Ionospheric effects and ii) Tropospheric effects.

   The ionosphere is comprised between 70 km and 1000 km above the Earth's surface. The ultraviolet rays from the sun ionize gas molecules in that region, releasing free electrons. These free electrons impact the behavior of electromagnetic wave propagation, especially when these electrons are present at high densities. The ionospheric delay is frequency-dependent, which means that it can be estimated and eliminated by carrying out measurements with a dual-frequency receiver [70]. If a dual-frequency receiver is not available, models of

Table 2.3 Spoofing baseband signal models.

Spoofer class	Baseband signal model (per satellite)	Parameters
Simplistic Spoofer	$s(t) = \sqrt{P_s} \sum_n d_n c_n (t - \tau_{\mathrm{sp}}) \exp(j 2\pi \Delta f_{\mathrm{sp}} t + \Psi)$ (2.12)	$P_s, d_n, \tau_{\mathrm{sp}}, \Delta f_{\mathrm{sp}}$
Intermediate Spoofer	$s(t) = \sqrt{P_s} \sum_n \hat{b}_n c_n \left(t - \hat{\tau} - \tau_{\mathrm{sp}}\right) \exp(j 2\pi \left(\hat{f}_D + \Delta f_{\mathrm{sp}}\right) t + \hat{\Psi})$ (2.13)	$P_s, \tau_{\mathrm{sp}}, \Delta f_{\mathrm{sp}}$
Sophisticated Spoofer	$s(t) = \sum_{k=1}^{K} \sqrt{P_s^{(k)}} \sum_n \hat{b}_n c_n \left(t - \hat{\tau} - \tau_{\mathrm{sp}}^{(k)}\right) \exp(j 2\pi \left(\hat{f}_D^{(k)} + \Delta f_{\mathrm{sp}}^{(k)}\right) t + \hat{\Psi}^{(k)} + \Phi^{(k)})$ (2.14)	$K, P_s^{(k)}, \tau_{\mathrm{sp}}^{(k)}, \Delta f_{\mathrm{sp}}^{(k)}, \Phi^{(k)}$
Meaconer	$s(t) = \sqrt{P_s} \sum_n b_n c_n \left(t - \tau - \tau_{\mathrm{sp}}\right) \exp(j 2\pi f_D \left(t - \tau - \tau_{\mathrm{sp}}\right) + \Psi)$ (2.15)	P_s, τ_{sp}

the ionosphere are employed to correct the ionospheric delay [70]. The troposphere is the layer of the atmosphere closer to the Earth's surface, comprising about 18 km altitude from the Earth's surface. The effect of the troposphere on the GNSS signals influences an extra delay in the measurement of the signal traveling time from the satellite to the receiver. This delay depends on many factors, such as the temperature, pressure, and humidity, as well as the transmitter and receiver antenna's location. To ease these effects, tropospheric models are also available in the literature.

b) **Atmospheric Scintillation**: It is an atmospheric phenomenon due to high levels of solar and geomagnetic activities and particles, which provokes a quick variation in the amplitude and/or phase of the GNSS signals [98]. Receivers are not usually designed to accommodate these sudden and fast changes in the received signal. In consequence, the receiver may lose the lock condition with the GNSS signal, which is needed for the regular functioning of most GNSS receivers.

c) **Multipath**: The cause of multipath is the reflection or diffraction of the transmitted signals in the environment (e.g., buildings, cars, water bodies, people moving, the ground, etc.), which enters the receiver RF front-end and are mixed with the direct signal [70]. These reflected copies are delayed with respect to the original source due to the higher travel paths. The effects of the multipath components superposition are noticeable (especially for the components generated nearby the receiver, with a smaller delay) in the correlation property, which is no longer able to distinguish as accurately among self-correlation and cross-correlation of the different PRN codes used by the satellites. In addition, this multi-component signal produces large positioning errors in the PNT solution.

d) **Absence of LoS**: Obstructions due to structures, obstacles, and foliage may occur, provoking partial or even total absence of LoS condition from the user receiver location. This lack of LoS can be treated as an additional attenuation, typically suffered by the direct path, and commonly known as shadowing [70]. Due to this phenomenon, multipath components might arrive with higher power than the direct path, since due to the different paths of propagation might not be affected.

e) **Doppler impairments**: Doppler shift is due to the relative motion between the satellites and receiver. Each satellite will have its Doppler shift, is also affected by the propagation channel, and produces modifications on the direct Doppler transmission.

2.6 Summary of Contributions

In the chapter, the author of this thesis has mainly contributed to:

- Presenting the state-of-the-art of the currently operative GNSS constellations, including a brief description about the currently deployed GNSS constellations, system architecture, frequencies of operation, signals transmitted by the satellites, GNSS receiver description, etc.
- Identifying the future navigation satellite-based positioning systems trends, es-

pecially in the scope of interference resilience and challenging environments.

- Providing a state-of-the-art and literature review about RF interference types and impairments, comprising naturally caused (e.g, due to channel, atmosphere, etc) and with artificial origin (e.g., jamming, spoofing, etc).
- Offering mathematical models for different jamming and spoofing types, and classifying them according to the signal type and difficulty to be detected and its degree of complexity, respectively.

Chapter 3

Interference Management Solutions in GNSS

In this chapter, we describe specific interference management solutions, namely detection, classification, localization and/or mitigation techniques, against the attacks described in Chapter 2 (Section 2.3). These attacks consisted of jammer signals transmitted with higher power with respect to the received GNSS power. We face the interference solutions from two ends: i) purely detection mechanisms, and ii) classification and detection algorithms. With the detection algorithms, we can determine if an attack exists or not. Whereas with classification algorithms, we can in addition determine the presence of an attack, and which type of signal is producing the interference. We first start by giving some basics about detection theory. Basically, we describe the classical binary detection problem, where two hypotheses are considered. In our case, one hypothesis is for the jammer-free scenario, and the other hypothesis is for the jammer-present scenario. After this brief description of detection theory, we list the main stages in a typical GNSS receiver chain where the interference management algorithms can be implemented. In addition, we provide specific detection algorithms, with explanations about their functioning, mathematical models, and some illustrative examples. Next, we describe the methodology we used for the classification studies of jamming signals. We mainly used spectrogram images containing different jammer scenarios, which were used for training machine learning algorithms. A different set of images were used for training and testing the machine learning algorithms. The results for both detection and classification analysis are finally found in Section 3.4. The classification algorithms were tested with MATLAB simulated data (both GNSS and jammers), while detection algorithms were tested with MATLAB simulated data and in-lab GNSS data, recorded in the laboratory.

3.1 Problem Statement

Due to the latest advances in GNSS technology and RF hardware and software, new challenges dealing with interference over wireless channels have arisen. In particular, in the aviation industry, this fact is becoming a real and likely threat nowadays. The aviation domain is typically divided into two main categories: manned and unmanned aircraft. Manned aircraft comprises those vehicles which require the presence of a human on board, while unmanned aircraft refers to when no human is needed on board. In this case, the aircraft is wireless and remotely controlled. The service provided by the GNSS systems is a key element for both manned and unmanned flying aircraft. The PNT solution allows to continuously locate and track the aircraft from both ground and onboard. This continuous access to the aircraft's exact location is needed not only to allow the safe routing of lots of aircraft worldwide, but also to avoid collisions, facilitate emergency aids, and support future services such as aerial taxis and ad-hoc aerial networks [99]. The motivation for focusing on aviation use cases has been two folds: first, it was motivated by project needs within the team (e.g., the work in EU-funded GATEMAN project [35]) and secondly, because of the current fast-paced developments in unmanned aerial vehicles (UAV) domain, it is expected that interference management in GNSS will be a crucial aspect on-board of any aircraft in the future which will contribute to increased safety and security.

The crucial element of PNT solution in the aviation domain, in combination with the low, received power of GNSS signals, makes the RF interferences a real and critical threat, as we have seen in Chapter 1 with real-case examples. For this reason, in this chapter, we analyze specific detection and classification techniques to provide awareness of an attack on the service provided by GNSS. With the focus in mind that after determining the presence of an attack, we need as well to consider alternative positioning methods besides the current MEO GNSS in case we cannot mitigate those interferences. We provide simulation-based results to support the awareness of an attack and the possible consequences.

Some organizations such as ICAO, RTCA, EUROCONTROL, and EUROCAE, among others, try to characterize, classify and standardize methodologies dealing with RF interferences in new generation standards. These entities provide reports in which different interferences are characterized and reported [100, 101].

3.2 Interference Detection Mechanisms

3.2.1 Basics of Detection

The detection of a single type of interferer at a time can be formulated as the deeply studied classical binary detection problem [102], in which a received signal might be (or might not) influenced by an interference signal. These two conditions are considered two different hypotheses. The hypothesis *H0* reflects the interference-free scenario and the hypothesis *H1* stands for the case when the jammer is present [25]. In order to find a decision condition to distinguish between *H0* and *H1* hypothesis, one can rely on the PDF under *H1* and *H0* (in case it is known) of a measurable test statistic. An illustration of the PDF under *H0* and *H1* test statistic is shown in Figure 3.1. In Figure 3.1 both PDF correspond to a Gaussian distribution. The PDF for *H0* is Gaussian, as we have seen in the previous chapter (Section 2.1.2). GNSS signal is mainly noise-like, since it is a superposition of independent (and weak) CDMA signals (i.e., the GNSS signal) and an AWGN noise (more details are given in Section 2.1.2 and Figure 2.4 for more details). But the PDF for *H1* may not fit a Gaussian distribution, and it is dependent on the interference type [25] is present. Given that the jammer signal is typically unknown, the power of the received signal is often used as a test statistic. For *H1*, the power of the interference is usually considered as much stronger than the signal under *H0*. For this reason, the corresponding PDF of the received samples is mostly influenced by the jammer contribution. An appropriate threshold can separate between the two hypotheses, *H0* and *H1*, such that the P_d is maximized and the P_fa is minimized, as it is shown in Figure 3.1. The probability of detection P_d and the probability of false alarm P_fa are described mathematically as

$$\begin{aligned} P_{\mathrm{d}} &= \mathbb{P}(\Gamma > \gamma | H_1) \\ P_{\mathrm{fa}} &= \mathbb{P}(\Gamma > \gamma | H_0) \end{aligned}, \tag{3.1}$$

where $\mathbb{P}(\cdot)$ stands for the probability function, Γ stands for the test statistic, and γ represents a fixed or adaptive threshold. The choice of the test statistic is challenging, and it limits the direct applicability of this hypothesis testing in interference detection. In case the PDFs is known under both H_0 and H_1, the Generalized Likelihood Ratio Test (GLRT), can be applied, as shown in Equation (3.2)

$$\Gamma = \frac{\max\limits_{\theta_1} \mathbb{P}(r|H_1, \theta_1)}{\max\limits_{\theta_0} \mathbb{P}(r|H_0, \theta_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma, \tag{3.2}$$

where r represents the received signal, $\mathbb{P}(r|H_0, \theta_0)$ and $\mathbb{P}(r|H_1, \theta_1)$ is the conditional PDFs under H_0 and H_1 hypotheses, respectively. The θ_0 and θ_1 are the unknown parameters by the interferer. The GLRT approach is not usually applied in realistic scenarios because the jammer PDF is not usually known. Instead of applying the classical detection techniques described above, the GNSS interference detection algorithms rely on different assumptions about the interference and channel type. The next subsection discusses some interference detection algorithms encountered in GNSS literature, that are applicable to the aviation domain.

Figure 3.1 shows an example of test statistic comparison for θ_0 and θ_1. We observe as θ_1 test statistic mean value is slightly higher than θ_0, and by selecting a proper threshold (yellow vertical line) we can determine if we are under hypothesis θ_0 or hypothesis θ_1, with a certain error (P_{fa}).

3.2.2 Detection Algorithms

The detection techniques, as well as classification techniques, can be applied at different stages of the GNSS receiver chain [25], as it is depicted in Figure 2.3. We can classify them as [25]:

a) **Front-end Techniques**: These techniques typically work independently on the interference type. They are applied in the first block of the GNSS receiver chain, as it is shown in Figure 2.3. The raw analog signal received by the antennas (before ADC) is typically used.

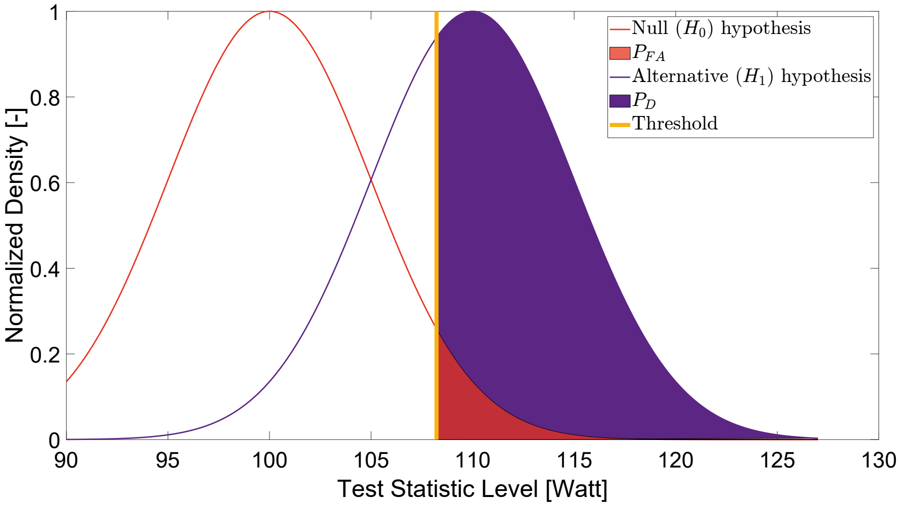


Figure 3.1 Illustration showing the PDF under *H0* (red) and *H1* (purple) conditions, with an example of a detection threshold (yellow). The probabilities of False Alarm (red area) and Detection (purple area) are also depicted. The threshold is represented by the vertical yellow line.

b) **Pre-Correlation Techniques**: Most of the interference detection algorithms are applied at the pre-correlation stage. This is the second stage in a typical GNSS receiver chain as we can see from Figure 2.3. These techniques typically operate on the I/Q samples of the signal r(n) after the ADC block. Before the signal acquisition processing stage.

c) **Post-Correlation Techniques**: Detection techniques at the post-correlation level use the signal r(n) after the correlation with the PRN code of a certain satellite signal. Thus, they focus on a single satellite-receiver link at a time. These techniques are typically implemented in the tracking block, as they typically use the information produced by the tracking correlators. Post-correlation level techniques are widely preferred and most powerful for spoofing monitoring rather than interference detection.

d) **Navigation Techniques**: Navigation techniques are performed during the last stage of a typical GNSS receiver, as we can see from Figure 2.3. These techniques use the signal received from all the satellites in view at the pseudorange domain, which means after the tracking module (check Figure 2.3). These techniques typically incorporate additional data to monitor the GNSS receiver status. They effectively disclose anomalies of the receiver observables, through cross-checks with other PRNs, data from other frequency bands, different receivers, or additional sensors. For these reasons, they are typically used for spoofing monitoring instead of jamming detection.

Figure 3.2 lists some of the analyzed detection and classification techniques according to the receiver stage at which are performed. As front-end techniques, we can find Automatic Gain Control (AGC) (as representative of detectors) and Support Vector Machine (SVM) and Convolutional Neural Network (CNN) techniques (as representative of detection plus classification techniques). As for pre-correlation techniques, we can find a broader list of alternatives: Probability Density Function (PDF) (analyzing the PDF distribution of the received samples), Time Power Detector (TPD), Frequency Power Detector (FPD), Welch, kurtosis analysis, Adaptive Notch filter, multi-antenna array analysis, Hough-Radon transform analysis and Singular Value Decomposition (SVD) analysis (which compares the SVD of a known interference-free signal with the currently received). For its part, in the post-correlation techniques, we can find: Power Distortion Monitoring (PDM) (monitoring both the power and the correlation function to detect sudden changes), multi-correlator banks (analyzing the signal and observables during the tracking stage), Multi-Correlator output with Auto Regressive modelling (MCAR), C/N_0 and absolute power monitoring (which monitors the received C/N_0 and/or received power), and Signal Quality Monitoring (SQM). Finally, in the navigation block, we included the following techniques: Correlation of measured observables with propagation models, consistency check with Alternative Positioning, Navigation, and Timing (APNT), Angle of Arrival (AoA) discrimination (for example by not-processing the signals coming from a specific direction), Sum-of-Squares (SoS) (exploiting the fact that phase difference measurements of signals coming from the same direction share a common geometrical term), polarization discrimination, and crowd-sourcing correlation.

Next, we describe in more detail some of the techniques listed in Figure 3.2. We focus on those techniques which were finally selected for further analysis, which appear in a bold letter in Figure 3.2. We selected for further investigations a subset of the initial set of techniques after an initial pre-selection based on their characteristics, suitability to aviation use cases, and complexity. These final selected techniques are: Automatic Gain Control (AGC), Time Power Detector (TPD), Frequency Power Detector (FPD), Welch, kurtosis and Notch filter:

a) **Automatic Gain Control (AGC) monitoring Technique** [72, 103, 104]: The

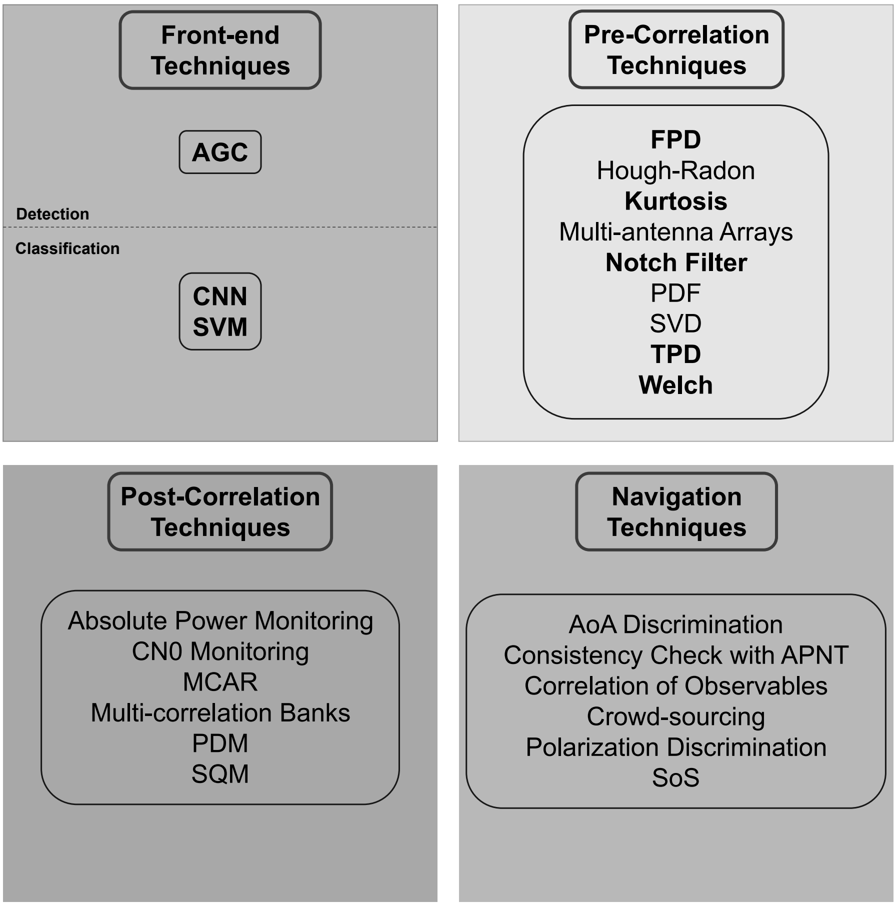


Figure 3.2 Detection and classification techniques grouped according to GNSS receiver chain application. [[25]]

AGC is a circuit present in most of the GNSS receivers in the front-end block (see Figure 2.3). This circuit maintains the control of the received signal power in order to provide an appropriate power level to the next elements in the receiver chain such as the quantizer, in order to minimize the quantization loss [72, 103]. The AGC typically operates at the ambient noise levels, since the GNSS signal power is usually really low. In the presence of high interference, the AGC decreases its gain to keep the AGC output signal level stable enough and avoid large fluctuations in the signal power. These variations on the AGC gain level can be used to detect the presence of a jammer. An AGC interference detector uses the AGC gain over N consecutive samples and compares it with a predefined threshold corresponding to a known jammer-free scenario. If all the N samples are below the threshold, then the interference is declared present (received signal will have intrinsically more power due to the jammer presence, so the AGC gain will need to decrease its value to keep a constant power level). The baseline AGC level is manufacturer and antenna specific. This baseline level needs to be previously known to determine an adequate detection threshold. Figure 3.3 depicts an example of an AGC detector for a two-tone AM jamming signal and Galileo E1. Jammer JSR was set to 40 dB, and Galileo E1 signal C/N_0 was set to 50 dBHz. Figure 3.3 shows the situation when the jammer is disabled during the first 8 ms, enabled for the next 4 ms, and then switched off again. A clear drop in the AGC gain is observed when the jammer is on since less gain is required since the signal at the input is stronger.

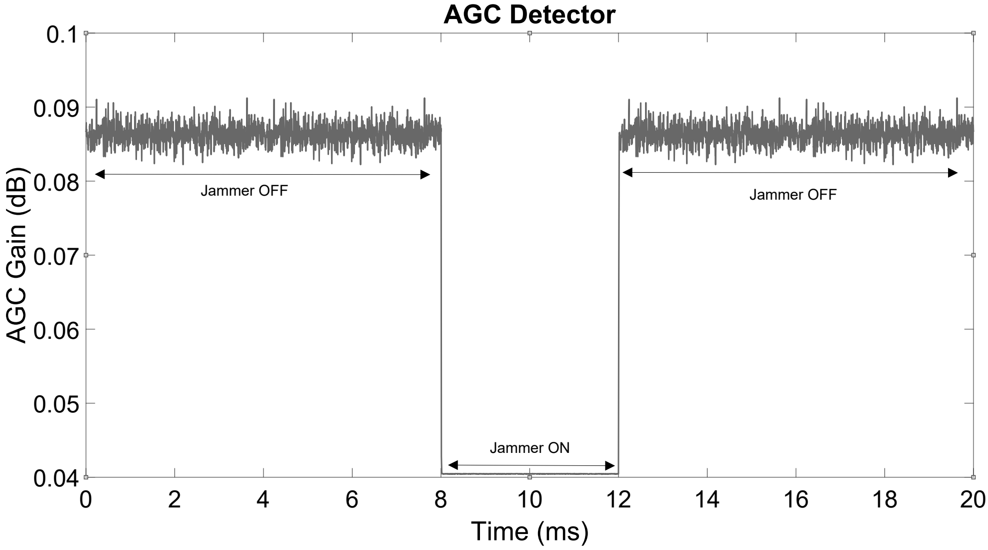


Figure 3.3 Illustration of test statistic of AGC detector for a double-tone AM jammer. JSR and C/N_0 are set to 40 dB and 50 dBHz, respectively.

b) **Time Power Detector (TPD) Technique** [102, 105, 106, 107, 108, 109, 110]: This technique is also known as Power Law Detector (PLD) [109] or simply energy detector [102, 110]. This method measures the energy of the received signal before correlation with the PRN code replica over a short time interval. Energy is defined as the power multiplied by time; for time-finite signals, we usually deal with energy measures, while for bandwidth-limited signals we talk about power. The TPD test statistic can be modeled as:

$$T_{\mathrm{TPD}} = \frac{1}{JN} \sum_{j=1}^{J} \sum_{n=1}^{N} |r(n+(j-1)N)|^{2\eta}, \tag{3.3}$$

where N is the number of samples of the considered short signal interval, J is the number of short intervals under the observations (thus the signal is observed in total over JN samples) and η is a positive number that determines the power-law, e.g., $\eta = 1$ for the square-law detector and $\eta = 0.5$ for the amplitude detector. The measured power is usually normalized by the number of samples N and by the noise variance. Then it is compared with a suitable threshold. If the test statistic exceeds this threshold ($T_{\mathrm{TPD}} > \gamma$) the interference is declared to be present. An example of TPD is depicted in Figure 3.4. It illustrates how the test statistic of TPD detector evolves with time while the jammer is absent and present. We observe as the signal power increases considerably after 7 ms, which corresponds to the time instant in which the jammer is turned on. When the jammer is activated, the estimated input power starts to increase, until it reaches a maximum. This maximum corresponds to the window of N samples including all samples with the jammer activated. At approximately 20 ms, the jammer is switched off, and then the detected power returns to the baseline level before the jammer was enabled.

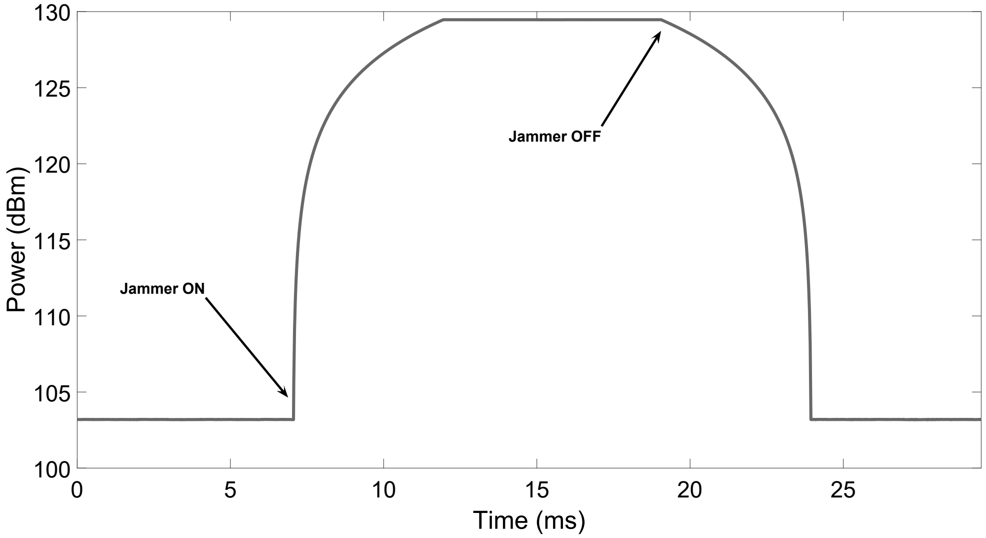
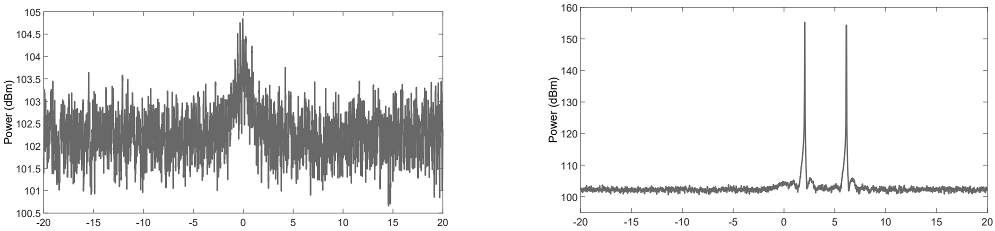


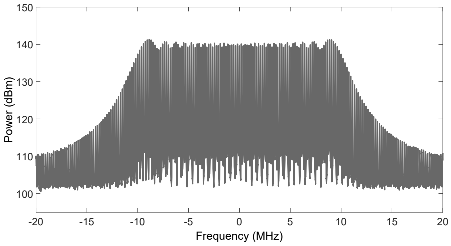
Figure 3.4 Illustration of TPD test statistic for double-tone AM jammer. JSR and C/N_0 are set to 40 dB and 50 dBHz, respectively. The window time used for the algorithm is set to 5 ms.

c) **Frequency Power Detector (FPD) Technique [102, 105]**: The FPD algorithm is analogous to the TPD detector described above, since, according to Parseval's theorem, the average power of a signal in time domain equals the average power in frequency domain. The periodogram is used to estimate the signal's spectral density required for this method. Similarly as in TPD, if the test statistic exceeds the set threshold, the interferer is declared as present, otherwise is determined as a jammer-free scenario. Figure 3.5 shows an example of FPD detector. Figure 3.5a shows the FPD's test statistic when the jammer is not present. In Figure 3.5b, the case of a double-tone AM jammer is depicted. The power of the AM tone jammer is set to approximately 50 dBm above the GNSS signal, composed by Galileo E1. Finally, Figure 3.5c shows a chirp jammer with a power of 35 dBm higher than the GNSS Galileo E1 signal, over the whole sweep range with a signal bandwidth of 20 MHz.



(a) No presence of jammer scenario

(b) Double-tone AM scenario



(c) Chirp jammer scenario

Figure 3.5 Test statistic example of FPD detector for jammer-free, double-tone AM, and chirp jammer. The time window used for the detection algorithm is set to 5 μs.

d) **Welch-based Technique [105, 111]**: Welch-based algorithm can be considered as an alternative to the FPD. This method can also be used to estimate the periodogram of the signal. The main difference with FPD technique, is that Welch's method divides the input signal into overlapping pieces of a specific length. Then it applies a window to these pieces and finally computes the periodogram; this results in averaged periodograms. The size of each window has to be sufficiently small such that the frequency content can be assumed to be constant for each piece. Once more, the test statistic obtained by applying Welch's method needs to be compared with a previously set threshold to determine the presence of a jammer.

e) **kurtosis Technique**: This method performs the kurtosis to the received signal. The kurtosis of a signal is defined as

$$\Gamma = \frac{\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^4}{\left(\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^2\right)^2}, \tag{3.4}$$

where $\mu_r = \frac{1}{N}\sum_{n=1}^{N} r(n)$ is the mean of the GNSS signal $r(n)$. Here $r(n)$ are the incoming pre-correlation samples at the GNSS receiver (second processing block in Figure 2.3). In the absence of jamming, the kurtosis is typically close to 3 (since $r(n)$ will follow a Gaussian distribution) [112]. In the presence of an active jammer, the kurtosis may deviate from the baseline value of 3. The deviation is positive (> 3) or negative (< 3) depending on the type of jamming present [105, 113] and how it affects statistically the signal. Figure 3.6 shows that as long as the jammer is off, the kurtosis is approximately 3. Otherwise, the value of the kurtosis drops significantly (e.g., it is divided by half in this example), manifesting the presence of a jammer.

f) **Adaptive Notch Filter (ANF) Technique [114, 115, 116, 117]**: Notch filters have been traditionally used for jamming mitigation, but they can also provide detection capabilities [115]. In [115] a design for an Infinite Impulse Response (IIR) notch filter is provided, whose z-transform is

$$H_n(z) = \frac{1 - z_0(n)z^{-1}}{1 - k_a z_0(n)z^{-1}} \tag{3.5}$$

and which is adapted using a stochastic gradient approach. The term $z_0(n)$ is the notch filter's time-varying zero, whose angle determines the center frequency of the notch, and k_a is the pole contraction factor (a user-defined parameter between 0 and 1). The zero $z_0(n)$ is adapted to be in accordance with the jammer instantaneous frequency in the complex plane. The notch filter

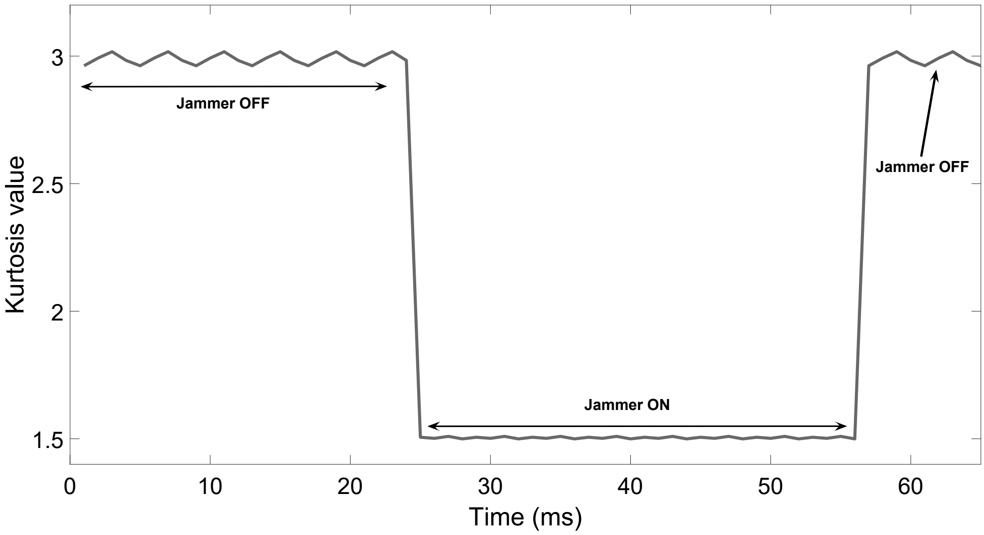


Figure 3.6 Test statistic example of a kurtosis detector for an AM jammer. JSR is set to 40 dB and C/N_0 for the Galileo E1 signal is set to 50 dBHz. The window time for the detector algorithm is set to 1 ms.

magnitude $|z_0(n)|$ is applied to the received signal before correlation can be used as a detection metric. Again, an appropriate threshold must be set to distinguish the interference-free case from the jammer present case.

Section 3.4 provides some results for the above-mentioned techniques against the jammer types described in Section 2.3.

3.3 Classification Mechanisms

Signal classification typically relies on machine learning algorithms. When machine learning is used, interference classification is typically performed as a two-step process [28]: first, we need to perform feature extraction, and then the actual signal classification. In addition, we usually need a pre-processing step of the signal, in order to represent the data in a uniform and usable way for the algorithms. In principle, any feature of a signal we can extract could be used for classification. Nevertheless, the more distinctive and representative the features are, the better is for the classifier, and it would be easier to discriminate among the different categories [28]. In this thesis, we propose and compare two classification methods using images from spectrograms, based on the fact that different jamming types affect in a different manner the GNSS signal. By using Support Vector Machines and Convolutional Neural Networks, we are able to categorize those jammers, as a previous step of jamming mitigation. With this approach, we are able to first detect if a jamming attack exists, which jammer signal is affecting our signal, and then apply the best performance mitigation technique for the specific jammer type. The first classification method makes use of SVM [118, 119] in combination with BoF [120], which extracts the image features from the images used for the SVM classifier. These image features are used as input data to the SVM classifier. The second studied classifier is the CNN, based on multi-layer neural networks [121]. Both classifiers SVM and CNN needs first to be trained, in order to learn the individual signal features for each category. We selected SVM and CNN algorithms after analyzing the capabilities and features of a larger set of machine learning techniques. Some other algorithms such as XGboost [122], Random Forest [123], Artificial Neural Network [124], K-nearest neighbor [125], and Decision tree [126] were also initially pre-selected. The main reason why XGboost was discarded, is because it does not perform so well on sparse and unstructured data and its scalability is low. Artificial Neural Network was discarded due to the complexity it can achieve to be implemented. The number of trainable parameters increases drastically with an increase in the size of the image. In addition, Artificial Neural Networks lose the spatial features of an image, which is crucial for determining the jamming type and jamming signal parameters from the image. Random forest lacks the flexibility for feature processing and modeling that for example CNN has. It also requires much computational power and requires much time for training compared with CNN and SVM. The main drawback of K-nearest neighbor is that this algorithm typically does not work well with very large data sets and it's pretty sensible to noise. Finally, the Decision tree was discarded due to its sensibility to noise and it can become very complex and requires a large number of computing operations. For these reasons, only SVM and CNN were consider for further analysis.

The steps for jamming classification after training the algorithms are depicted in Figure 3.7. The proposed work-flow consists in: i) receiving the GNSS (with jamming mixed if any) raw signal; ii) generating the spectrogram of the received raw signal; iii) plotting and saving the image from the generated spectrogram; IV) choosing among the two main classification algorithms; V) performing the jammer classification. Additional variations of this workflow can be performed. For example, instead of reproducing images of the spectrogram, we can save the full spectrogram data and carry out similar classification algorithms. More details regarding the image generation characteristics (e.g., bit color, resolution, etc) are given in subsection 3.3.1.

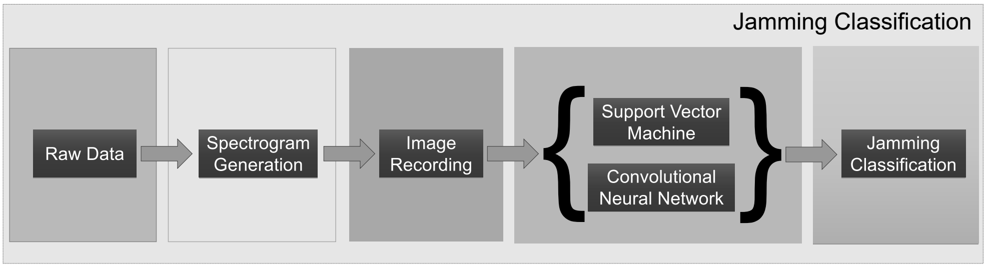


Figure 3.7 Block diagram of the proposed methodology for jamming classification.

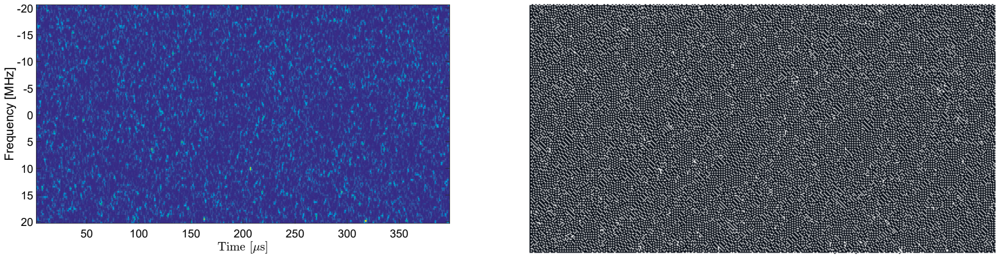
3.3.1 Spectrogram Images Generation

In order to train and further test the algorithms, we created a database of images comprising different scenarios, containing jamming-free and different types of jammers. For the jamming free, we only considered GPS L1 signal. On the contrary, for the jamming case, we considered a combination of GPS L1 signal with the specific type of jammer signal. To understand the performance bounds, we consider only a single type of jammer at a time in each simulated scenario. Although using different parameters (including jammer power and noise) in order to cover as much as possible different jammer configurations. As some of the jammer types are non-stationary (e.g., chirp jammers), the best time-frequency modeling is a short-time short-frequency transform such as the spectrogram [28, 127]. In order to compute the spectrogram, we generate first a short signal of 1 ms, containing a specific single jamming type combined with GPS L1 signal, or just GPS L1 signal. To this generated signal, we apply the short-time short-frequency spectrogram transform, setting the window length to 128 samples, the samples overlap to 120 samples, and a Fast Fourier Transform (FFT) size of 128 samples [28]. We selected these parameters based on a trade-off between achieving a good spectrogram resolution for all the considered jammer types and maintaining a low complexity in order to be efficient in the process. The generated spectrogram images are then converted to black-and-white (binary, setting the values of the image to '1' if the luminescence level of a specific pixel is greater than a pre-defined threshold, otherwise set to '0'), in order to reduce the number of (irrelevant) features, re-scaled to a resolution of 515 x 512 pixels and 600 Dots-Per-Inch (DPI), and they are finally saved. The reason for converting the color spectrogram images to black-and-white was motivated by our empirical studies, as well as by the intuition that SVM classifiers are known to work better with binary images than with multi-level images. In Figure 3.8 we depicted some examples of spectrogram images. In the left part, we provide the spectrogram image for the non-active jammer, AM jammer, and Chirp jammer, respectively from top to bottom. On the right side, we provide for comparison of the binary images for the same scenarios. For obtaining the plots in Figure 3.8, we set the C/N_0 and JSR to 45 dBHz and 50 dB, respectively. In the absence of jamming, in Figure 3.8a and Figure 3.8b, we observe a spectrogram composed basically of noise, since there is no other contribution more than the GNSS signal itself, which as we have seen, is a low-power CDMA signal, and thus noise-like. On the contrary, for the rest of scenarios Figure 3.8c – Figure 3.8f certain jammer contribution can be noticed. For example, in Figure 3.8c and Figure 3.8d, we clearly notice a horizontal straight line at a specific frequency, which correspond to the frequency of the AM tone. In Figure 3.8e and Figure 3.8f we observe the typical spectrogram of a saw-tooth signal, showing the sweep range and sweep periods of an up-chirp signal.

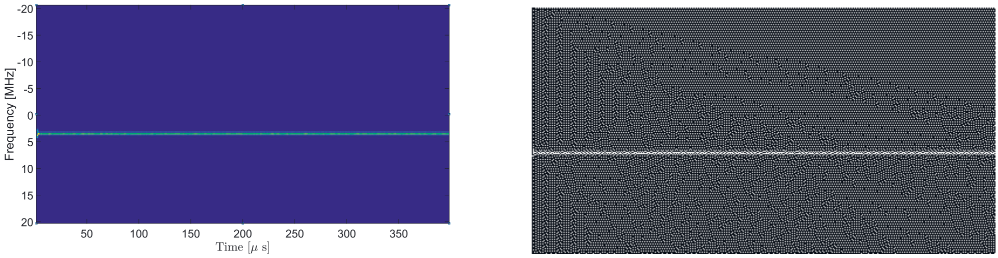
3.3.2 Support Vector Machine (SVM) Algorithm

3.3.2.1 Extracting Image Features: Bag of Features (BoF)

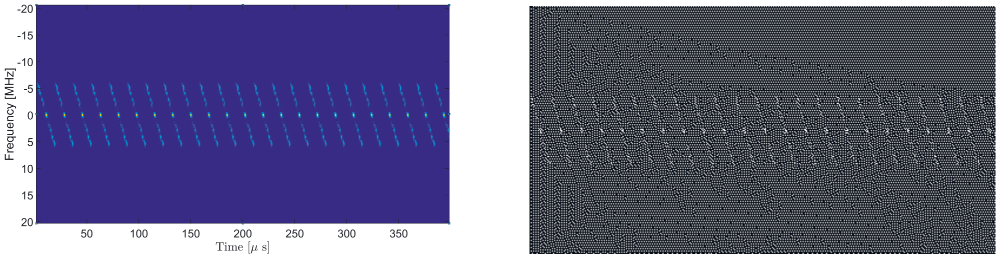
Before applying the SVM algorithm, we need a prior step for being able to classify the images according to different categories. This process consists of feature extraction from the input images described in the previous section. For this purpose, we use the so-called Bag of Features (BoF). A BoF basically consists of representing images based on extracting local features. The name comes from the Bag of Words (BoW) representation used in textual information retrieval [120]. Analogously as in BoW, in which we represent a certain document as a normalized histogram of word counts and build up a words dictionary By using BoF, we can do a similar approach but replacing the words with image features. The representative features of the images are gathered in clusters, which contain similar features. Every time a new representative feature is detected it is matched to the nearest cluster feature from the visual vocabu-



(a) Jammer-free **(b)** Jammer-free, binary image



(c) AM jammer **(d)** AM jammer, binary image



(e) Chirp jammer **(f)** Chirp jammer,binary image

Figure 3.8 Examples of spectrograms and binary image conversion of common jamming signals in baseband. All graphs contain a signal mixture of jamming signal and GPS L1 signal. C/N_0 is set to 45 dB and JSR is set to 50 dB.

lary. These similarities of BoF with respect BoW were the main reason for choosing BoF since most of the classification algorithms are also compatible with it. BoF makes it really easy to extract the image features used for the algorithm. At a high level, the procedure for generating a BoF image representation can be summarized in three steps [120]:

a) **Vocabulary Building**: In the first place, the whole collection of features from all the images from the training dataset are extracted. These features are stored in the so-called visual vocabulary dictionary, where each feature represents a "visual word" or "term".

b) **Terms Assignment**: After extracting all the features from the images, they are gathered in clusters. The clusters collect those terms whose features are the closest in the vocabulary dictionary in order to reduce the complexity of the dictionary.

c) **Term-vector Generation**: Finally, the term vector is generated by recording the counts of each term that appear in each image to create a normalized histogram, counting the times it is repeated in the cluster. This term vector is the final BoF representation of the images.

The set of features contained in the term vector is then used by the SVM algorithm to classify the data into different classes. In the following section, we will describe the main functioning principle of SVM.

3.3.2.2 SVM Basics

SVM's operation consists of a set of supervised learning methods that can be used for classification, regression, and/or ranking. By supervised learning, we mean that the user must take part in the training process of the algorithm. The user must label the training data, used for helping the algorithm to learn which classes will need to categorize, and to which class it belongs. SVM's uses machine learning theory as a principle of operation for both training and classification. SVM performs classification by transforming (if needed) the original training data into multidimensional space and constructing a multidimensional hyper-plane with it. The established hyper-planes will split the different classes to categorize. The hyper-plane with the maximum distance between the closest data points to the hyperplane, which is called support vectors, is the hyper-plane used for classification. It is typically called optimal hyper-plane. Therefore, our goal is to maximize the margin between the edge data points and the hyper-plane to be able to classify with minimal miss-classification error. Two examples of hyper-plane separation for two independent example data sets are depicted in Figure 3.9. The green squares represent the positive (above optimal hyper-plane) class and the red dots represent the negative (below optimal hyper-plane) class. The bold green squares and bold red dots are the support vectors, which are the samples the most difficult to classify because are closer to the hyper-plane separation. Support vectors are used to determine which is the optimal hyper-plane. The optimal hyperplane in Figure 3.9 is drawn with a dotted line and it is the hyperplane with the maximum distance between the different support vectors. In Figure 3.9a the classification can be easily done since the data is linearly separable and we only have two classes. For more than two classes, a graphical representation is harder to represent in a graphical form. For its part, Figure 3.9b, shows the example where the features data-set is non-linearly separable, and the multidimensional optimal hyper-plane (depicted as a 2-D hyper-plane in the figure) is not a straight line.

In order to find the optimal hyper-plane, we start modeling the hyper-plane as

$$\mathbf{w}^{\mathbf{T}}\mathbf{x} + b = 0 \tag{3.6}$$

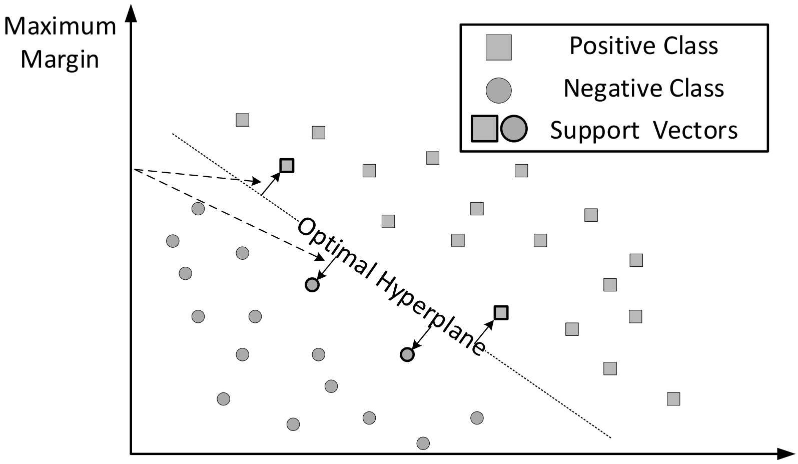
where $\mathbf{w}^{\mathbf{T}}$ is the normal vector to the hyper-plane, containing the weights towards the different data points, $\mathbf{x}$ contains the points defining the hyper-plane and b is a bias constant. If we assume that our data set is composed by $\mathbf{z} = z_1, z_2, ..., z_m$, and $y_i \in -1, 1$ being the class label of $\mathbf{z}$, which is -1 or 1 for the negative and positive class of the example shown in Figure 3.9, respectively. We can define the decision boundary, which should separate all the points as

$$\begin{aligned} \mathbf{w}^{\mathbf{T}}\mathbf{z} + b \geq 1 \quad if \quad y_i = 1 \\ \mathbf{w}^{\mathbf{T}}\mathbf{z} + b \leq -1 \quad if \quad y_i = -1 \end{aligned}$$

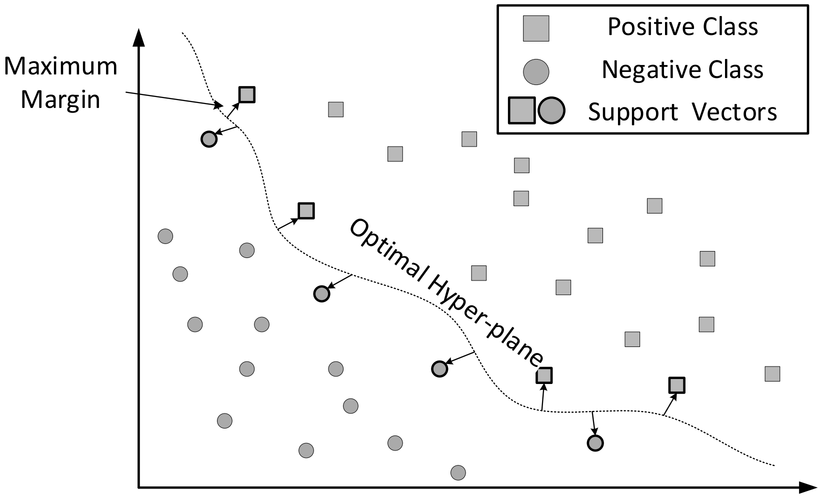
where $\mathbf{z}$ contains the features obtained with the BoF to be classified by the hyper-plane contained in $\mathbf{w}^{\mathbf{T}}$ and y_i is the resulting binary class. Among all the hyper-planes separating the data $\mathbf{z}$, there is an optimal hyper-plane yielding the maximum margin of separation between the classes to classify, which minimizes the miss-classification error. The optimal hyper-plane can be found by optimizing Equation (3.6) as

$$\max_{\{\mathbf{w},b\}} \quad min\{\| \mathbf{x} - \mathbf{z} \| : \mathbf{x}, \mathbf{z} \in \Re^N, (\mathbf{w}^{\mathbf{T}}\mathbf{x} + b = 0)\} \tag{3.7}$$

The weights vector $\mathbf{w}$ will consider the values of $\mathbf{z}$ closer to the hyper-plane with a higher value, being the closest ones of each class of the Support Vectors, as it is shown in Figure 3.9. To solve Equation (3.7), we can find different algorithms in the literature. The most popular ones are: i) Iterative Single Data Algorithm (ISDA) [128], ii) L1 soft-margin minimization by quadratic programming (L1QP) [129] and iii)



(a) Linear data separation



(b) Non-linear data separation

Figure 3.9 SVM binary classification hyper-plane representation. In the upper plot, a linear separable data representation is depicted. In the lower plot, the data is non-linear, and cannot be divided by a straight line.

Sequential Minimal Optimization (SMO) [130].

As we have seen, not all the classification tasks are easily separable (see Figure 3.9). When a linear separator of the data cannot be found, the data points are typically projected into a higher-dimensional space where the data points become linearly separable [28]. This transformation is carried out by functions called kernels. These functions basically map the non-linear separable data set into a higher-dimensional space where we can find a hyperplane that can separate linearly the samples. In the literature, multiple kernel types can be found to transform the data into a higher-dimensional space. Some of the most popular ones are: i) the linear kernel, ii) the polynomial kernel, and iii) the Radial Basis Function (RBF) kernel [28].

3.3.3 Convolutional Neural Network (CNN) Algorithm

The second algorithm we analyzed during the classification mechanism analysis is called CNN or Convolutional Neural Network (ConvNet). CNN consists of a sequence of layers. Each layer transforms the data into a simplified version of it through a differentiation function. The block diagram in Figure 3.10 shows the list of layers used in the proposed CNN architecture [28]. The number of layers shown in Figure 3.10 was selected to keep as simple as possible the algorithm, in order to evaluate the baseline performance of the method. So the layers architecture contains the minimum amount of layers for running the algorithm. Much more complex CNN architectures can be found in the literature [131, 132, 133], in which extra and multiple interconnected layers are used. The main features of each one of the layers described in Figure 3.10 are:

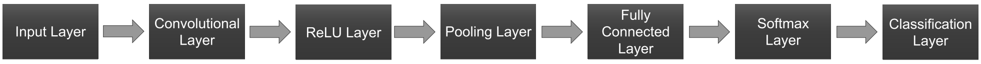


Figure 3.10 List of layers for the proposed CNN architecture.

1. **Input layer**: This layer converts the input image into $mxnxr$ matrix of data usable for the next layers. m is the height, n is the width in pixels of the image, and r is the depth (e.g., 1 for gray-scale images and 3 for Red Green Blue (RGB) images). Therefore, the purpose of this layer is to convert the image into data usable by the algorithm.
2. **Convolutional layer**: Computes the output number of 'neurons' that are con-

nected to local regions of the input image by computing a dot product between their weights and a small region they are connected to in the input. This layer is converting all the pixels in its receptive field into a single value. By using this layer we are decreasing the image size as well as bringing all the information in the field together into a single pixel.

3. **ReLU layer**: Also known as Rectified Linear Unit layer (ReLU), applies an element-wise activation function, such as the $\max(0, x)$ for transforming the summed weighted input from the node into the activation of the node or output for that input. In other words, it will output the input directly if it is positive, otherwise, it will output zero. It has become the default activation function for many types of neural networks because easiness while training the algorithm and often achieves better performance.

4. **Pool layer**: Performs a down-sampling operation along width and height. Pooling layers are used to reduce the dimensions of the feature maps. Therefore, it reduces the number of parameters to be learned by the algorithm, and the amount of computation performed in the convolutional network. In addition, the pooling layer summarises the features present in a specific region of the feature map generated by a convolution layer. So, further operations are performed on summarised features instead of precisely positioned features generated by the convolution layer. This makes the model more robust to variations in the features' position in the input image. For example, in the proposed architecture the pool size is [2,2], which means that if the layer returns the values $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, the maximum value in the regions of height 2 and width 2 will be selected, which is 4.

5. **Fully connected layer**: It takes the results of the convolution/pooling process and uses them to categorize the image. Therefore, it provides the ability to mix signals of information between each input dimension and each output class, and hence the decision can be based on the whole image and a class can be assigned to it.

6. **Softmax layer**: This layer is in charge of turning a vector of real values into a vector of real values that sum 1. The input values can be positive, negative, or zero. The softmax layer transforms these values into values between 0 and

1 so that they can be interpreted as probabilities. If one of the inputs is too small or negative, the softmax turns it into a low probability. If an input is large, then it is turned into a large probability, but always remains between 0 and 1.

7. **Classification layer**: Computes the cross-entropy loss for multi-class classification problems with mutually exclusive classes. In other words, it performs the actual classification based on the output of the previous layer.

3.3.4 Algorithms Training and Classification

Both algorithms, SVM and CNN needed to be initially trained, before being able to autonomously classify further input images [28]. For such a purpose, we generated a dataset of images such as the one shown in Figure **??**, containing different jammer types in a wide variety of conditions. Table 3.1 summarizes the main parameters settings for each jammer type. AM and FM tones were assumed to be uniformly distributed between 0.1 MHz and 10 MHz. Chirp T_{swp} and F_{swp} were uniformly distributed between $5-20$ μs and $5-20$ MHz, respectively. The bandwidth for Narrow Band (NB) Jammers was set between 20 MHz and 2 GHz. Finally, for the pulsed jammer, the duty cycle (τ) and repetition frequency (F_r) were set between $1-19$ μs and $0.1-1.9$ THz. The GNSS C/N_0 was set as well as uniform distributed between 25 dBHz and 50 dBHz. The JSR was set between 40 dB and 80 dB. In Table 3.1, $\mathcal{U}(a, b)$ represents a variable uniformly distributed between a and b.

Table 3.1 Jammer parameters summary used in the provided simulations. $\mathcal{U}(a, b)$ represents a variable uniformly distributed between a and b.

Jammer Type	Parameter
AM jammer	$f_J \sim \mathcal{U}(0.1, 10)$ MHz
Chirp	$T_{\text{swp}} \sim \mathcal{U}(5, 20)$ μs $F_{\text{swp}} \sim \mathcal{U}(5, 20)$ MHz
FM jammer	$f_J \sim \mathcal{U}(0.1, 10)$ MHz
NB jammer	$B_w \sim \mathcal{U}(20, 2000)$ kHz
Pulsed jammer	$\tau \sim \mathcal{U}(1, 19)$ μs $F_r \sim \mathcal{U}(1 \cdot 10^{-1}, 19 \cdot 10^{-1})$ THz

For training purposes, we generated 6000 images (i.e., 1000 images per jammer type, 5 jammer types plus the jammer-free scenario). Each one of the images was labeled during the image generation since the algorithms needed to know which features were most representative for each jammer type. It means that during the algorithm training, the algorithm needs to know the image features for each category to be classified later. While the testing dataset was composed of 54000 images (i.e., 9000 images per jammer type). With the algorithms already trained, and the testing library of images we carried out the simulations shown in Section 3.4.3.

3.4 Numerical Evaluations and Results

3.4.1 Detection Results using simulated GNSS data

This section shows a comparison between the different detection algorithms described in Section 3.2.2 against three different jammer types, namely AM, chirp, and pulsed jammers. To carry out this study, we considered simulated GPS C/A L1 signal mixed up with specific jammer signals, as well simulated using Matlab. The C/N_0 and JSR were set to 45 dB-Hz and -20–50 dB, for the GNSS and jammer signals, respectively. Figure 3.11 shows the probability of detection for these three jammer types at different JSR levels. AM probability of detection is depicted in Figure 3.11a, chirp results are shown in Figure 3.11b, finally in Figure 3.11c are depicted the results for a pulsed jammer. We can observe as, in general terms, the best detection performance against the different jammer types is generally yielded by the power-based detectors, namely AGC, TPD, FPD, Welch and periodogram. In the case of AM and chirp signal, the jammer can be reliably detected even at JSRs below 0 dB. Further comparison of Figure 3.11a and Figure 3.11b shows that the detection methods behave similar for AM and chirp signals. The detection probability start to be non-zero at JSR higher than -15 dB. The detection algorithms that have the lowest performance are the ones based on notch filter and kurtosis. The notch filter algorithm requires up to 15 dB more jamming power to detect the jammer compared with the rest of the methods. In addition, in order to achieve a $P_\mathrm{d} = 1$, we need a strong jammer transmitting with a JSR of at least 0 dB. In addition, we can observe from Figure 3.11c that the kurtosis algorithm does not work at all with pulsed jammers. The main cause of this is that the pulses of the considered signal are too short and are not repeated constantly, which makes it harder or even undetectable with some of the considered detectors, such as kurtosis.

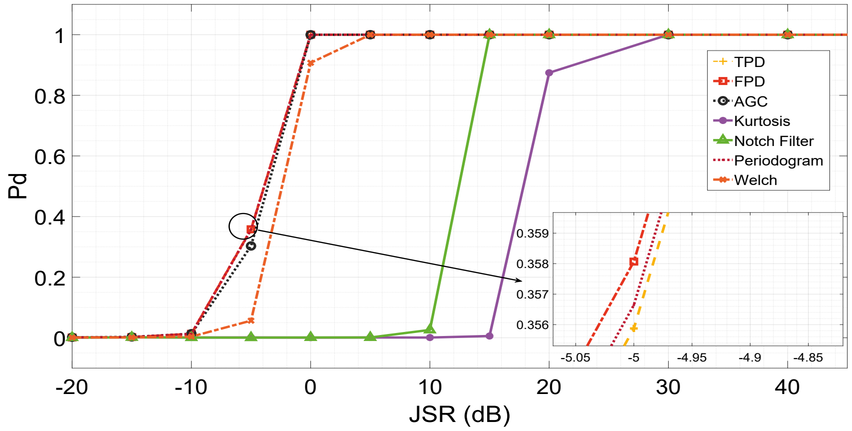
3.4.2 Detection Results using real GNSS data

Similarly, as we did with the simulated data, we tested the same detection algorithms described in Section 3.2.2 against in-lab generated data [26, 134]. For obtaining the results in this section, we adopted the following procedure: i) we generated the jamming and GNSS RF signals with two separate signal generators, namely VST for jamming and Spectracom for GNSS signal; ii) we recorded the generated signals with the help of a National Instruments USRP model 2954; and iii) we fed these signals to the selected jamming detection algorithms in our software. The last step was done in software and consists of conditioning the digital baseband signals, application of the channel model, and evaluating the algorithms.

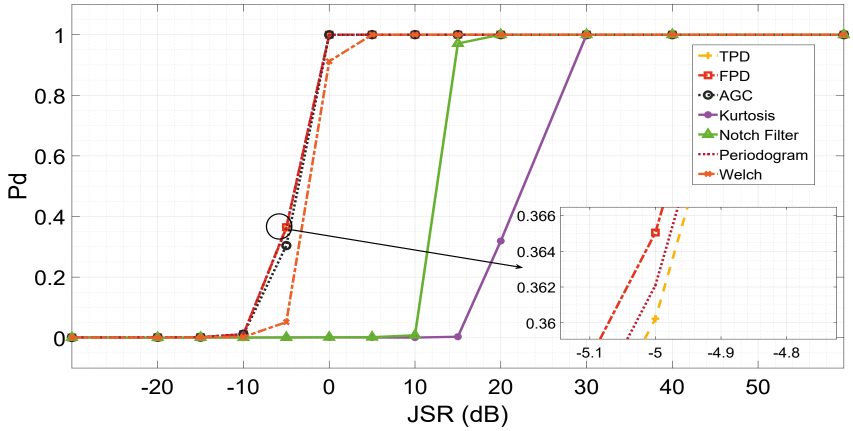
The laboratory hardware setup used during the signal generation and recording is shown in Figure 3.12. It shows a Spectracom GNSS signal generator (GSG), used to generate the GNSS signals, a VST, used to generate the different jamming signals, and a USRP used as a receiver. A computer is in control of the VST and the USRP through MATLAB and LabVIEW software, respectively. In addition, this computer receives the baseband I/Q data from the USRP and saves it on the hard disk.

The full signal chain is illustrated as a block diagram in Figure 3.13.

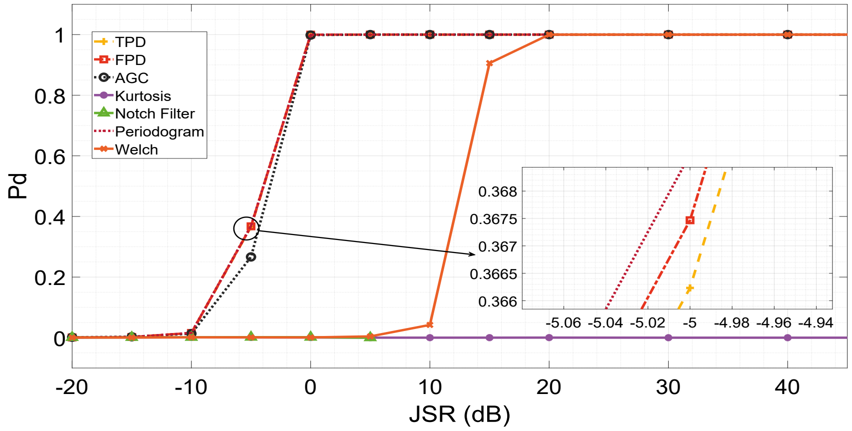
We generated the baseband jamming signals with MATLAB and then we sent them to the VST. The GSG is standalone and it generates the GNSS RF signals according to the parameters that we set in its user interface. After generating both the interference and GNSS signals, they were sent through cables to the USRP. We configured the USRP to receive each signal in a separate channel synchronously. To record the signals we adapted a LabVIEW user interface through which we configured the USRP. The two baseband I/Q sample streams provided by the USRP were buffered and then sent to the computer and saved into files. For more details, the readers are referred to [134]. All the remaining processing was done in software. This includes the channel models that account for fading and different propagation paths between transmitter and receiver, the power adjustments to meet specific JSR at the antennas, etc. All the tested algorithms were assessed in Matlab following the models given in Equations 3.3-3.5. In particular, the AGC detector made use of the AGC system



(a) AM jammer



(b) Chirp jammer



(c) Pulsed jammer

Figure 3.11 Comparison of the probability of detection for AM, chirp and pulsed jammer types using different test statistic metrics.

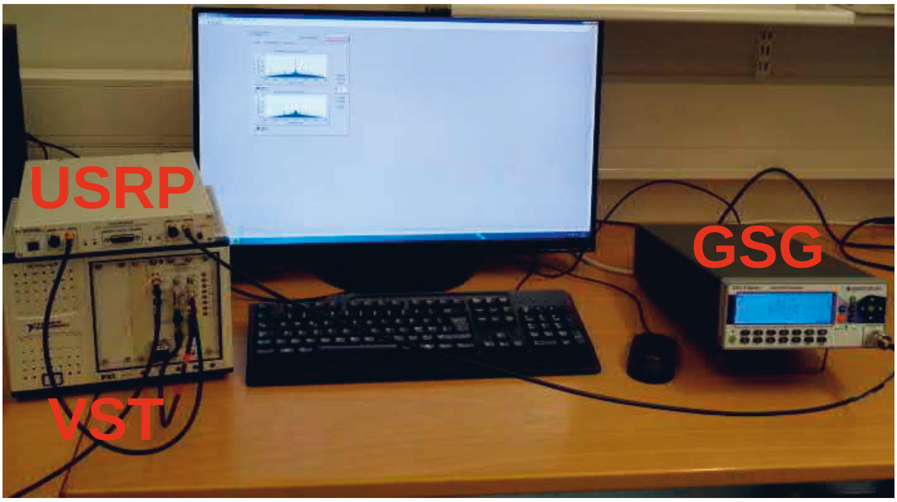


Figure 3.12 Hardware setup to record GNSS and jamming signals.

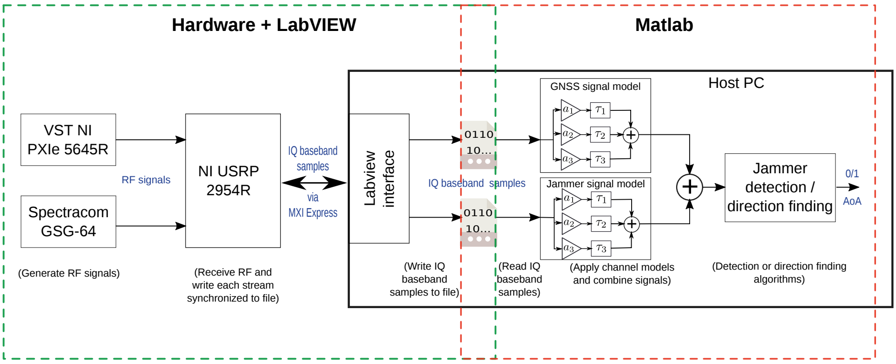


Figure 3.13 Block diagram of the jammer detection and direction finding methodology.

modeling provided by the Communication Toolbox of Matlab.

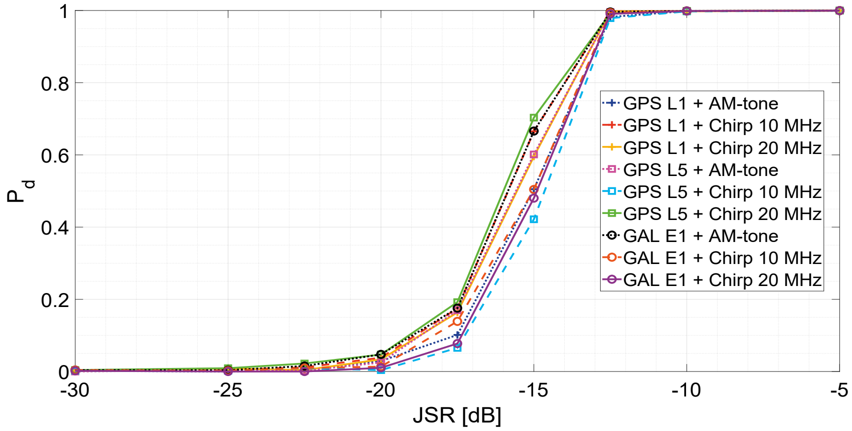
To carry out the simulations, we computed the test statistics under H_0 and H_1, fixing the probability of false alarm to the desired reliability level (e.g., 10^{-3} and we computed the corresponding threshold and detection probability. The simulations were computed over 500 Monte Carlo iterations. The SNR (GNSS signal & noise) was set to -10 dB. The used GNSS signals are combinations of i) three GNSS signals: GPS L1, GPS L5 and Galileo E1 signals, and ii) three common interference signals: AM-tone and two chirp signals with 8.64 µs sweep period and 10 MHz and 20 MHz sweep range.

Figure 3.14 shows the detection performance for TPD, FPD and AGC algorithms, depicted in top, center and bottom plots, respectively, for all the considered GNSS signals. All three algorithms show similar performance in terms of detection probability. This was also noticed with the simulated data (see Figure 3.11). For the Galileo E1 & 10 MHz chirp, the TPD requires about 2 dB less JSR for achieving the same P_d than the AGC for most of the tested signal combinations. In general, all detectors start detecting the presence of jammer at a JSR of about -25 dB and all of them reach a P_d close to 1 at a JSR of -10 dB, for all the considered scenarios. No clear pattern for best/worse performance combination of GNSS signal plus jammer was found by analyzing Figure 3.14. The outcome we get though is that the performance of the detectors is dependent on the GNSS signal type, especially for some of the detectors, such as AGC.

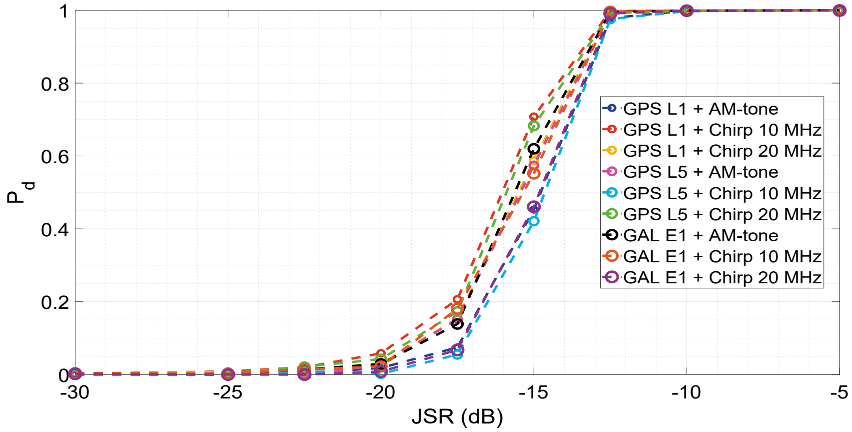
Comparing Figure 3.14 (using in-lab recordings) with Figure 3.11 (using simulated data), we can observe as by using in-lab data the algorithms are slightly more sensible in terms of minimum JSR to achieve detection (-25 dB rather than -10 dB). One possible reason can be due to the fact that while recording the signal in the laboratory, both GNSS transmissions and noise were added and collected together. So while applying the corresponding level of JSR, the GNSS signal was more affected by noise, and hence we were able to see the jammer effects more clearly. In any case both Figure 3.14 and Figure 3.11 show similar performance overall.

3.4.3 Classification Results

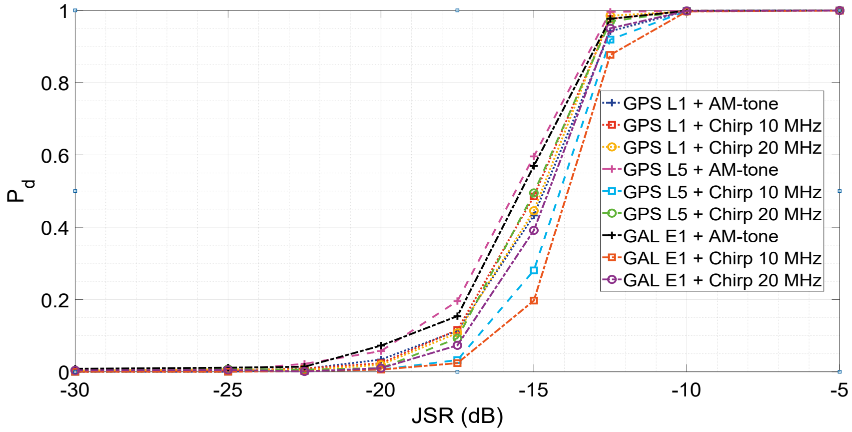
To analyze the performance of both classifier algorithms, we compared the confusion matrices obtained based on the testing dataset of images described above. The confusion matrix shows how accurate a classifier is, in terms of how well it classifies and miss-classifies the test data in the different categories it is handling. Comparing both confusion matrices in Figure 3.15, we observe that SVM algorithm has a mean accuracy of 94.90 %, while CNN algorithms mean accuracy is 91.36 %. If we analyze more deeply the results, algorithm by algorithm, we can observe from Figure 3.15a that just less than 2 % cases are miss-classified as jamming-present scenarios when in fact there was no interference. For their part, NB jammers are classified correctly almost 94 % of the time. Pulsed and chirp jammers offered detection probability close to 100 %. And finally, the obtained AM and FM single-tone jammers classification accuracy performance was similar in both cases, with an accuracy of



(a) TPD algorithm



(b) FPD algorithm



(c) AGC algorithm

Figure 3.14 P_{d} vs JSR for TPD (top), FPD (center) and AGC detectors with AWGN 5-path fading channel. 500 Monte Carlo iterations and a fixed P_{fa} of 10^{-3} have been used.

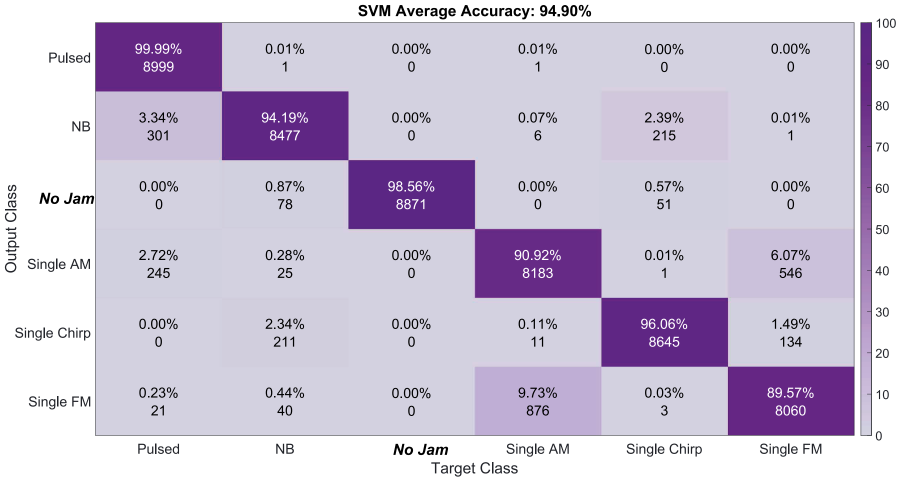
about 90 % each. Using the SVM algorithm we can determine the presence or absence of any interference with an accuracy of more than 98 %. About CNN, we observe from Figure 3.15b that the accuracy determining the presence of a jammer signal is slightly higher compared to SVM, although only with 0.4 %. We can also notice from Figure 3.15b that pulsed jammers classification accuracy is as well close to 100 %, similarly to what we obtained with SVM algorithm. Chirp jammer's accuracy is more than 91 %, but this is about 5 % lower compared with SVM algorithm. AM and FM jammers shows an accuracy of almost 91 % and 89 %, respectively, which is slightly lower than with SVM. Lastly, for NB jammers, we get an accuracy of only 78 %, which is about 5 % lower than with SVM algorithm.

We would like to emphasize that these promising shown results were obtained by using a total training dataset of only 6000 images, 1000 images per category. By increasing the dimensions of the training dataset, the algorithms will most likely be able to learn better the main features of each jammer type, and then distinguish better among the different considered classes, increasing the classification performance.

3.5 Summary of contributions

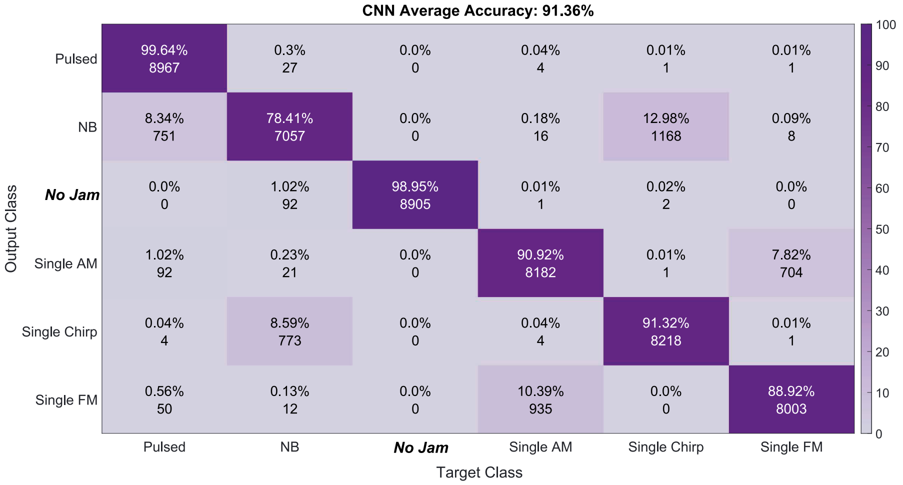
The main contribution to this thesis by the author in this chapter can be summarized as follows:

- Formulating the interference detection problem in the context of classical binary detection problem and reviewing state-of-the-art detection algorithms applicable to GNSS.
- Analyzing the trade-offs of various time and frequency-based detectors and selecting a subset of them for further analysis via simulations and measurements in the laboratory.
- Investigating the advantages and drawbacks of different classification algorithms based on machine learning for image classification. Among those evaluated, only the ones with the best potential use for GNSS jamming classification were selected for further analysis.
- Implementing a classification architecture based on machine learning using two algorithms from the literature: SVM and CNN. These classification algorithms employed spectrogram images for classification.


SVM Average Accuracy: 94.90%

Output Class \ Target Class	Pulsed	NB	**No Jam**	Single AM	Single Chirp	Single FM
Pulsed	99.99% 8999	0.01% 1	0.00% 0	0.01% 1	0.00% 0	0.00% 0
NB	3.34% 301	94.19% 8477	0.00% 0	0.07% 6	2.39% 215	0.01% 1
No Jam	0.00% 0	0.87% 78	98.56% 8871	0.00% 0	0.57% 51	0.00% 0
Single AM	2.72% 245	0.28% 25	0.00% 0	90.92% 8183	0.01% 1	6.07% 546
Single Chirp	0.00% 0	2.34% 211	0.00% 0	0.11% 11	96.06% 8645	1.49% 134
Single FM	0.23% 21	0.44% 40	0.00% 0	9.73% 876	0.03% 3	89.57% 8060

(a) SVM algorithm


CNN Average Accuracy: 91.36%

Output Class \ Target Class	Pulsed	NB	**No Jam**	Single AM	Single Chirp	Single FM
Pulsed	99.64% 8967	0.3% 27	0.0% 0	0.04% 4	0.01% 1	0.01% 1
NB	8.34% 751	78.41% 7057	0.0% 0	0.18% 16	12.98% 1168	0.09% 8
No Jam	0.0% 0	1.02% 92	98.95% 8905	0.01% 1	0.02% 2	0.0% 0
Single AM	1.02% 92	0.23% 21	0.0% 0	90.92% 8182	0.01% 1	7.82% 704
Single Chirp	0.04% 4	8.59% 773	0.0% 0	0.04% 4	91.32% 8218	0.01% 1
Single FM	0.56% 50	0.13% 12	0.0% 0	10.39% 935	0.0% 0	88.92% 8003

(b) CNN algorithm

Figure 3.15 SVM and CNN confusion matrix.

- Fine-tuning the classification algorithm parameters for achieving the best performance according to the minimum chosen baseline.

- Contributing with the following observations: i) power-based detectors (namely AGC, TPD, FPD, Welch, and periodogram) offered the best performance for jamming detection among the studied algorithms; ii) the analysis with recorded-data matched, in general terms, the simulated-based results; and iii) Both SVM and CNN are highly promising classification algorithms, achieving high accuracies even with a moderate training dataset in terms of jammer classification. SVM has proved to be slightly better than CNN, no doubt due to the relative small-to-moderate sizes of training datasets.

Chapter 4

LEO-based Positioning as Complementary or Alternative Positioning to GNSS

In this chapter, we discuss the suitability of LEO satellites for positioning purposes. We first discuss the potential need for additional satellite navigation systems, describing the advantages and disadvantages of LEO constellations with respect MEO and what can LEO offer. Next, we provide some basics about satellite miniaturization and we describe the current state of small satellites. We list the main advantages and disadvantages of each small satellite class, which are typically used in LEO, with respect to the regular-sized satellites. After that, we provide some basics about satellite constellations and how we can uniquely identify them. We give an overview of the main constellation architectures, orbit altitudes, and orbital parameters that can be tuned in order to reproduce custom constellations according to the system's needs. Finally, we provide some numerical evaluations by comparing existing and planned LEO and MEO constellations. The analysis of these constellations is done from the point of the potential positioning performance. The metrics we study are DoP (i.e., GDoP, PDoP, etc), coverage (i.e., how many satellites are in view from an specific Earth location), and link budget (i.e., which is the strength we can receive signals from LEO satellites).

4.1 Why LEO-PNT satellite constellations? Advantages and Disadvantages and Main Features With Respect to MEO constellations

GNSS PNT services are currently operated mostly with MEO satellites. With the exception of Chinese Beidou system which is also using 5 GEO and 3 Inclined geosynchronous orbit (IGSO) satellites in addition to about 27 MEO satellites. MEO provides some advantages with respect to LEO, but also several drawbacks. In Table 4.1 we compare the main advantages and disadvantages of MEO and LEO orbits. LEO satellites are much closer to the Earth's surface (up to 175 times with respect MEO). This translates into a higher received power (up to 30 dB [135]), which in turn might improve the PNT service availability in indoors and other challenging scenarios. MEO signals are weaker than LEO signals, and, therefore, they are subjected more to intentional and unintentional interference, as shown in previous chapters. In turn, the coverage per satellite is reduced in LEO, since the single satellite footprint is much smaller due to the closest proximity of satellites to the Earth's surface. For this reason, LEO constellations typically need hundreds of satellites in the sky to cover the Earth entirely, while MEO constellations only need tens of satellites. Figure 4.1 depicts a MEO vs LEO footprint comparison, showing the potential area of the Earth covered by a single satellite at MEO and LEO altitudes. Besides the larger footprint per satellite, MEO satellites are in view for more time in a specific location (up to a few hours), while LEO satellites are only available for a few minutes (typically 15-20 min).

For their part, LEO satellites are much easier and cheaper to be launched and to be replaced, mainly again due to the lower orbit altitude and much closer proximity to the Earth. Less effort is needed for putting in LEO orbit compared to MEO orbit the satellites, which turns into lower costs. In addition, LEO satellites can be much lighter due to the lack of necessity for additional and heavy protection for the sensitive and expensive components due to space radiation. In LEO, the atmosphere acts as natural radiation protection for the satellite components. This also considerably reduces the cost of the satellite itself, in addition to the launching cost. But one of the main drawbacks is that LEO satellite lifetime is much lower ($<$ 5 years in front of 10-20 years for MEO), mainly due to the higher drag affecting the satellites in LEO

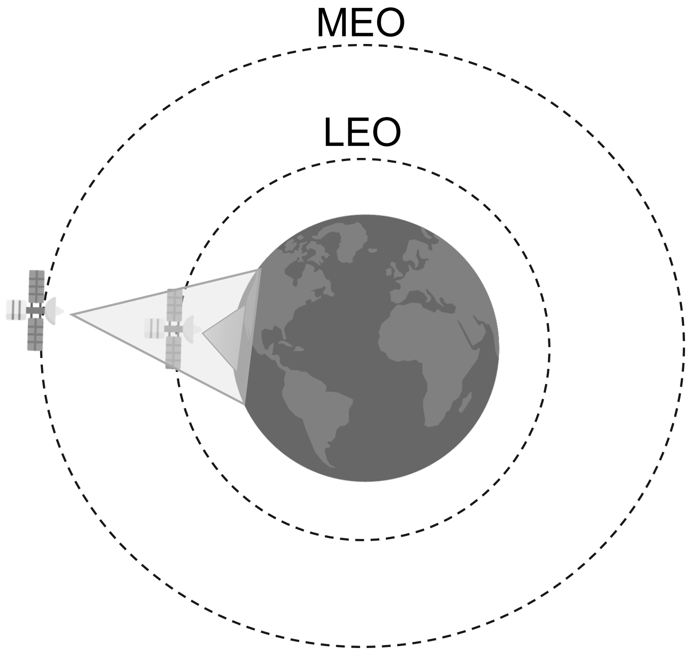


Figure 4.1 MEO vs LEO footprint comparison.

suffer. The drag effects are heavier the closer we are to its surface since the satellite orbital drag is mainly due to the presence of the atmosphere and the Earth's gravitational attraction. For this reason, the orbits of LEO satellites are much more affected by the atmosphere and Earth's attraction, and therefore orbital drag is higher. This provokes a more severe de-orbit in LEO rather than MEO satellites, reducing the time the satellites are maintained in the correct orbit. Due to the heavier Earth's influence, LEO satellites follow much more complex orbital dynamics, which typically are more difficult to predict [136]. MEO orbital dynamics have been typically more studied and are currently better known, which in turn provides more accurate models of orbit prediction [137, 138, 139]. In addition, physical phenomena, such as the Doppler shift, change quickly due to the lower altitude and much faster orbit speeds. Therefore LEO satellite's orbit parameters are typically more difficult to estimate and track accurately in the receiver, compared to MEO ones, especially when one takes into account the fact that LEO satellites are only visible for a few minutes.

Table 4.1 MEO and LEO advantages and disadvantages comparison summary.

Comparison Aspects	MEO		LEO	
	Advantages	**Disadvantages**	**Advantages**	**Disadvantages**
Orbital	The Earth is covered with less satellites	Transmissions need to travel longer distances	Orbits closer to Earth's surface	Lower coverage per satellite; more satellites needed to cover the whole Earth
Cost	Longer satellite life span	More expensive constellation deployment; extra weight due to additional radiation protection	Cheaper and easier to launch and replace; natural protection from space disturbances	Satellite shorter life span mainly due to atmospheric drag
Channel	N/A	Reduced indoor availability	Higher received power (up to 30 dB); better protection to interferences and multipath, and better indoor and challenging environments availability	N/A
Receiver	Well known orbit dynamics; easily trackable Doppler shift	N/A	N/A	Orbit prediction is harder due to more complex dynamics; Doppler shift changes faster
Visibility	A single satellite is visible for a longer time (up to few hours)	N/A	N/A	Lower in-view time per satellite; a single satellite is only visible for about 15-20 min

4.2 CubeSats and Miniaturized satellites: Main features of Small Satellites With Respect to Regular-Sized Satellites

Current advances in materials and components for spatial applications in combination with the use of lower orbit altitudes have opened the possibility to utilize miniaturized satellites [140]. These miniaturized satellites are smaller, lighter, and more compact compared to traditional satellites. For this reason, they are able to provide low-cost and low-power satellite solutions [140]. Table 4.2 shows a classification of satellite types according to their mass. Examples of satellite systems, already in the sky or currently under development belonging to each category are also given. The four GNSS constellations, namely Galileo, GPS, GLONASS, and BeiDou, are also listed among these examples, as they will represent the benchmark for any future LEO-PNT solution [141] with regular-sized satellites (satellites with a mass < 500 kg). These regular-sized satellites are divided into: i) Large satellites, ii) Medium satellites, and iii) Small satellites.

Currently, the Attosat and Zeptosat categories are still in the research phase, without any commercially available satellite system. The main reason is the big challenge of building long-durable satellites with masses as low as 10 grams. Nowadays, the most used classes of miniaturized satellites are the Micro- and Nano- classes [142], corresponding to 10-100 kg and 1-10 kg of mass, respectively. Micro- and Nano-classes encompass more than 50% of existing small satellites [142]. CubeSat standard is the most common for current Nano- and Microsatellites. By definition, the CubeSat is a cube-shaped satellite of dimensions $10 \times 10 \times 10\ cm^3$ with a mass up to 1.33 kg [143]. Although typically, the mass of a small satellite beyond 500 Kg is defined in CubeSats unit (U), under the form of 1U CubeSat (reference CubeSat), 2U CubeSat, etc with a maximum of 24U [144]. For example, a 16U CubeSat would have a mass of about $16 \cdot 1.33 \approx 21$ kg and dimensions, putting it in the Microsats category. An example of a 1U, 3U, and 6U CubeSat is given in Figure 4.2 along with its dimensions.

Satellite miniaturization provides several advantages with respect to regular-sized satellites:

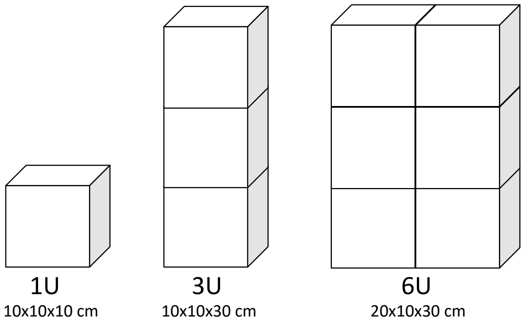


Figure 4.2 Example of 1U (left), 3U (middle) and 6U (right) CubeSat.

a) **More accessible**: New advances in technology, the reduction in prices, the appearance of new manufacturers, and the reduction in waiting times for the implementation of new projects in space have had a decisive influence on the reduction in space barriers for all types of companies and countries. Before CubeSats and miniaturized satellites, only a few countries and multinationals had the financial and technical capacity to access space [31, 32].

b) **Higher affordability**: A regular-sized satellite can cost approximately between 100 and 300 million euros [145]. A CubeSat, typically costs less than 500k euros [145]. Nevertheless, the price depends on many factors, such as its final size, its complexity, or whether it is the first satellite of the constellation or not.

c) **Shorter development times**: A conventional satellite needs very long development times, between 5 to 15 years [146]. In contrast, the first CubeSat of a constellation can be in space within 9 months [144] and even less if it shares the architecture and hardware.

d) **More up-to-date technology**: CubeSats are usually designed for a span life of 2-4 years [144]. Due to their shorter lifetime than respect regular-size satellites, a replacement satellite can incorporate a more updated technology. In this way, the services offered can be significantly improved and extended with the help of the latest available technology. In contrast, a regular-sized satellite's lifetime is typically much longer (> 10 years) than small satellites, and it can be the case where the satellite is still operative but using obsolete technology.

e) **Smaller size and weight**: Size and weight are closely related to the price.

The heavier and bulkier a satellite is, the more expensive it is to put in orbit. Small satellites such as CubeSats are much smaller and lighter than regular-size satellites, and hence cheaper to put in orbit.

f) **Higher scalability**: Small satellites can be replaced in a very short period of time and at a lower cost in case of malfunctioning. In addition, more satellites can be appended into the constellation to increase the features, provide backup or simply provide redundancy to the services they offer easier and at a lower cost compared with regular-sized satellites.

g) **More flexibility**: Small satellites such as CubeSats are much more adaptable and flexible rather than regular-sized satellites, which have a more specific application. In case of a new business opportunity is detected, it is possible to implement new functionalities and services in a relatively simple and quicker way with small satellites. Moreover, if the small satellite use one of the available SDR platforms, re-configuring the payload of small satellites in space becomes pretty easy.

Of course, small satellites have some disadvantages as well over regular-size satellites. The main disadvantages of small satellites are their limited performance and the power supply they can offer due to their container size. In small satellites, there is no room for big and heavy, although high-performance and power-consuming, payloads. In addition, big elements such as antennas, solar panels, and propulsion systems must be kept in reduced dimensions. Therefore in small satellites, we have critical elements such as maximum radiated power, efficiency in data processing, and a propulsion system for orbit correction hardware-limited.

4.3 LEO Constellation Design for Positioning

In this section, we will focus on the design aspects for the space segment of a LEO constellation, although most of the described information is generic and hence also applicable to any other type of orbital altitude. The space segment definition of the satellite constellation is one of the most critical and most difficult stages, as there are many degrees of freedom, such as the type of orbit (i.e., polar, sun-synchronous, etc), the constellation architecture/shape (i.e., Walker Delta [147], Ballard Rossette [148], Flower[149], etc), the altitude of the orbital, the orbit inclination, the number of

Table 4.2 Satellite classification with respect to satellite mass and orbital altitude.

MEO & GEO			LEO		
Satellite Class	Mass [kg]	Examples	Satellite Class	Mass [kg]	Examples
Large satellites	>= 1000	GPS, Beidou, Glonass, Boeing 702, O3B mPower, Telstar 19V, Thales Alenia Leosat, Ziyuan 3	**Minisats**	100-500	Space X Starlink, OneWeb, Amazon Kuiper, Hongyun, Telesat
Medium satellites	500-1000	Galileo, Iridium/Iridium NEXT, Telesat	**Microsats**	10-100	Iceye, Capella Space, BlackSky Global, Kepler Communications, Hellas-Sat, Tekever
			Nanosats	1-10	PlanetLabs Dove/SuperDove CubeSats, Spire Global Lemur-2 and Minas, Myriota, UWE-4, Xiaoxiang-1, Tyvak nanosats, DICE CubeSats, QuakeSat, NanoAvionics, Hiber, Kleos space CubeSat, Horizon Technologies Amber
			Picosats	0.1-1	warm Technologies SpaceBEE, Gauss PocketQubes, Alba Orbital Unicorn, Fossa Systems (FossaSat)
			Femtosats	0.01-0.1	SunCube FemtoSat
			Attosats	0.001-0.01	N/A
			Zeptosats	0.0001-0.001	

independent orbits/orbital planes, the number of satellites in each orbital plane, and some other orbital parameters such as the Right Ascension of the Ascending Node (RAAN), rate of perigee rotation, drift between satellites (e.g., for several orbital planes with different inclinations, satellites will drift apart), etc.

4.3.1 Orbital Parameters for Describing Orbits: Keplerian Orbital Elements

The orbital parameters that uniquely identify a specific orbit are typically called Keplerian orbital elements or just Keplerian elements. The Keplerian elements are divided into a set of six elements: eccentricity, semi-major axis, inclination, Right Ascension of the Ascending Node (RAAN), argument of periapsis, and true anomaly.

The two elements defining the shape and size of the orbit are:

a) **Eccentricity (e)** : Determines the deviation of an orbit from a perfect circle. A value of 0 corresponds to a perfectly circular orbit. It has values between 0 and 1 corresponding to an elliptic orbit shape. A value equal to 1 corresponds to a parabolic escape orbit and greater than 1 corresponds to a hyperbolic orbit.

b) **Semi-major axis (a)** : It is the longest diameter of the orbit with respect to the center of the orbit (or focus). In circular orbits, a can be measured as the Earth's radius plus the orbit altitude with respect to the Earth's surface. The parameter a is typically measured in km.

The elements defining the orientation of the orbital plane in which the orbit is embedded are:

a) **Inclination (i)** : It is the vertical tilt of the orbit with respect to the reference plane. The tilt angle is measured perpendicular to the line of intersection between the orbital plane and the reference plane (typically the equator). It can take values in the range [0, 180] degrees.

b) **Right Ascension of the Ascending Node (RAAN) (Ω)** : Defines the angle between the reference direction and the upward crossing of the orbit on the reference plane. It can take values in the range [0, 360] degrees.

And finally, the two remaining elements that define the satellite's position in the orbit are:

a) **Argument of periapsis (ω)** : It is the angle from the orbiting body's ascending node (where the orbiting object moves north through the plane of reference) to its periapsis (the closest point the satellite comes to the Earth), measured in the direction of motion. Therefore, it defines the angle between the ascending node and the periapsis.

b) **True anomaly (ν)** : Determines the angular position of the orbiting body with respect to the orbit. It can take values in the range [0, 360] degrees.

4.3.2 Orbit type

The possibilities for the satellite orbits are very diverse [150, 151, 152]. A classification of the most common orbit types is listed below, according to their altitude, direction, inclination, eccentricity, and synchronicity.

4.3.2.1 Altitude

According to the altitude, we can divide the orbits as:

a) **LEO**: Geocentric orbits (orbits in which the Earth is the central body) with altitudes between 200 km and 2000 km.

b) **MEO**: Geocentric orbits with altitudes ranging from 2000 km to 35786 km.

c) **GEO**: Geosynchronous orbit that matches Earth's orbital period – taking 23 hours 56 minutes and 4 seconds –. This happens at an orbit altitude of exactly 35786 km.

d) **High Earth Orbit (HEO)**: Geocentric orbits above 35786 km.

4.3.2.2 Direction

Depending on if the satellites are moving in the same direction of the Earth's rotation or not, we can divide the orbits as:

a) **Prograde-orbits or direct orbits** [153]: In Prograde-orbits, the satellites move in the same direction as the Earth's rotation. In addition, the orbital inclination angle is strictly less than 90° (e.g., GNSS MEO satellites and Amazon Kuiper LEO satellites). Most satellites are launched in a prograde orbit because the Earth's rotational velocity provides part of the required orbital velocity to be in orbit, with a consequent saving of fuel.

b) **Retrograde-orbits** [153, 154]: In Retrograde-orbits, the satellite moves in the opposite direction with respect to the Earth's rotation. and the orbital inclination angle is strictly higher than 90° and lower than 180° (e.g., OneWeb and BlackSky Global LEO satellites). The particular case in which the inclination is exactly 180°, is called *equatorial orbit*. Retrograde orbits are not typically used because the quantity of fuel required to put in orbit the satellite is greater than for prograde orbits, especially for communications. But are usually used for Earth observation, given the fact that both bodies (Earth and satellite) are moving in opposite ways, increasing the relative velocity of the satellite, and providing a higher frequency of updates in the measurements. An example of a constellation using retrograde orbits is the reconnaissance satellites constellation called Ofeq [155].

4.3.2.3 Inclination

The orbits can be classified according to their inclination with respect to the equator as:

a) **Inclined Orbits**: If the orbit exhibits an angle other than 0° with respect to the Earth's equatorial plane, is considered that the orbit is inclined. Depending on the degree of inclination, we can face different types of inclined orbits:

   i) **Polar orbits** [156]: In polar orbits, in a strict-sense definition, the orbital inclination angle must be ±90° (i.e., the satellites travel around the Earth from pole to pole). However, according to European Space Agency (ESA), also angles close to 90° are referred to as polar (e.g., Iridium LEO satellites, with inclinations of 86.4° are considered as having polar orbits). A single satellite in a polar orbit can provide coverage to the entire Earth, although there are long periods when the satellite is out of view from a particular location. This is one of the reasons why this type of orbit is not typically used for communications. The lack of accessibility can be improved by employing more satellites in different orbital planes.

   ii) **Sun-synchronous Orbit (SSO)**: These are nearly polar orbits (orbits with an inclination angle of $\approx 90°$) that pass the equator at the same local solar time on every pass. It means that a satellite is visible from a specific location at the same local time.

b) **Non-inclined orbits**: Non-inclined orbits, in turn, can be divided in:

   i) **Equatorial orbits**: These orbits lie close to the Earth's equatorial plane. The orbital inclination is 0° for prograde orbits and 180° for retrograde orbits.

   ii) **Ecliptic orbits**: These orbits lie in the ecliptic plane, which is defined as the imaginary plane containing the Earth's orbit around the sun.

c) **Near equatorial orbits**: Similar to Equatorial orbits, but its inclination is not strictly zero, but still very low.

4.3.2.4 Eccentricity

According to the eccentricity of the orbit, which is the parameter that determines how circular is the orbit, the orbits can be classified as:

a) **Circular orbit**: In circular orbits, the eccentricity is equal to 0, and the orbit traces a circle.

b) **Elliptic orbit**: In elliptic orbits, the eccentricity is greater than 0 but lower than 1. The orbit traces an ellipse.

c) **Parabolic orbit**: In Parabolic orbits, the eccentricity is exactly equal to 1. In these orbits, the satellites have a velocity equal to the escape velocity (a velocity greater than the velocity to escape the gravitational pull of the planet). For this reason, the orbit is typically not a closed loop, and the periodicity is not determined.

d) **Hyperbolic orbit**: In Hyperbolic orbits, the eccentricity is greater than 1. The orbit traces a hyperbole, which again does not depict typically a closed loop.

Figure 4.3 depicts an example for each orbit type according to the eccentricity. The purple color shows the circular case, the yellow color is the elliptic orbit type, while red and green depict a parabolic and hyperbolic orbit, respectively.

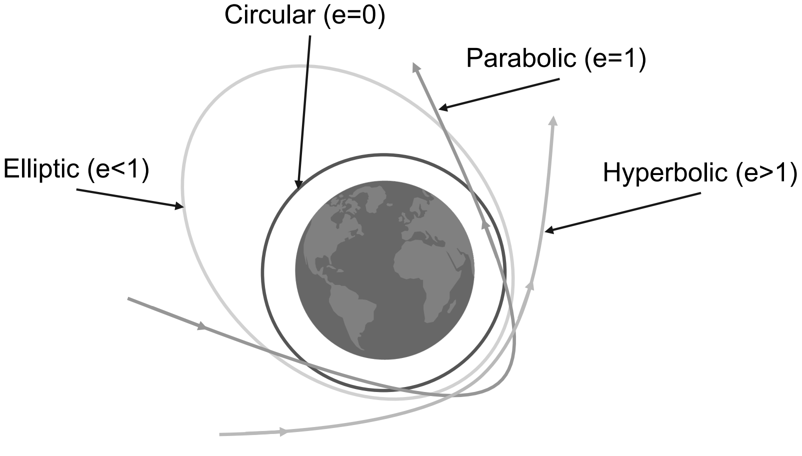


Figure 4.3 Orbit type according to eccentricity.

4.3.2.5 Synchronicity

Depending on the synchronicity, the orbits can be classified as:

a) **Synchronous orbits**:

   i) **Sun-synchronous orbits**: Sun-synchronous orbits are a particular type of polar orbit, where the satellite is always seen at the same hour and at the same point on the Earth (e.g., a satellite is visible in Tampere exactly at noon each day), which means that the orbital planes are synchronized to always be in the same fixed position relative to the Sun.

   ii) **Sun-Geosynchronous orbits**: Sun-Geosynchronous orbits are analogous to sun-synchronous orbits, in which the satellite's motion is synchronized with the Earth instead of the Sun. A satellite is visible in the same position at any time from a specific Earth location. This type of orbit is typically implemented at high altitudes, beyond LEO and MEO. Two special cases of geosynchronous orbits are Geostationary and Tundra orbits. In Geostationary a satellite appears as a fixed point in the sky for an observed. In Tundra orbits, the orbital period is one sidereal day, but the orbit is highly eccentric.

b) **Sub-synchronous orbits**:

   i) **12-hour semi-synchronous orbits**: These orbits are geosynchronous in which the rotational period is half the Earth's. This means that a satellite can be seen twice a day at the same location.

   ii) **Molniya orbits** [157]: Molniya orbits are highly elliptical orbits with an inclination of exactly 63.4° degrees, an argument of perigee of 270°, and an orbital period of approximately 12 hours. These particular orbits give much better coverage at high altitudes (beyond LEO and even MEO).

4.3.3 Constellation Topology

The constellation pattern on the sky directly influences the choice of the number of satellites needed to achieve certain performance targets. There are currently many constellation topologies in the literature. Some of the most typically studied are:

a) **Walker constellation** [142, 158]: There are two main types of Walker constellation: i) Walker Star [148] and ii) Walker Delta [147] (also called Ballard Rosette). Walker constellations are by far the most encountered constellation types, based on symmetrical circular orbits (i.e., orbital planes) around the Earth, all having the same inclination and the same eccentricity. In Walker Star [150] constellations, all the orbits cross near the Earth's poles, and if the orbit lines are viewed from one of the Poles, the intersection of the orbital planes produces a star shape. The orbital planes are evenly spaced along with the Earth, and half of them are counter-rotating (i.e., in half of the orbital planes, the satellites are moving away from the north pole, and the other half are moving towards the north pole). Walker Delta [150] constellations are similar to a Walker Star but more generalized than just considering the polar case and the total set of satellites are evenly distributed in each orbital plane.

   The Walker configuration is mainly characterized by $T/P/F$ parameters, where T represents the total number of satellites in the constellation, P is the total number of orbital planes and F is the relative spacing between satellites in adjacent planes. Besides these three main parameters describing the Walker orbit, other important parameters are the eccentricity, the inclination, and the orbital altitude.

   For example, Galileo MEO constellation is based on Walker Delta orbits, providing continuous Earth coverage of at least four satellites. Some LEO systems using Walker constellations are OneWeb [84] and Iridium [159]. It is important to remark that although the orbit is circular, the real eccentricity of the satellites is not typically exactly zero, due to the atmospheric drag in the trajectories (e.g. eccentricity is about $e = 0.00015$ for the satellites in OneWeb and Iridium constellations).

b) **Elliptical-orbit constellation** [160, 161]: Elliptical orbits are also known as HEO. Elliptical orbits are very similar to a Walker constellation, but the satellite orbits depict an ellipse shape instead of a circular one. Each elliptical orbit is defined by a semi-major axis parameter a, typically equal to the Earth radius plus the orbit altitude, and a semi-minor axis b. The eccentricity $e \triangleq \sqrt{1-\left(\frac{b}{a}\right)^2} \in [0,1)$ measures the flatness of the orbit (the higher e, the 'flatter' the ellipse). Walker orbits are particular cases of elliptical orbits with

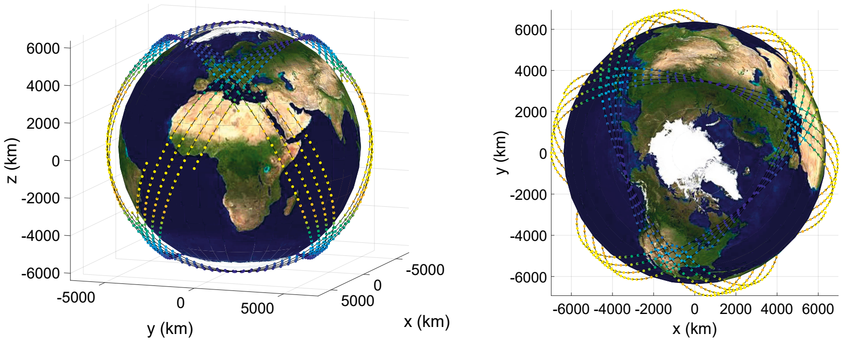
$e = 0$. A particular case of such elliptical orbits is the Molniya orbit. Elliptical orbits can also be divided into polar orbits and inclined (prograde or retrograde) orbits, similar to Walker orbits. Circular orbits typically offer better Earth coverage than the elliptical ones (especially in terms of symmetry), and therefore seem more promising in the LEO-PNT context. Although elliptical orbits may achieve better efficiency in terms of the total impulse to launch a satellite in orbit than circular orbits at LEO altitudes [162]. An example of a satellite constellation using an elliptical orbit is the Sirius Satellite Radio (currently Sirius XM Radio) [163].

c) **Flower constellation** [142, 149, 164]: This is a type of constellation whose orbit relative to the Earth-Centered Earth-Fixed (ECEF) coordinates framework resembles to flower petals. By choosing different orbits in a flower constellation, one can optimize each orbit to a particular latitude region (e.g., equatorial, polar, etc.) in such a way that the sum of the orbits will cover the whole Earth according to specific target metrics. Flower constellations depend on five independent parameters: the number of petals N_{pt}, the number of days duration of an orbit N_d, the angular velocity of the rotating reference frame ω, the orbit eccentricity (or the perigee altitude) e, and the orbit inclination i.

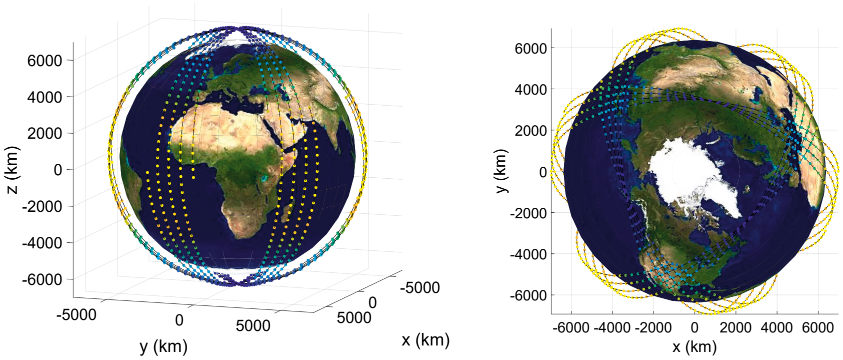
d) **Street-of-coverage constellation** [150]: Street-of-coverage refers to multiple circular orbits, with the same orbital centers placed at exactly the same altitude. It is similar to a Walker constellation, but in which the orbital planes are unevenly spaced.

Figure 4.4 shows an example of the Walker Delta, Walker star, and Flower constellation. 12 satellites in 3 orbital planes are depicted, with an inclination of 60, 90, and 80 for Walker Delta, Walker Star, and Flower, respectively. In Figure 4.4f we observe the flower petal shape of the Flower constellation.

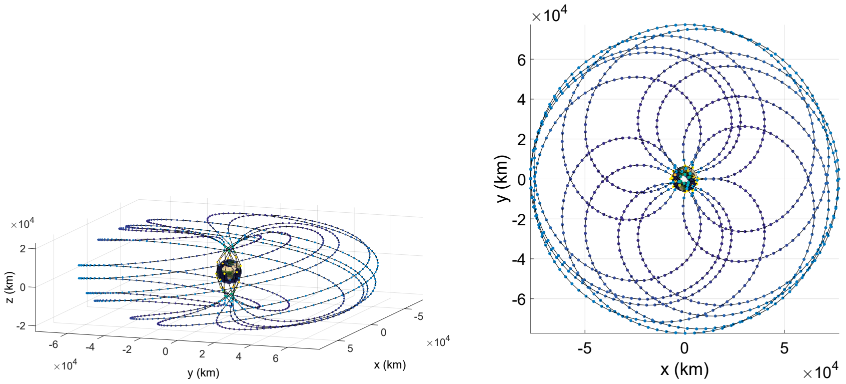
According to the classification criteria given above, the current MEO GNSS constellations use circular, semi-synchronous, prograde, and inclined orbits. In LEO systems, the most common is to find LEO constellations using circular, polar, prograde, and semi-synchronous orbits. But by analogy with GNSS MEO constellations, we believe that a well-suited orbit type for LEO-PNT would be also a circular, prograde, and semi-synchronous orbit. Such a choice would offer the constellation



(a) Walker Delta **(b)** Walker Delta XY-view



(c) Walker Star **(d)** Walker Star XY-view



(e) Flower **(f)** Flower XY-view

Figure 4.4 Topology examples for a constellation with 12 satellites and 3 orbital planes. The inclination is 60, 90, and 80 for Walker Delta, Walker Star, and Flower, respectively.

the symmetry needed for uniform coverage, synchronicity in the visible satellites, and a lower launching cost rather than other more complex orbit types.

4.4 Orbit Perturbations

Satellite orbits are highly influenced by the atmosphere and gravity. The main perturbations affecting the orbit of a satellite are: the Earth being a non-perfect sphere (also called Earth oblateness), the atmospheric drag, and the gravitational pull of astronomical bodies (e.g., the Sun, Moon, etc.), and the solar radiation pressure [165]. Nonetheless, in LEO, the main perturbations to consider are the Earth's oblateness and atmospheric drag. These two effects are directly affected by the altitude of the orbit with respect to the Earth.

4.4.1 Earth Oblateness Perturbation

The Earth is an oblate rather than a perfect sphere, in which the equatorial radius is about 21 km larger than the polar radius. This flattening at the poles provokes small perturbations in the orbits, such as the precession of ascending node, drifts in the argument of perigee and the mean anomaly, etc [166].

4.4.2 Atmospheric Drag

The atmospheric drag is caused by impact between the particles in the Earth's atmosphere with the satellite surface [165, 167]. The atmospheric drag force F_{Drag} can be computed as

$$\mathrm{F_{Drag}} = -\frac{1}{2} C_d S \rho V_r^2, \tag{4.1}$$

where C_d is the drag coefficient (considered as constant and typically between 2 and 3, being a common value of 2.2), S is the reference area of the satellite (usually the projected area of the satellite normal to the velocity vector), ρ is the air density at the satellite altitude, and V_r is the relative speed between satellite and the particles composing the atmosphere. Figure 4.5 shows the drag force experienced by a satellite as a function of the orbit altitude. We can see that the drag force is especially noticeable at low LEO altitudes (< 600 km), while at high altitudes (> 800 km) is barely noticeable. In the example depicted in Figure 4.5, V_r was modeled the atmosphere speed as the Earth's rotation speed and ρ was computed as the annual average atmospheric density using MSIS-86 model [168]. The reference area of the satellite was taken as 20 m (modeling it as a rectangle, with a wingspan of 10 meters and 2 meters altitude).

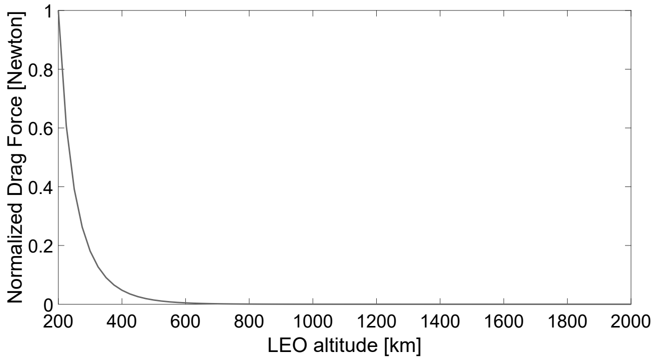


Figure 4.5 Normalized drag force experienced by a satellite in orbit as a function of the altitude.

4.5 Tackling LEO-PNT: Numerical Evaluations and Results

In this section, we provide an overall look at how could LEO-PNT service be addressed. On the one hand, we could re-use partially or even completely the existing or planned LEO constellations, even though their purpose is different than positioning (e.g., communications, Earth Observation (EO), etc). Employing signal processing techniques, one can use signals for a different purpose than the initially planned one. This is called SoO [169, 170, 171]. This approach would drastically reduce the economic cost of developing and maintaining a completely new PNT-dedicated LEO constellation. The main drawback of this approach is that the control of the constellation is kept by the companies and organizations owners of the constellation. Therefore, any change in the signal design, frequency bands of operation, continuity of the constellation in the sky, etc may affect the performance or even be unable to continue offering positioning from these signals. One step more could be including dedicated PNT payload to future LEO constellations or even future LEO satellites to be launched. This would increase the price with respect to using the LEO signals as SoO since the dedicated payload needs to be designed and launched with the future satellites to be put in orbit. Although it would be still much more affordable than a completely new and PNT-dedicated constellation. On the other hand, a new constellation can be developed from scratch, emphasizing PNT service during its design. This would of course be the most expensive approach, but the entity in charge of the constellation will have full control of the constellation, from the early design to the future maintenance and viability. By this, we would assure that the LEO-PNT constellation is fully optimized from the point of view of the positioning service.

With this in mind, this section provides simulations from two ends: i) analyzing which configuration a dedicated LEO-PNT constellation should have (e.g., number of satellites, orbital planes, orbit altitude, etc); ii) making a feasibility study of different launched or planned LEO constellations for being used as SoO. In this study, besides some LEO constellations we have also included some MEO constellations, as they are the benchmark and reference constellations for any future LEO-PNT.

We will first analyze and compare the minimum coverage needed and the coverage provided by the different satellite constellations, from the point of view of the average number of satellites in view. Then, we will analyze the DoP of the different constellations, which shows the degree of accuracy in positioning a certain system (in this case a satellite constellation) can provide. In particular, we will focus on the GDoP, which is a metric that can be related to both the coverage and the maximum achievable positioning accuracy that a certain positioning system can offer. GDoP illustrates how well geometrically distributed are the transmitters (e.g., relative geometrical distribution of the satellites with respect to a certain user). But we will also include some other DoP metrics such as PDoP, TDoP, HDoP and VDoP. Finally, we will analyze the link budget for different constellations, analyzing the path loss, received SNR and received C/N_0 in both outdoor and indoor scenarios.

The main parameters of the analyzed constellations, namely Astrocast, BlackSky Global, Galileo, Globalstar, GPS, ICEYE, Iridium, Kuiper, Myriota, OneWeb, Starlink, and Telesat are summarized in Table 4.3 and Table 4.4. Table 4.3 summarizes the global view of each constellation, showing the orbit altitude according to Section 4.3.2.1, the typical mass of the satellites used in the constellation, the total number of satellites and orbital planes in the final constellation, the typically used frequency band for downlink (e.g., L-band, S-band, Ku-band, etc.) and the purpose of the constellation (e.g., NB/BB communications, IoT applications, PNT, etc.). For

Table 4.3 General parameters for the analyzed constellations. IoT = Internet-of-Things (IoT), EO = Earth Observation (EO), PNT = Pseudo Navigation and Timing (PNT), NB = Narrow Band (NB) and BB = Broadband (BB).

Constellation Name	Orbit Altitude	Sat. Mass [kg]	# Sat.	# Planes	Freq. Band	Purpose	Ref.
Astrocast†	LEO	5	80	10	L	IoT	[172]
BlackSky Global†	LEO	56	60	10	X	EO	[173]
Galileo	MEO	700	27	3	L	PNT	[174, 175]
Globalstar 2nd Gen	LEO	700	24	6	L/S	NB	[176]
GPS	MEO	1600	30	6	L	PNT	[177]
ICEYE†	LEO	85	18	6	X	EO	[178, 179]
Iridium Next	LEO	860	66	6	L	NB	[180]
Kuiper†	LEO	250	7774	1173	Ku/Ka	BB	[181, 182]
Myriota†	LEO	5	26	18	UHF	IoT	[183]
OneWeb†	LEO	386	7808	100	Ku/Ka	BB	[184]
Starlink†	LEO	145	34404	478	Ka/Ka	BB	[185, 186]
Telesat†	LEO	≈700	1671	67	Ka/Ku	BB	[187]

† The parameters shown in the table are based on the latest information publicly available, corresponding to the planned final constellation (status Feb 2022).

its part, Table 4.4 summarizes the main orbital parameters that uniquely identify each selected constellation. Table 4.4 shows the constellation topology as described in Section 4.3.3, the orbit altitude in km, the number of satellites in each orbital plane, the number of independent orbital planes, the inclination in degrees of each orbital plane, and the typical Effective Isotropic Radiated Power (EIRP) in dBm. Table 4.4 is read as follows: Telesat constellation follows a Walker Star topology, with 2 independent orbit altitudes, 1015 km and 1325 km. At 1015 km it contains 351 satellites split into the 27 orbital planes (13 satellites in each orbital plane), with an orbital plane inclination of 98.98°. At 1325 km it contains 1320 satellites split into the 40 orbital planes (33 satellites in each orbital plane), with an orbital plane inclination of 50.88°. Analogously, for the remaining constellations, if more than one parameter exists (e.g., altitude), the parameter order is consecutive.

Table 4.4 Orbital parameters for the analyzed constellations.

Constellation Name	Const. Topology	h [km]	Total # of Satellites	Orbital Planes	i [deg]	EIRP [dBm]
Astrocast†	N/A	530	80	10	97.5	40
BlackSky Global†	N/A	550/585	30/30	5/5	97.6/97.77	40
Galileo	Walker Delta	23222	27	3	56	59
Globalstar 2nd Gen	Walker Star	920	24	3	52	56.8
GPS	Walker Delta	20200	30	6	55	59
ICEYE†	Walker Star	570	18	6	97.7	65
Iridium Next	Walker Star	730	66	6	86.4	67
Kuiper†	Walker Star	590/610	784/1296	28/36	33/42	76
		630/590	1156/784	34/28	51.9/33	
		610/630	1296/1156	36/34	42/51.9	
		640/650	652/650	652/325	72/80	
Myriota†	N/A	530	10/4/12	10/2/6	54/54 97.7	33.3
OneWeb†	Walker Star	1200	720/588	18/12	87.9/87.9	65
			128/1764	8/36	55/87.9	
			2304/2304	32/32	40/55	
Starlink†	Walker Star	550/540	1584/1584	72/72	53/53.2	69.1
		570/560	720/348	36/6	70/97.6	
		560/340	172/5280	4/48	97.6/53	
		345/350	5280/5280	48/48	46/38	
		360/525	3600/3360	30/28	96.9/53	
		530/535	3360/3360	28/28	43/33	
		604/614	144/324	12/18	148/115.7	
Telesat†	Walker Star	1015	351/1320	27/40	98.98	69
		1325			50.88	

† The parameters shown in the table are based on the latest information publicly available, corresponding to the planned final constellation (status Feb 2022).

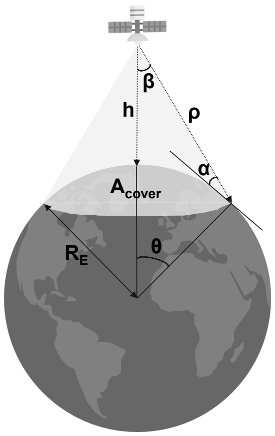
The constellations shown in Table 4.4 were simulated in MATLAB using the Satellite communication Toolbox (available from MATLAB r2021a). For propagating the satellite orbits we used an SDP4 deep space perturbation model, in which perturbation effects such as Earth oblateness and atmospheric drag are considered. In all the performed simulations, we used 10^4 Monte Carlo runs, each one containing a random user position along with the Earth, in order to average the obtained results. The coverage per constellation was measured as the number of satellites in view with a minimum elevation of 10° from the user position. The average number of satellites in view $\overline{\#Sat}$ averages the satellites in the view over the 10^4 Monte Carlo runs. Specific details about how DoP and link budget are measured, as well as the obtained results, can be found next.

4.5.1 Constellation Coverage Considerations

The satellite coverage area is defined as the region of the Earth where a single satellite is seen at a certain minimum elevation angle defined by the system/application (e.g. typically 10° in GNSS). This coverage area depends on the satellite orbit design of the specific constellation. Figure 4.6 illustrates a simplified approach to computing a coarse approximation of the coverage area A_{cover} on Earth for a certain satellite. The satellite is assumed to be placed at an altitude h from the Earth's surface, and it has a minimum elevation angle (or elevation mask) α (below this elevation mask, the satellite is no longer 'seen', as it will go below the horizon). The ρ edge represents the slant range and R_E denotes the Earth radius. From Figure 4.6 and generalized Pythagoras formulas we can obtain:

$$\begin{aligned}
\rho &= -R_E \sin(\alpha) + \sqrt{R_E^2 \sin^2(\alpha) + 2R_E h + h^2}, && (4.2)\\
\beta &= \sin^{-1}\left(\frac{R_E}{(R+h)} \cdot \sin(\alpha)\right), && (4.3)\\
\theta &= \cos^{-1}\left(\frac{R_E}{(R+h)} \cdot \sin(\alpha)\right) - \alpha, && (4.4)\\
\mathrm{A}_{\mathrm{cover}} &= 2\pi(1-\cos\theta), && (4.5)
\end{aligned}$$

where ρ is the slant range, θ is the cap angle, α is the elevation mask, β is the Off-Nadir angle, h is the satellite altitude, A_{cover} is the Earth's area covered by the satellite and R_E is the Earth's radius, as depicted in Figure 4.6.



Parameter	Description
β	Off-Nadir angle
ρ	Slant range
α	Elevation angle
θ	Cap angle
h	Satellite altitude
A_{cover}	Area covered
R_E	Earth's radius

Figure 4.6 Illustrative example of coverage per satellite, showing the main geometric aspects.

From Equation (4.2), Equation (4.3), Equation (4.4) and Equation (4.5) we can define the minimum constellation size and minimum orbit inclination providing global Earth's coverage. We can define the minimum orbital inclination as [188]

$$i_{min} = \max(\Phi_{max} - \theta, 0), \tag{4.6}$$

where the cap angle θ is given in Equation 4.4 and i_{min} is the minimum inclination angle (in degrees), Φ_{max} is defined as $max(|\phi_l|, \phi_u)$, with ϕ_l and ϕ_u being the minimum and maximum latitudes within the coverage area, respectively. For full Earth coverage from $-90°$ to $+90°$ latitudes, $\Phi_{max} = 90°$.

The number of planes is typically chosen as a trade-off between the desired coverage and constellation complexity. The more orbital planes (and satellites in orbit) the constellation has, the most coverage is typically provided. The minimum number of orbits to give global coverage can be computed as

$$\mathrm{N}_{\mathrm{minPlanes}} = \frac{360}{2\theta}, \tag{4.7}$$

where θ is the cap angle in degrees shown in Figure 4.6.

Finally, we can compute the minimum number of satellites in the constellation as [189]

$$\mathrm{N}_{\mathrm{minSV}} = \frac{2K}{(1 - \cos(\theta))}, \tag{4.8}$$

where K is the desired K-fold coverage (i.e. K=1 for at least 1 satellite in view in any Earth's location and time instant, K=4 for at least 4 satellites in view, etc).

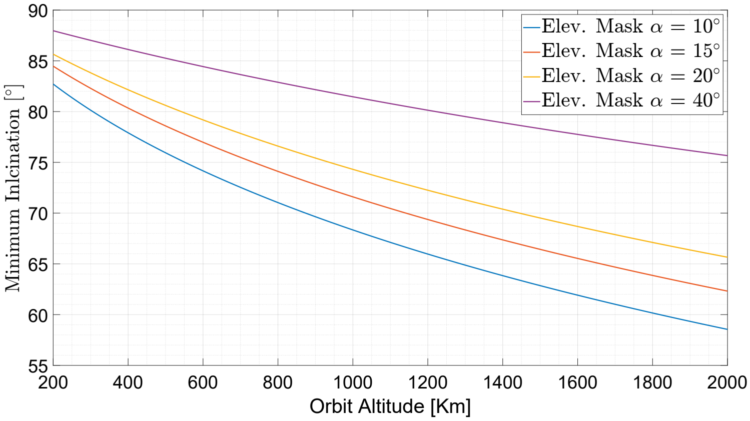
Figure 4.7a depicts the minimum orbit inclination as a function of the orbit altitude for four different elevation mask angles. Figure 4.7a shows that the minimum orbit inclination range for LEO constellations with the provided minimum elevation masks must be between 55° (high orbit altitudes) and 88° (low orbit altitudes) to achieve global coverage. Figure 4.7b depicts the minimum number of orbital planes a constellation must have with four different minimum elevation mask angles to achieve global coverage. Figure 4.7b shows that the minimum number of orbital planes to achieve global coverage must comprise between 85 and 10 orbital planes, depending on the orbit altitude and minimum required elevation mask. Finally, Figure 4.7c shows the minimum number of satellites in orbit a constellation must have to provide 4-fold coverage. Figure 4.7c shows that depending on the minimum required elevation, the minimum number of satellites must comprise between a few hundred (higher LEO altitudes) to a few thousand (lower LEO altitudes). Notice that is important noticeable the effect of the minimum elevation mask in the final constellation complexity. As higher the elevation mask is, the more dense the constellation should be.

In order to define more clearly how the expected LEO-PNT constellation should be in terms of minimum orbit inclination, the minimum number of orbital planes, and the minimum number of satellites, we have carried out an optimization procedure based on these findings and the expected perturbations according to the orbit altitude (for more details check Section 4.4).

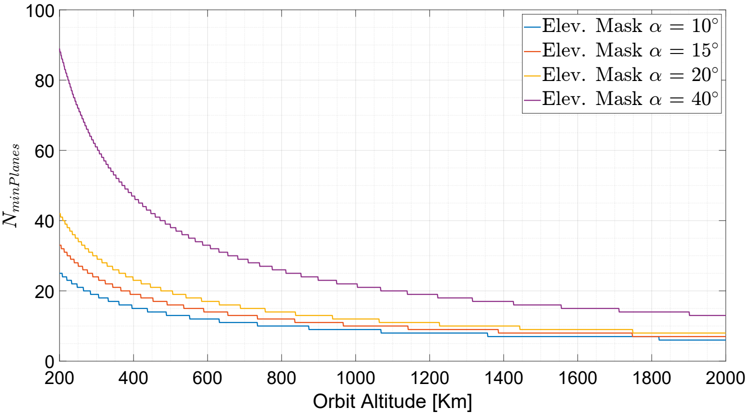
We used the four normalized optimization cost functions described in Equation (4.9) to Equation (4.12).

$$\mathrm{Cost1} = \frac{\mathrm{N_{minSV}}}{\max(\mathrm{N_{minSV}})}, \tag{4.9}$$

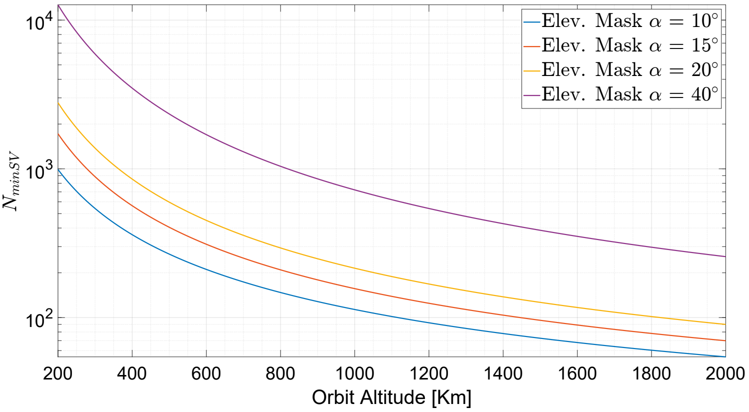
where $\mathrm{N_{minSV}}$ is a vector containing the minimum number of satellites needed to provide global coverage for different LEO orbit altitudes, such as shown in Figure4.7c. $\max(\mathrm{N_{minSV}})$ corresponds to the largest number of satellites needed to provide global coverage over all considered orbit altitudes (typically, this maximum occurs at the



(a) Minimum orbit inclination



(b) Minimum number of orbital planes



(c) Minimum number of satellites for 4-Fold coverage

Figure 4.7 Example of minimum orbital inclination, the minimum number of orbital planes, and the minimum number of satellites as a function of the orbit altitude for three required minimum elevation masks (α=10°, α=15°, α=20°), and α=40°.

lowest LEO altitude) for a specific minimum elevation mask.

$$\mathrm{Cost2} = \frac{C/N_0}{\max(C/N_0)}, \tag{4.10}$$

where C/N_0 is a vector containing all the C/N_0 measured at the receiver after the transmission through the wireless channel (which is described in Section 4.5.4). $\max(C/N_0)$ represents the maximum received C/N_0 over all the considered altitudes (typically, this minimum also occurs at the lowest LEO altitude).

$$\mathrm{Cost3} = \frac{\mathrm{CRLB}_{\mathrm{trackvar}}}{\max(\mathrm{CRLB}_{\mathrm{trackvar}})}, \tag{4.11}$$

where $CRLB_{trackvar}$ is a vector containing the Cramer-Rao Lower Bound [190, 191] values of the position when distance estimates are based on time-of-arrival estimates for all considered orbit altitudes. $CRLB_{trackvar}$ depends on the geometry of the satellites, the available receiver bandwidth, and the received C/N_0. It is a measure of how good accuracy one can achieve in positioning. The value $\max(CRLB_{trackvar})$ corresponds to the highest $CRLB_{trackvar}$ over all the considered orbit altitudes.

$$\mathrm{Cost4} = \frac{F_{Drag}}{\max(F_{Drag})}, \tag{4.12}$$

where F_{Drag} is the drag force experienced by the satellites, and can be computed using Equation (4.1) (check Section 4.4 for more details).

The overall cost function for optimization is defined as the sum of all normalized cost functions described in Equation (4.9)-(4.12), taking into account if they need to be minimized (Cost1, Cost3 and Cost4) or maximized (Cost2):

$$\mathrm{Cost_T} = Cost1 + \frac{1}{Cost2} + Cost3 + Cost4, \tag{4.13}$$

Figure 4.8 shows three different curves, based on three different carrier frequencies in the optimization cost functions by using Equation (4.13). Each curve corresponds to a different carrier frequency used in the transmitter, namely 1 GHz, 3 GHz, 10 GHz, and 30 GHz. A transmitter power of 32 W, transmitter and receiver gain of 10 dB and 24 dB, respectively, and a receiver bandwidth of 5 MHz was used in this simulation. Regarding the channel scenario, an outdoor LoS condition

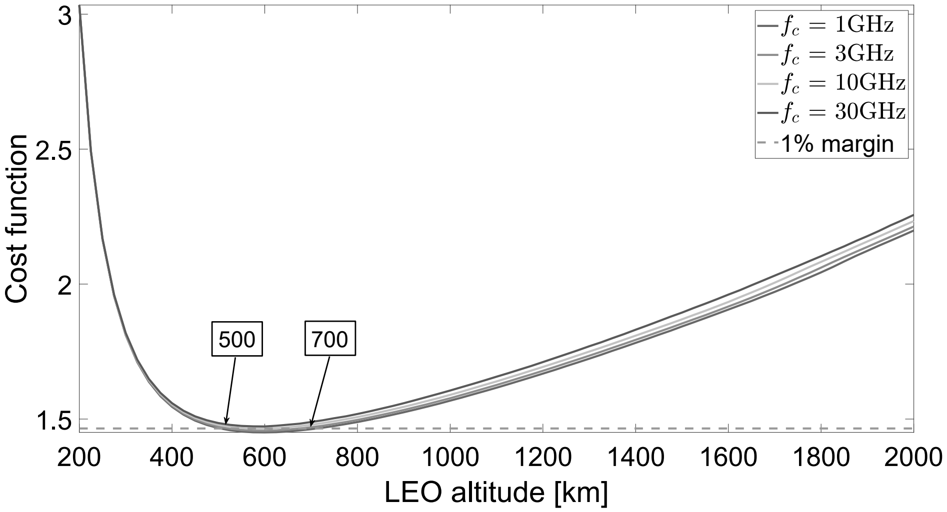


Figure 4.8 Illustrative example of optimization output using the four cost functions and four different frequency bands: 3 GHz, 5 GHz, and 30 GHz. Minimum elevation mask is 10°

was selected.

As we can see in Figure 4.8, for all four frequency bands, the results look very alike in terms of optimal orbit altitude range. The optimal altitude given by the optimization in Equation (4.13) is approximately 600 km. We have included a 1% margin in order to consider non-idealities such as variations in the de-orbiting time, Doppler effects, etc. With this 1% margin, the optimal altitude range is approximately between 500 km to 700 km. Comparing Figure 4.8 with Figure 4.5, the minimum in the total cost function matches with the altitude where the drag force starts to be not as strong as at lower orbits.

To conclude this section, once we have evaluated the optimal altitude according to our cost function, we can further determine the minimum orbit inclination, the minimum number of orbital planes, and the minimum number of satellites by just looking at Figure 4.7. By doing so we can state that the optimal constellation fulfilling our optimization (and considering a minimum elevation mask of 10° and a 4-fold coverage) is composed of 216 satellites distributed in 12 orbital planes with a minimum orbit inclination of about 75°-85°.

4.5.2 Coverage Comparison Between LEO and MEO Constellations

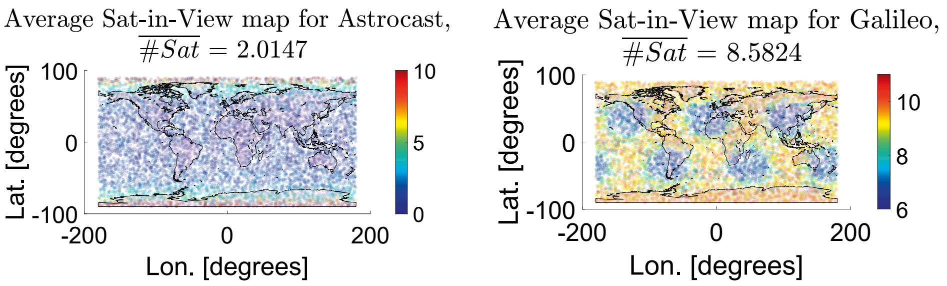
In this subsection, an analysis of the different analyzed constellations is provided. Figure 4.9 depicts the coverage maps for the above-mentioned constellations. For the sake of simplicity, 8 out of 12 constellations have been depicted, as the most representatives for each LEO and MEO category. At first, sight, looking at Figure 4.9 we can observe as there is a huge difference between the average number of satellites in view offered by regular-sized satellite constellations (e.g., Galileo, Iridium, etc.) and mega-constellations (e.g., OneWeb, Starlink, etc). In the case of regular-sized constellations, we observe as the mean number of satellites in view $\overline{\#Sat}$ is below 10 (for the selected MEO constellations), which is below the minimum number of satellites in view required for positioning (which is 4, as we have to solve a system of equation with 4 unknowns, the 3-D user coordinates and time). On the contrary, in the analyzed mega-constellations we observe that the average number of satellites in view $\overline{\#Sat}$ is between 70 and 370 satellites, which is much larger than the minimum needed for positioning. Analyzing the results depicted in Figure ?? constellation by constellation, we observe that Astrocast, ICEYE, and Iridium would not be suitable for positioning purposes because the average amount of satellites-in-view is below the minimum of 4. For its part, Galileo, which has the advantage of orbiting at much higher altitudes with respect LEO constellations (more than 20000 km above) offers an average amount of satellites-in-view of ≈ 8 with a much lower amount of satellites in the constellation. The results obtained for Galileo can be extrapolated to GPS. When it comes to Kuiper, OneWeb, Starlink, and Telesat, the coverage offered is hundreds of satellites in view at any time. This is due to the huge amount of satellites in orbit these constellations have. From analyzing the coverage maps in Figure 4.9, we can state that not all the constellations provide the same level of coverage at all latitudes. Depending on the inclination, the number of orbital planes, and the number of satellites (check Table 4.3 and Table 4.4 for more details), the constellations provide higher coverage at the equator or nearby the poles. For example, OneWeb and Iridium, whose satellite inclination is nearly-polar (for at least some of the orbital planes), provide higher coverage at high latitudes (e.g., latitudes higher than 80°) than some other constellations such as Starlink or Telesat. The latest provide better coverage in the equatorial region (e.g., mid and low latitudes). The reason is that the higher the orbit inclination is, the higher the coverage is at the poles.

Therefore, OneWeb or Iridium concentrates a larger amount of satellites in orbit at high (polar or nearly-polar) inclinations, while Starlink or Telesat concentrates the satellites at much lower inclinations.

The coverage maps depicted in Figure 4.9 were obtained considering a full orbit period (approximately 2 hours for LEO and 12 hours for MEO constellations). But the coverage provided by a certain constellation at a specific time can differ from the values depicted in Figure 4.9. Especially for those constellations with a low number of satellites in the sky (e.g., ICEYE). Figure 4.10 and Figure 4.11 shows an example of this. we can see as in Figure 4.10, which corresponds to a small constellation (ICEYE has 18 satellites) the global coverage provided by the constellation at the two-time instants is different. At time instant t= 1 s the satellites are spread approximately symmetrically close to the poles and at the equator. For this reason Figure 4.10a shows big green circles at the equator and at high and low latitudes, but no coverage at mid-latitudes. These green areas correspond to those red dots in Figure 4.10b, which represent the satellite position. At time instant t= 15 min, the position of the satellite has considerably changed as can be seen in figure Figure 4.10d in comparison with Figure 4.10b. Looking at Figure 4.10c we observe as the coverage areas again correspond to those areas where the satellites are located, and therefore are in view. On the contrary, for bigger constellations such as Telesat, this phenomenon is not so noticeable, as is shown in Figure 4.11. In both Figure 4.11a and Figure 4.11c the provided coverage is pretty similar. In addition, Figure 4.11b and Figure 4.11c shows that even though the satellites have moved with time, given the huge amounts of satellites in the constellation the coverage provided is kept almost constant. This fact is not important for the ICEYE constellation. ICEYE's main objective is Earth observation, therefore it must cover the whole Earth but there is no need to give full coverage at any time instant. Although Telesat must provide global coverage at any time instant to provide reliable broadband service. From the point of view of positioning, the constellation must provide global coverage at any time to be able to rely on the signals at any time instant and not only when the satellites are in view.

4.5.3 Dilution of Precision (DoP) Analysis

DoP measurements can be expressed as [70]: i) HDoP – Horizontal DoP; ii) VDoP – Vertical DOP; iii) PDoP – Position (3D) DoP; iv) TDoP – Time DoP; and v) GDoP

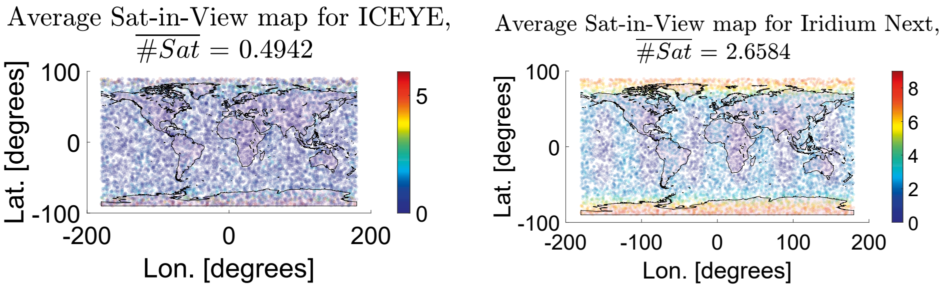


Average Sat-in-View map for Astrocast, $\overline{\#Sat} = 2.0147$

Average Sat-in-View map for Galileo, $\overline{\#Sat} = 8.5824$

(a) Astrocast

(b) Galileo

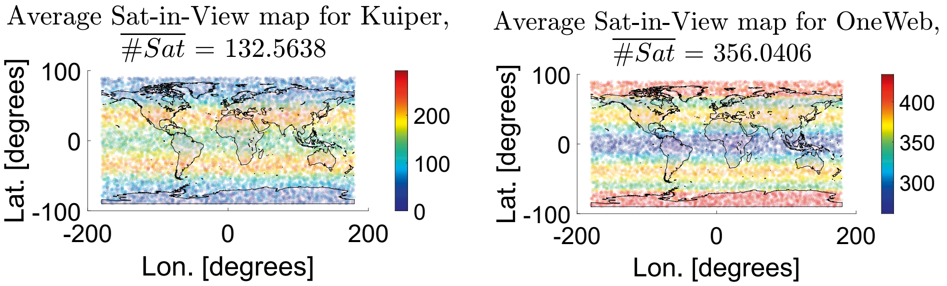


Average Sat-in-View map for ICEYE, $\overline{\#Sat} = 0.4942$

Average Sat-in-View map for Iridium Next, $\overline{\#Sat} = 2.6584$

(c) ICEYE

(d) Iridium Next

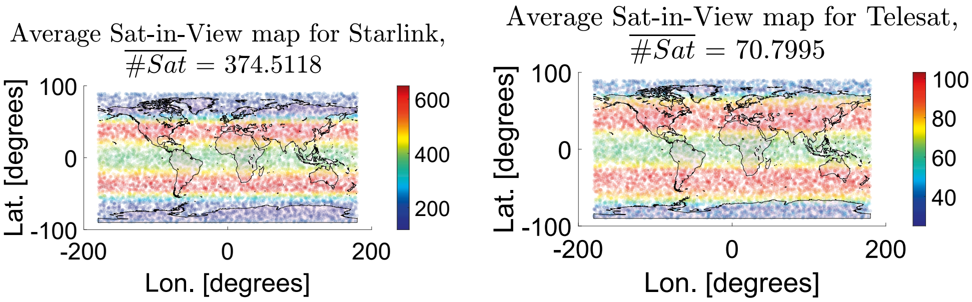


Average Sat-in-View map for Kuiper, $\overline{\#Sat} = 132.5638$

Average Sat-in-View map for OneWeb, $\overline{\#Sat} = 356.0406$

(e) Kuiper

(f) OneWeb



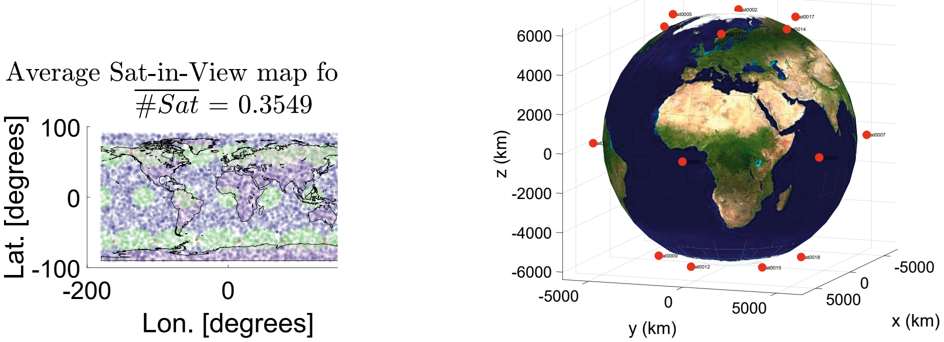
Average Sat-in-View map for Starlink, $\overline{\#Sat} = 374.5118$

Average Sat-in-View map for Telesat, $\overline{\#Sat} = 70.7995$

(g) Starlink

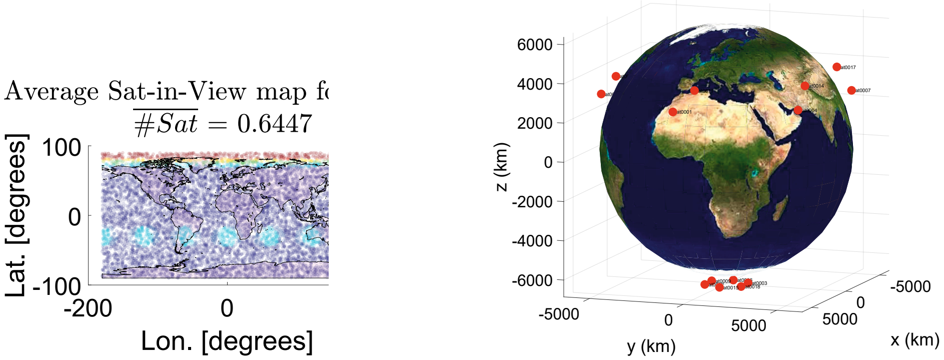
(h) Telesat

Figure 4.9 Coverage and the average number of satellites-in-view for eight different constellations: a) Astrocast (LEO, small); b) Galileo (MEO); c) ICEYE (LEO, small); d) Iridium (LEO, small); e) Kuiper (LEO, mega); f) OneWeb (LEO, mega); g) Starlink (LEO, mega); h) Telesat (LEO, mega).



(a) ICEYE coverage at t=1 s

(b) ICEYE satellite position at t=1 s



(c) ICEYE coverage at t=15 min

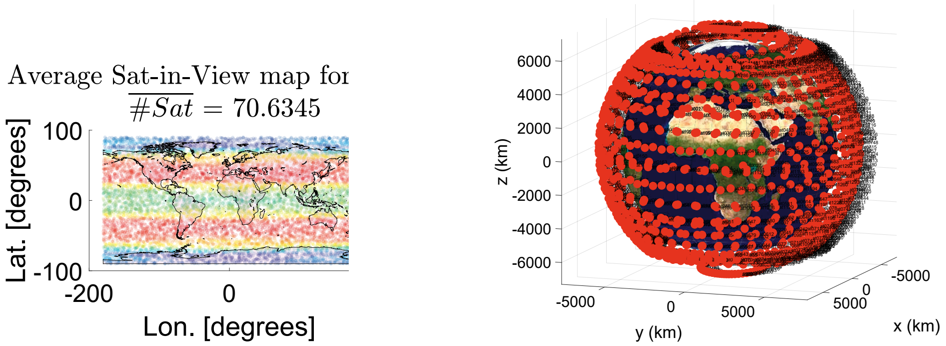
(d) ICEYE constellation on the sky at t=15 min

Figure 4.10 Example of ICEYE coverage and satellite position at two different time instants (1 second and 15 min).

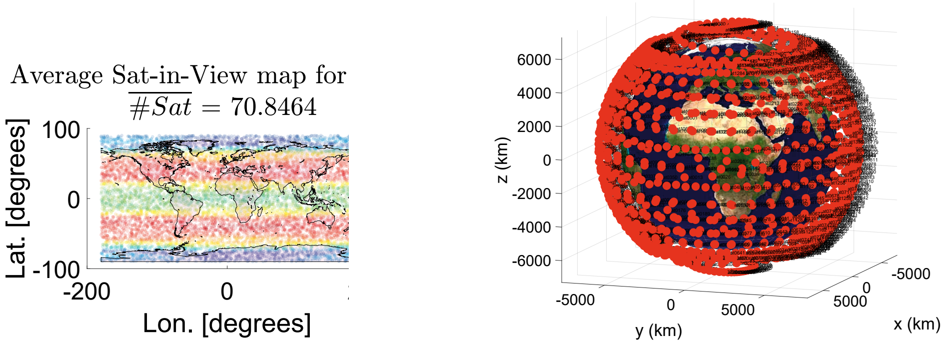
– Geometric DoP. The DoP measurements can be computed from the measurement matrix $\mathbf{Q}$, which is computed as:

$$\mathbf{Q} = (\mathbf{H}^{\mathrm{T}}(\Sigma_{\mathrm{all}})^{-1}\mathbf{H})^{-1} = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \sigma_{13} & \sigma_{14} \\ \sigma_{21} & \sigma_{22} & \sigma_{23} & \sigma_{24} \\ \sigma_{31} & \sigma_{32} & \sigma_{33} & \sigma_{34} \\ \sigma_{41} & \sigma_{42} & \sigma_{43} & \sigma_{44} \end{bmatrix}, \tag{4.14}$$

where $\mathbf{H}$ is a matrix containing the K range or code measurement residuals. $\mathbf{H}$ is



(a) Telesat coverage at t=1 s **(b)** Telesat satellite position at t=1 s



(c) Telesat coverage at t=15 min **(d)** Telesat constellation on the sky at t=15 min

Figure 4.11 Example of Telesat coverage and satellite position at two different time instants (1 second and 15 min).

computed as

$$\mathbf{H} \triangleq \begin{bmatrix} h_{x1} & h_{y1} & h_{z1} & 1 \\ h_{x2} & h_{y2} & h_{z2} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ h_{xK} & h_{yK} & h_{zK} & 1 \end{bmatrix}, \tag{4.15}$$

where $h_{xi} = \dfrac{x_{si} - x}{R_i}$, $h_{yi} = \dfrac{y_{si} - y}{R_i}$ and $h_{zi} = \dfrac{z_{si} - z}{R_i}$ are the components of a unit vector from the receiver to the ith satellite. x_{si}, y_{si}, z_{si} are the ith satellite coordinates, x, y, z are the user coordinates and R_i is the pseudorange, defined as $R_i = \sqrt{(x_{si} - x)^2 + (y_{si} - y)^2 + (z_{si} - z)^2}$.

In Equation (4.14), Σ_{all} is a diagonal error covariance matrix containing the error variances (e.g., error due to clock synchronization, orbit perturbations, atmospheric effects, etc) from all K considered systems and from all N_k visible transmitters per system [192]. It is defined as $\Sigma_{all} = diag(\Sigma_1, \ldots, \Sigma_K)$ [192].

Finally, the DoP metrics can be measured using Equation (4.14) and Equation (4.15) as:

$$\mathrm{GDOP} = \sqrt{\sum_{i=1}^{K+3} \mathbf{Q}(i,i)} = \sqrt{PDOP^2 + TDOP^2}, \tag{4.16}$$

$$\mathrm{PDOP} = \sqrt{\sum_{i=1}^{3} \mathbf{Q}(i,i)}, \tag{4.17}$$

$$\mathrm{TDOP} = \sqrt{\sum_{i=4}^{4} \mathbf{Q}(i,i)}, \tag{4.18}$$

$$\mathrm{HDOP} = \sqrt{\sum_{i=1}^{2} \mathbf{Q}(i,i)}, \tag{4.19}$$

$$\mathrm{VDOP} = \sqrt{\sum_{i=3}^{3} \mathbf{Q}(i,i)}, \tag{4.20}$$

GDoP provides information about how good is the satellite orbit geometry for positioning. PDoP provides information about how good positioning error we are able to obtain. VDoP and HDoP measure how accurately the vertical and horizontal position can be achieved, respectively. Finally, TDoP measures how accurate the time measurements can be for the specific satellite constellation.

Figure 4.12 depicts the averaged DoP metrics, namely GDoP, PDoP, TDoP, HDoP and VDoP for 8 (7 LEO and 1 MEO) out of 12 most representative constellations listed in Table 4.3 and Table 4.4. The DoP averaging was performed over 10^4 random user positions. From Figure 4.12 we can see that among the depicted constellations, Astrocast and Iridium offer the worst performance in terms of DoP. Especially the PDoP is noticeably high being almost 20 and almost 10, respectively for Astrocast and Iridium. While GDoP is kept between 6-8 for both constellations. One of the reasons for such a low DoP performance is that both constellations were considered from the point of view of communications rather than positioning. Therefore these constellations might not offer a good geometry for positioning purposes, but their configuration is optimal for providing global coverage with the minimum number of satellites. For its part, Galileo, which is the only depicted MEO constellation with the main purpose of offering PNT service, provides a considerably low average GDoP < 5. Finally, as we could expect LEO mega-constellations, namely OneWeb, Starlink, Telesat and Kuiper offer the best performance in terms of DoP, mainly due to the huge amount of satellites in the sky, which offers a wide range of geometric diversity. But with one exception: the Kuiper constellation. Kuiper DoP, specially PDoP is relatively large compared with OneWeb or Starlink, being ≈ 10 and < 1, respectively, for Kuiper and OneWeb/Starlink.

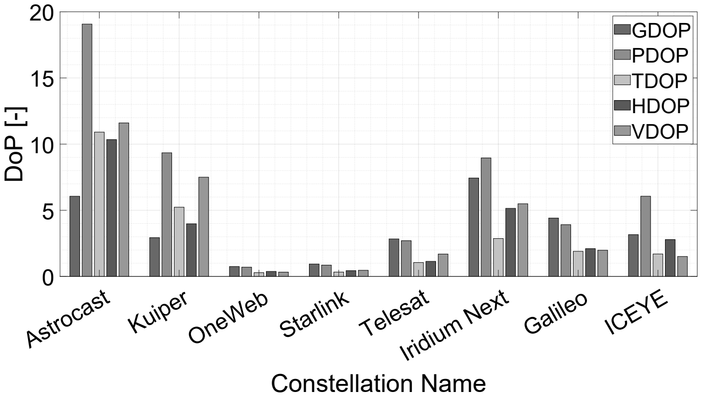


Figure 4.12 Barplot showing the average GDoP, PDoP, TDoP, HDoP and VDoP for the most representative 8 constellations (7 LEO and 1 MEO).

4.5.4 Link Budget Analysis

The link budget consists of the analysis of the received signal power strengths, in both uplink and downlink transmissions, by taking into account specific path-loss models in order to estimate the losses over the wireless channel during the transmission propagation as well as the maximum achievable C/N_0 for a specific system. In the positioning context though, the downlink propagation (from the satellite to the Earth receiver) is the one of interest in terms of positioning targets. Therefore the analysis regarding user performance is typically done in downlink since the receiver does not communicate much or at all with the satellites. Therefore, in this section, we will focus on the downlink transmission. Widely speaking, the received signal strength P_{Rx} depends on the transmitted signal strength P_{Tx} via

$$P_{Rx} = P_{Tx} + G - P_L, \tag{4.21}$$

where G is the sum of all gains in the transmission chain (e.g., transmitter and receiver antenna gains) and P_L is the cumulative path-loss over the wireless channel, which depends on the transmitter-receiver distance, on the carrier frequency f_c, on the various atmospheric effects (e.g., gaseous and rain absorption, tropospheric, and possible ionospheric absorption), and on the terrestrial scenario (e.g., absorption due to reflections, scattering effect, and refraction on buildings and trees, wall losses for indoor propagation, etc.). From Equation 4.21 we can compute the SNR (in dB) as

$$SNR = P_{Rx} - 10\log_{10}(N_0), \tag{4.22}$$

where N_0 is the receiver noise density defined as $N_0 = 10\log_{10}(kT)$, where k is the Boltzmann constant ($1.38 \cdot 10^{-21}$ J/Kelvin) and T is the receiver temperature in Kelvin. In GNSS applications, N_0 is typically considered to be −204 dBW/Hz (considering 290 Kelvin receiver temperature). Finally the received C/N_0 can be computed from SNR measurements as:

$$C/N_0 = SNR + 10\log_{10}(BW_{Rx}), \tag{4.23}$$

where BW_{Rx} is the receiver bandwidth in Hz.

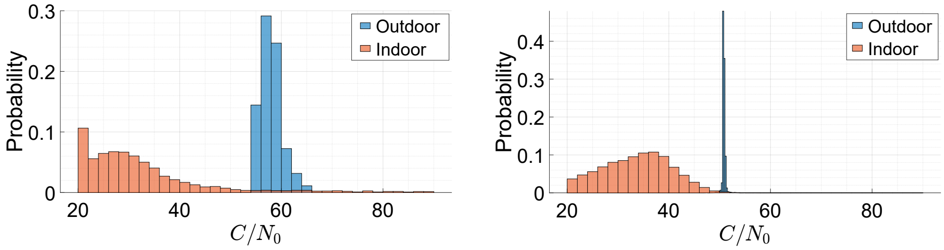
To model the channel and carry out the simulations in this section, we have used the QuaDRiGa [193, 194] framework. QuaDRiGa is a MATLAB-based software developed by Fraunhofer HHI that enables the modeling of radio wireless channels by generating realistic radio channel impulse responses for system-level simulations. It is very flexible, allowing the simulation of different layouts by just modifying a few parameters. In addition, QuaDriga offers the possibility to modify both transmitter and receiver positions, including movement profiles. In addition, it allows one to choose among different antenna type models, customize the scenario to simulate, etc. The specific available downlink channel models are described in detail in [195]. The scenarios contain rural, suburban, urban, and dense urban models, as well as LoS and NLoS propagation conditions.

In the simulations shown in this section, we considered an urban scenario in both outdoor and indoor analysis. The considered urban channel model consists on 10 channel paths components (containing LoS and NLoS), with scatters at distances between 0.1 m and 200 m, with an altitude up to 30 m, as described in [195]. In the indoor scenario, we considered that the receiver was at approximately 10 m indoors.

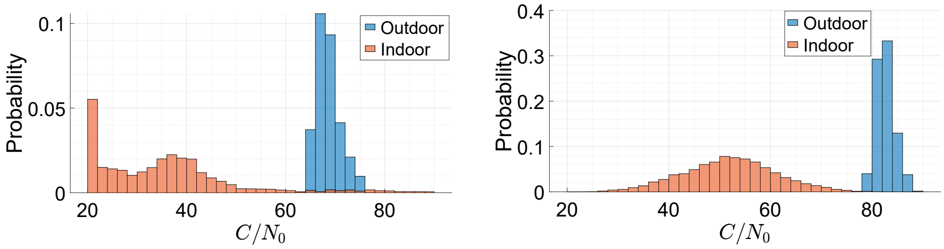
Figure 4.13 depicts the C/N_0 measurements in indoor and outdoor condition for 8 different LEO and MEO constellations, namely Astrocast, Galileo, ICEYE, Iridium Next, Kuiper, OneWeb, Starlink, and Telesat. A generic picture we can get from Figure 4.13 is the big difference in C/N_0 reception between indoor and outdoor. Typical values for C/N_0 indoors comprises between $20-40$ dB-Hz, while outdoors C/N_0 values are > 50 dB-Hz. By comparing the MEO and LEO constellations depicted in Figure 4.13 we can clearly observe that C/N_0 levels, especially outdoors are benefited from the closer proximity to the Earth. While MEO constellation typically offer about $45-50$ dB-Hz (e.g., Galileo), LEO offer up to 85 dB-Hz (e.g., Iridium). On the contrary, indoors, the signal is hugely attenuated due to the extra penetration losses, although in higher or lower degrees depending on the carrier frequency employed by the constellation. This extra indoor attenuation is more severe for those constellations employing higher carrier frequencies. For this reason, constellations such as Kuiper, OneWeb, Starlink, or Telesat, which use Ku-/Ka-frequency bands, offer similar received C/N_0 as the analyzed MEO constellations. Although on average, the received C/N_0 levels indoors for the LEO constellations can be up to about 15 dB-Hz higher, as we will see later. The potential increase in C/N_0 reception is compensated by a higher path loss, especially indoors, due mainly to extra indoor loss penetration (e.g., wall attenuation, glass attenuation, etc), which reduces significantly the received C/N_0 at higher frequencies. Moreover, the LEO constellations using lower carrier frequencies, such as Iridium Next (L-band), can offer much higher C/N_0 levels indoors since it benefits from both closer proximity to the Earth and reduced indoor attenuation. In its regard, LEO constellations such as Astrocast or ICEYE, the main reason for the reduced indoor C/N_0 levels is the relatively lower transmitted powers (see Table 4.3), being up to 30 dBm lower with respect the rest of LEO constellations in the comparison.

4.5.4.1 Frequency band considerations

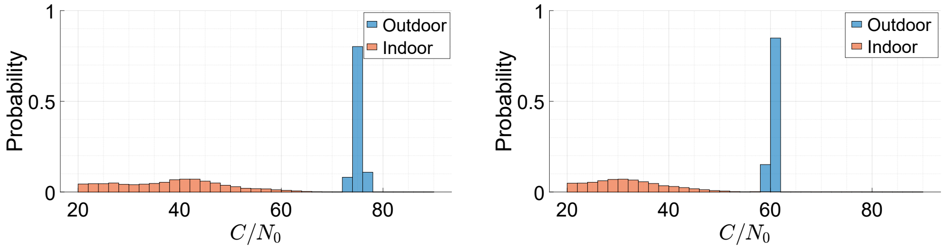
The provided results in Section 4.5.4 suggested that by decreasing the carrier frequency (keeping the same transmitted power level) the path loss and hence the measured C/N_0 in the receiver will be considerably higher than at higher frequency



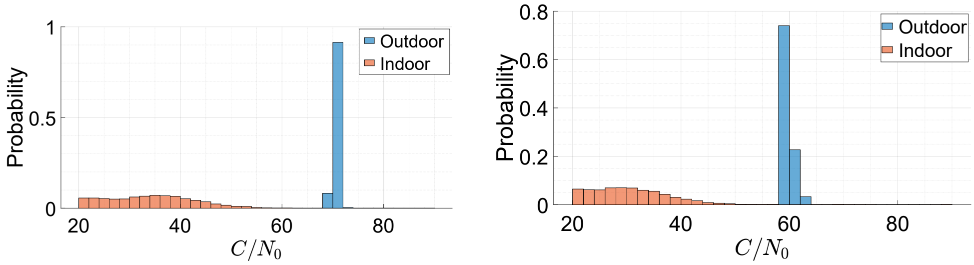
(a) Astrocast **(b)** Galileo



(c) ICEYE **(d)** Iridium Next



(e) Kuiper **(f)** OneWeb



(g) Starlink **(h)** Telesat

Figure 4.13 C/N_0 measurements in indoor and outdoor scenario for eight different constellations: a) Astrocast (LEO, small); b) Galileo (MEO); c) ICEYE (LEO, small); d) Iridium (LEO, small); e) Kuiper (LEO, mega); f) OneWeb (LEO, mega); g) Starlink (LEO, mega); h) Telesat (LEO, mega).

bands. The selection of radio frequencies in space, as in many other cases, cannot be freely chosen. Any entity willing to transmit signals must notify International Telecommunication Union (ITU) to comply with the Radio Regulations. ITU determines and coordinates how the radio frequency spectrum is shared between different users and services [196, 197]. The commonly used frequency bands in space and their typical use is listed below [196, 197]:

1. L-band (1–2 GHz): Typically used for satellite navigation and satellite mobile phones, such as Iridium or Inmarsat, providing communications at sea, land, and air. It is also used for amateur radio and aircraft surveillance.
2. S-band (2–4 GHz): Commonly used for weather radar, surface ship radar, and some communications satellites, especially those of NASA for communication with ISS and Space Shuttle.
3. C-band (4–8 GHz): Primarily used for satellite communications, satellite TV, and raw satellite feed. It is also commonly used in areas that are subject to tropical rainfall since it is less susceptible to rain fade than higher frequency bands such as Ku-band.
4. X-band (8–12 GHz): Usually used by the military, typically in radar applications including continuous-wave, pulsed, single-polarisation, dual- polarisation, synthetic aperture radar and phased arrays. It is also used for weather monitoring, air traffic control, maritime vessel traffic control, defense tracking, and vehicle speed detection for law enforcement.
5. Ku-band (12–18 GHz): Typically used for satellite communications and direct broadcast satellite services.
6. Ka-band (26–40 GHz): This band is also typically used for satellite communications. It is also used for high-resolution, close-range targeting radars on military aircraft.
7. Q- and V- bands: Typically Q/V bands are considered. These bands lie between 33-75 GHz. These frequencies are planned to be used mainly for satellite communications, remote sensing, terrestrial microwave communications, and radio astronomy studies.

Moreover, it is important to notice that not all services have been allocated to specific frequency bands. For example services such as those for the safety of life, applications have not been awarded yet a specific frequency.

4.5.5 Summary of Results

To conclude this chapter, we will summarize the main outcomes obtained through this study. Both the results from the choice of a dedicated LEO-PNT and from re-utilizing an available LEO constellation will be comprised. Table 4.5 summarizes the main results obtained during our simulations. It contains the main results for the 12 chosen satellite constellations (10 LEO and 2 MEO). Table 4.5 contains the main DoP results (average GDoP and PDoP), satellite coverage (average number of satellites in view per Earth point) and link budget (average path loss and C/N_0) performance for these 12 MEO and LEO constellations. From the results shown in Table 4.5, we can state the following:

- From the optimization study presented in Section 4.5.1, we can state that a dedicated LEO-PNT constellation is feasible in terms of design complexity. According to our study for an operative minimum elevation mask of 10°, the dedicated LEO-PNT should be composed of about 216 satellites, distributed in 12 different orbital planes with a minimum orbit inclination of 75°. From this study, we observe as the main constraint is in the number of orbital planes. Since independent launches should be made for each orbital plane, it is not typically possible to launch satellites at different orbital planes at the same time. Although a positive aspect of these results is that with about 200 satellites (properly distributed), we can offer 4-fold global coverage.
- The analyzed regular-sized MEO satellite constellations, namely Galileo and GPS, offer DoP performances of 4 and 5, respectively. Taking these values as a benchmark, observing the rest of the results, and knowing that lower DoP values are better, we can state that LEO constellations can benefit GNSS and increase their PNT accuracy. For example, regular-sized LEO satellite constellations, namely Globalstar, ICYE, and Myriota can offer DoP values up to 2-3. These values are below the benchmark from MEO GNSS. LEO mega-constellations, namely Kuiper, Starlink, OneWeb, and Telesat, offer incredibly good performance, achieving DoP values even below 1. Despite the fact that not all LEO constellations offer such a good DoP. For example, Iridium or Blacksky Global offers a performance above the specified MEO GNSS benchmark, achieving a DoP of 8. Therefore, we can state that by selecting a geometrically efficient configuration, LEO constellations can contribute to

improving GNSS accuracy.

- Although some constellations might offer a good geometry for positioning purposes (with DoP values below current MEO GNSS), not all of them offer the minimum average of 4 satellites in view in every Earth's location. For example, ICEYE and Myriota offer lower DoP than the benchmark GNSS (which is good in terms of positioning capabilities), but at the same time, these constellations also offer a very poor coverage in terms of the average amount of visible satellites (< 1). Therefore, even though these configurations offer low DoP, they are not suitable for positioning due to the lack of enough visible satellites. Some other bigger constellations such as Blacksky Global, Astrocast, or Iridium have a similar problem: the amount of satellites in view is not enough for providing a global positioning service. However, we have found that LEO mega-constellations offer an incredibly high amount of satellites in view, comprising up to 375 average satellites in view as well as DoP up to 5 times lower (on average) than MEO GNSS.
- LEO constellations typically offer lower path-loss and higher C/N_0 due to their closer proximity to Earth than MEO GNSS (which is about 20000 km below with respect the analyzed MEO constellations). Focusing on the expected received C/N_0, we observed that LEO constellations can offer up to 30 dB more outdoors compared with current MEO GNSS. Current MEO constellation offer average C/N_0 values of about 45 dBHz, while most of the LEO constellations provide at least 60 dBHz, and some (Iridium) even more than 80 dBHz of C/N_0. This C/N_0 level is basically dependent on two things: the orbit altitude and the carrier frequency band employed in the transmissions. Those constellations having satellites at lower altitudes can provide higher C/N_0 values than those in higher orbits. In addition, those constellations operating at lower carrier frequencies can provide higher C/N_0 than those using higher carrier frequency bands. In both cases is due to a lower path-loss attenuation by reducing the travel distance (lower altitudes) or reducing the carrier frequency. If we evaluate the results indoors, we observe as the C/N_0 for LEO satellites is reduced from 60-80 dB-Hz to about 40-50 dB-Hz. This is between 10 dBHz and 30 dBHz of C/N_0 less. MEO C/N_0 is about 25-30 dB-Hz, about 15-20 dB-Hz less with respect outdoors. So still LEO offers higher C/N_0 compared to MEO, but with a reduce performance with respect

outdoors. The main drawback of LEO satellite signals indoors is coming from the higher frequency bands of operation. Ku-, K-, and Ka- bands attenuation is much higher with respect for example L-band (typically used for GPS and Galileo), which partially compensates for the effects and smooths the potential gain of orbiting at such low altitudes of a few hundred km.

Table 4.5 Summary of results, including average DoP, coverage and average link budget calculations obtained in urban outdoor (blue) and indoor (orange) scenarios.

Constellation Name	GDOP	PDOP	Satellites-in-View	Pathloss [dB]	C/N_0 [dB-Hz]
Astrocast	6.06	19.07	2.01	158.45 / 175.73	58.03 / 41.81
BlackSky Global	7.68	16.37	1.62	173.01 / 195.23	56.47 / 35.34
Galileo	4.41	3.91	8.58	184.92 / 201.89	50.83 / 33.76
Globalstar 2nd Gen	2.08	1.61	0.64	155.91 / 179.73	76.57 / 63.55
GPS	5.25	4.65	9.17	183.55 / 201.29	51.94 / 34.34
ICEYE	3.16	6.06	0.49	172.86 / 200.10	68.62 / 44.63
Iridium Next	7.44	8.96	2.66	160.72 / 178.73	82.75 / 64.75
Kuiper	2.93	9.35	132.56	176.96 / 202.76	75.53 / 49.73
Myriota	2.49	2.31	0.48	146.49 / 160.57	63.29 / 49.21
OneWeb	0.75	0.70	356.04	181.10 / 206.80	60.41 / 34.92
Starlink	0.9	0.86	374.51	174.75 / 200.28	70.85 / 45.31
Telesat	2.84	2.70	70.80	186.04 / 213.55	59.66 / 32.63

🟦 Outdoor
🟧 Indoor

4.6 Summary of contributions

The main contribution to this thesis by the author in this chapter can be summarized as follows:

- Identifying the advantages and disadvantages of LEO constellations compared to MEO constellations and providing a list of positive and negative aspects of both.
- Providing a comparison between miniaturized satellites (or small-satellites) with regular-sized satellites and describing the main advantages and disadvantages of miniaturized satellites with respect to regular-sized satellites.

- Listing the main satellite classes according to the satellite mass. In addition, we have also provided examples of satellite constellations for each satellite class.
- Describing the Keplerian orbit parameters and summarizing the main constellation types.
- Classifying the different orbits by their altitude, satellite movement direction with respect to the Earth, orbit inclination, orbit eccentricity, orbit synchronicity, and constellation topology.
- Analyzing the main orbit perturbations, including mathematical models and examples for the atmospheric drag.
- Providing a literature review for the main LEO satellite constellation with potential capabilities for being used for positioning. This includes orbit parameters and propagation simulations to analyze their topology and structure in the sky.
- Providing mathematical models for modeling the satellite coverage from the geometric analysis. Including equations for selecting the minimum number of orbital planes, the number of satellites, and the minimum orbit inclination for achieving the desired coverage.
- Proposing a possible constellation architecture for a dedicated LEO-PNT based on an optimization study that includes the number of satellites, number of orbital planes, and minimum orbit inclination.
- Simulating different LEO and MEO satellite constellations, and analyzing their performance in terms of coverage, DoP and link budget.
- Comparing the selected LEO constellations with the benchmark MEO constellations.
- Comparing some LEO constellations according to their potential usage as SoO for positioning purposes. This analysis includes their geometric, coverage, and link budget viability.

Chapter 5

Conclusions and Open Research Directions

GNSS has nowadays gained a huge significance in our daily life. Its purpose is not only for navigation and positioning, but it is also used in many other types of applications such as item tracking, telecommunications, economic transactions, or transportation. However, GNSS signals are very weak and they are potentially subjected to interferences, both unintended and intentional. Such vulnerability of GNSS to various interference sources was the key driver behind the work in this thesis.

The first objective of this thesis was to understand and model the effects behind different types of interference signals as well as their effect on the GNSS receiver operation. We identified five jamming classes, namely CW jammers, single saw-tooth chirp jammers, multi saw-tooth chirp jammers, chirp with frequency bursts jammers, and other jammer types such as narrowband noise or pulsed jammer. We also identified four spoofing classes, namely simplistic spoofers, intermediate spoofers, sophisticated spoofers, and meaconing. We provided mathematical models for all of them. Jammers are typically used for degrading the resulting PVT solution (if low power is used) or for completely blocking the availability of the GNSS satellite transmissions (if high power is used).

If the jammer power is sufficiently high, it may overcome the weak GNSS signals, and hence block the GNSS satellite availability in a determined area. Typically, CW (e.g., AM and FM signals) jammers are less dangerous than other jammer types since the signal usually affects specific and measurable frequencies (also known as tones) and not partial or even the whole GNSS bandwidth. This fact makes these jammer types easier to be detected and mitigated. On the contrary, saw-tooth jammer types are more dangerous than other studied jammer types; especially the chirp jammers with frequency bursts are very challenging because they affect several frequencies at a time and are more difficult to be detected, tracked, and mitigated.

As for spoofers, they are mainly used for fooling the GNSS receivers by making them receive fake GNSS signals, with the purpose of producing a forged PVT solution, although a spoofer can also be used to deteriorate and block real GNSS transmissions. Depending on the type of spoofer, its fake signals are easier or more difficult to be detected and mitigated. For example, the most simple spoofers can be mitigated by just performing some AoA analysis (satellites signals will come from higher elevations than terrestrial spoofers) or integrity check (comparing the received navigation message with the received by some other trusted source such as a dedicated server on the Internet). A more advanced spoofer can almost perfectly mimic the GNSS signal coming from the satellites.

At the same time as succeeding with the second thesis objective, we answered the research questions *What interference management solutions exist and which one would be most suitable for a particular GNSS application such as aviation domain?* and *How different interference signals could be detected and/or classified based on machine learning approaches?*. To answer the question *What interference management solutions exist and which one would be most suitable for a particular GNSS application such as aviation domain?* we analyzed different interference detection and classification mechanisms in order to detect if interference was present, and if so, which signal type it was, in order to apply signal-specific interference mitigation mechanisms. We analyzed the performance of five jamming detection methods, namely AGC, FPD, kurtosis, TPD, and Welch. To answer the question *How different interference signals could be detected and/or classified based on machine learning approaches?* we analyzed some classification algorithms. We finally selected two of them as the most promising and we perform a classification mechanism based on spectrogram image classification using machine learning, namely SVM and CNN. The proposed classification approach consisted of training two different machine learning algorithms with black-and-white spectrogram images containing different types of jammers at different levels of JSR and C/N_0. Afterward, the algorithms were able to discriminate between the presence of a jamming signal or interference-free scenario, and also which type of jammer was present.

In the jamming detection analysis, it was noted that interferences were successfully detected with both simulated and in-lab data, even at JSR's as low as 0 dB for most of the analyzed interference signal types. The power-based detectors, namely AGC, TPD and FPD (and its variations such as Welch and periodogram) provided the best performance in terms of minimum JSR to detect the jammer attack, which was about −10 dB. As for the analyzed classification algorithms, the analysis proved the effectiveness of the approach, showing classification accuracies of more than 90% with both algorithms.

Finally, the third objective was to investigate the capabilities of LEO systems as an alternative in case GNSS is not available (or we cannot rely on the solution it provides due to interferences), or just as a complementary solution to increase the capabilities and accuracy of the current MEO GNSS. In this sense, we provided a feasibility study from two points of view: i) re-using partially or completely existing (or planned) LEO satellite constellations or ii) providing the basis for a dedicated LEO-PNT constellation.

On the one hand, in the case of re-using LEO constellations, we performed a feasibility study of ten LEO constellations, namely Astrocast, BlackSky Global, Globalstar, ICEYE, Iridium Next, Kuiper, Myriota, OneWeb, Starlink, and Telesat from the positioning point of view. We compared these LEO constellations to the existing MEO GNSS constellations (GPS and Galileo), as they are benchmark for any future LEO-PNT system. In this study, we found that not all the analyzed constellations are feasible for positioning.

Some constellations (Astrocast, BlackSky Global, Globalstar, ICEYE, and Myriota) do not provide 4-fold coverage (global coverage with at least 4 satellites-in-view at any time), which is the minimum coverage needed for positioning since to obtain the PVT solution we need the signal from at least 4 satellites. Therefore, only the so-called mega-constellations, namely Kuiper, OneWeb, Starlink, and Telesat, with thousands of satellites each, were able to provide 4-fold coverage. Most of these constellations were providing hundreds of satellites in view on average. From the positioning perspective, this is good, since as more references we have to compute the PVT solution, the more accurate this solution will be. Moreover, we found that, again, not all the LEO constellations provided a sufficiently low DoP, or at least a DoP good enough for positioning (with values in the range or lower values than the benchmark MEO GNSS).

Although one of the most important outcomes was that, for the mega-constellations, the DoP values were much lower than those in MEO GNSS. LEO mega-constellations achieved values even lower than 1, although only for OneWeb and Starlink (which are the densest constellations with 7808 and 34404 satellites, respectively). The last analysis comprised link budget computations of the different LEO and MEO constellations. In this analysis we found that, in average, LEO constellation provided higher C/N_0 values up to 30 dB-Hz for both outdoors and indoors scenario, with respect MEO GNSS constellations.

On the other hand, in the case of developing a completely new and dedicated LEO-PNT constellation, we provided an initial analysis of the space segment architecture. We performed an optimization method based on DoP, coverage, received C/N_0, and drag force metrics, to find the optimal altitude for the LEO constellation. With the found optimal altitude, which was about 600 km (or 500-700 km with 1% margin error), we were able to determine the minimum number of orbital planes, the number of satellites, and the minimum orbit inclination with the mathematical models we developed. By using the mathematical models, we found that with only 216 satellites, distributed in 12 orbital planes, and with a minimum orbit inclination of 75° we were able to provide 4-fold global coverage.

With this analysis we answered the research questions *Is LEO satellite-based positioning a good and feasible complementary or alternative to increase the robustness in situations when GNSS is strongly affected by interference?? If so, which are the main advantages it can provide?* and *Are LEO mega-constellations the answer to future global positioning using satellite systems?*.

As for open research directions to be further considered from the work done during this thesis, we have identified at least the followings:

- Testing some of the analyzed jamming algorithms also with spoofing signals, to test to which extent we can also detect spoofing attacks.
- Increasing the training dataset size in jamming classification via machine learning algorithms with more jamming types and more different signal parameters to have a better-trained model able to increase even further its accuracy capabilities.
- Expanding the classification methods for jamming (and include as well spoofing) classification with pre-/post-correlation data. Using the full data rather

than an image would allow performing further and more advanced signal processing methods to select which features we want to classify with the machine learning algorithms.

- Contributing to the signal design on board of a dedicated LEO-PNT satellite is also an important and yet-unsolved challenge. The selected signal modulation, coding mechanisms, and multiple access schemes should offer high robustness to atmospheric effects, multipath, and resilience to high Doppler shifts.

To conclude, in this thesis, we have proved through simulations with synthetic and in-lab data that jamming detection (and especially for the aviation domain) is possible even at JSR as low as 0 dB. We have also shown that jamming classification using machine learning algorithms can efficiently provide jamming classification with accuracies of more than 90%.

Moreover, we have shown that LEO constellations are a feasible option to complement MEO GNSS to provide positioning capabilities when current GNSS is not available due to interferences or due to a harsh environment. In addition, LEO constellations can definitely benefit the future of satellite navigation systems.

References

[1] A. C. O'Connor, M. P. Gallaher, K. Clark-Sutton, D. Lapidus, Z. T. Oliver, T. J. Scott, D. W. Wood, M. A. Gonzalez, E. G. Brown and J. Fletcher. *Economic Benefits of the Global Positioning System (GPS)*. Tech. rep. National Institute of Standards and Technology, June 2019. URL: `https://www.nist.gov/system/files/documents/2020/02/06/gps_finalreport618.pdf`.

[2] I. UK. *The economic impact on the UK of a disruption to GNSS*. Tech. rep. Innovate UK, June 2017. URL: `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf`.

[3] OSQZSS. *GPS-SDR-SIM*. `https://github.com/osqzss/gps-sdr-sim`. 2015.

[4] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon and J. Kintner. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. *21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*. Jan. 2008, 2314–2325.

[5] A. Kerns, D. Shepard, J. Bhatti and T. Humphreys. Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics* 31 (July 2014). DOI: `10.1002/rob.21513`.

[6] J. Bhatti and T. E. Humphreys. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *NAVIGATION* 64.1 (2017), 51–66. DOI: `https://doi.org/10.1002/navi.183`. eprint: `https:`

//onlinelibrary.wiley.com/doi/pdf/10.1002/navi.183. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.183.

[7] K. Hill. Jamming GPS Signals Is Illegal, Dangerous, Cheap, and Easy. *Gizmodo* (Aug. 12, 2017). URL: https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955 (visited on 02/18/2022).

[8] S. Peterson and P. Faramarzi. Iran hijacked US drone, says Iranian engineer. *The Christian Science Monitor* (Dec. 15, 2011). URL: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer (visited on 08/04/2021).

[9] G. W. Staff. Massive GPS Jamming Attack by North Korea. *GPS World* (Aug. 12, 2012). URL: https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/ (visited on 08/04/2021).

[10] BBCNews. North Korea jamming hits South Korea flights. *British Broadcasting Corporation* (May 2, 2012). URL: https://www.bbc.com/news/world-asia-17922021 (visited on 08/04/2021).

[11] C. Sebastian. Getting lost near the Kremlin? Russia could be GPS spoofing. *CNN Business* (Dec. 2, 2016). URL: https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/ (visited on 08/04/2021).

[12] M. Burguess. To protect Putin, Russia is spoofing GPS signals on a massive scale. *Wired* (Mar. 27, 2019). URL: https://www.wired.co.uk/article/russia-gps-spoofing (visited on 08/04/2021).

[13] G. Kates. When Putin's around, GPS goes haywire, study finds. *CBS News* (Apr. 5, 2019). URL: https://www.cbsnews.com/news/when-putins-around-gps-goes-haywire-study-finds/ (visited on 08/04/2021).

[14] M. Burguess. When a tanker vanishes, all the evidence points to Russia. *Wired* (Sept. 21, 2017). URL: https://www.wired.co.uk/article/black-sea-ship-hacking-russia (visited on 08/04/2021).

[15] M. Jones. Spoofing in the Black Sea: What really happened?: *GPS World* (Oct. 11, 2017). URL: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/ (visited on 08/04/2021).

[16] G. O'Dwyer. Norway accuses Russia of jamming its military systems. *Defense News* (Mar. 8, 2019). URL: `https://www.defensenews.com/global/europe/2019/03/08/norway-alleges-signals-jamming-of-its-military-systems-by-russia/` (visited on 08/04/2021).

[17] I. Korobko. OSCE SMM Spot Report 14/2021: Long-range unmanned aerial vehicle damaged in emergency landing due to dual GPS signal interference. *Organization for Security and Co-operation in Europe (OSCE)* (May 17, 2021). URL: `https://www.osce.org/special-monitoring-mission-to-ukraine/486769` (visited on 03/07/2022).

[18] A. Teivainen. Disruptions in GPS services hinder air traffic in central and eastern Finland. *Helsinki times* (Mar. 9, 2022). URL: `https://www.helsinkitimes.fi/finland/finland-news/domestic/21147-disruptions-in-gps-services-hinder-air-traffic-in-central-and-eastern-finland.html` (visited on 03/10/2022).

[19] Traficom. Unusual amount of reports about GPS interference near the eastern border of Finland. *Traficom* (Mar. 10, 2022). URL: `https://www.traficom.fi/en/news/unusual-amount-reports-about-gps-interference-near-eastern-border-finland` (visited on 03/10/2022).

[20] G. W. Staff. Finnish airline finds GPS interference near Russian border. *GPS World* (Mar. 10, 2022). URL: `https://www.gpsworld.com/finnish-airline-finds-gps-interference-near-russian-border/` (visited on 03/11/2022).

[21] D. Werner. HawkEye 360 detects GPS interference in Ukraine. *SpaceNews* (Mar. 4, 2022). URL: `https://spacenews.com/hawkeye-360-gps-ukr/` (visited on 03/10/2022).

[22] T. Cozzens. France develops GNSS backup service using nanosatellite. *GPS World* (Mar. 4, 2022). URL: `https://www.gpsworld.com/france-develops-gnss-backup-service-using-nanosatellite/` (visited on 03/11/2022).

[23] T. Cozzens. Xona Space readies for launch of commercial PNT satellite. *GPS World* (Sept. 22, 2021). URL: `https://www.gpsworld.com/xona-space-readies-for-launch-of-commercial-pnt-satellite/` (visited on 03/11/2022).

[24] I. GNSS. DARPA Plans to Put PNT in LEO. *Inside GNSS* (May 25, 2021). URL: `https://insidegnss.com/darpa-plans-to-put-pnt-in-leo/` (visited on 03/11/2022).

[25] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente and E. S. Lohan. A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft. *IEEE Communications Surveys & Tutorials* PP (Oct. 2019), 1–1. DOI: `10.1109/COMST.2019.2949178`.

[26] R. Morales-Ferre, P. Richter, A. De la Fuente and E. S. Lohan. In-lab validation of jammer detection and direction finding algorithms for GNSS. *International Conference on Localization and GNSS (ICL-GNSS)* (June 2019), 1–6. DOI: `10.1109/ICL-GNSS.2019.8752944`.

[27] E. S. Lohan, R. Morales-Ferre, P. Richter, E. Falletti, G. Falco and A. De la Fuente. GNSS Navigation Threats Management on-Board of Aircraft. *INCAS BULLETIN* 11 (Sept. 2019), 111–125. DOI: `10.13111/2066-8201.2019.11.3.10`.

[28] R. Morales-Ferre, A. De la Fuente and E. S. Lohan. Jammer Classification in GNSS Bands Via Machine Learning Algorithms. *Sensors, Special Issue Interference, Robustness and Complementary Solutions for GNSS-Based Navigation for Aerial Vehicles* 19 (Nov. 2019), 4841. DOI: `10.3390/s19224841`.

[29] R. Morales-Ferre, E.-S. Lohan, G. Falco and E. Falletti. GDOP-based analysis of suitability of LEO constellations for future satellite-based positioning. *IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)* (Oct. 2020), 147–152. DOI: `10.1109/WiSEE44079.2020.9262624`.

[30] R. Morales-Ferre and E. S. Lohan. Comparison of MEO, LEO, and terrestrial IoT configurations in terms of GDOP and achievable positioning accuracies. *IEEE Journal of Radio Frequency Identification* 5 (Sept. 2021). DOI: `10.1109/JRFID.2021.3079475`.

[31] R. M. Ferre, E. S. Lohan, H. Kuusniemi, J. Praks, S. Kaasalainen, C. Pinell and M. Elsanhoury. Is LEO-Based Positioning with Mega-Constellations the Answer for Future Equal Access Localization?: *IEEE Communications Magazine* 60.6 (2022), 40–46. DOI: `10.1109/MCOM.001.2100841`.

[32] F. S. Prol, R. M. Ferre, Z. Saleem, P. Välisuo, C. Pinell, E. S. Lohan, M. Elsanhoury, M. Elmusrati, S. Islam, K. Celikbilek, K. Selvan, J. Yliaho, K. Rutledge, A. Ojala, L. Ferranti, J. Praks, M. Z. H. Bhuiyan, S. Kaasalainen and H. Kuusniemi. Position, Navigation, and Timing (PNT) Through Low Earth Orbit (LEO) Satellites: A Survey on Current Status, Challenges, and Opportunities. *IEEE Access* 10 (2022), 83971–84002. DOI: `10.1109/ACCESS.2022.3194050`.

[33] M. Nicola, G. Falco, R. Morales-Ferre, E. S. Lohan, A. De la Fuente and E. Falletti. Collaborative Solutions for Interference Management in GNSS-Based Aircraft Navigation. *Sensors* 20.15 (2020). ISSN: 1424-8220. DOI: `10.3390/s20154085`. URL: `https://www.mdpi.com/1424-8220/20/15/4085`.

[34] R. Morales-Ferre, W. Wang, A. Sanz-Abia and E. S. Lohan. Identifying GNSS Signals Based on Their Radio Frequency (RF) Features—A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator. *Data* 5.1 (2020). ISSN: 2306-5729. DOI: `10.3390/data5010018`. URL: `https://www.mdpi.com/2306-5729/5/1/18`.

[35] *GATEMAN project*. `https://cordis.europa.eu/project/id/783183`. Accessed: 2022-04-05.

[36] R. Morales-Ferre, G. Seco-Granados and E.-S. Lohan. Positioning Reference Signal design for positioning via 5G. *XXXV Finnish URSI Convention on Radio Science* XXXV (2019). URL: `https://www.ursi.fi/2019/Papers/Morales.pdf`.

[37] *ULTRA project*. `https://projects.tuni.fi/ultra/`. Accessed: 2022-04-05.

[38] R. Morales Ferre, G. Seco-Granados and E.-S. Lohan. Energy-efficiency considerations for GNSS signal acquisition. *InsideGNSS* (Dec. 2021).

[39] *INCUBATE project*. `https://www.incubateproject.org/`. Accessed: 2022-04-05.

[40] G. Falco, M. Nicola, E. Falletti and M. Pini. An Algorithm for Finding the Direction of Arrival of Counterfeit GNSS Signals on a Civil Aircraft. Oct. 2019, 3185–3196. DOI: `10.33012/2019.17061`.

[41] E. Falletti, M. T. Gamba and M. Pini. Design and Analysis of Activation Strategies for Adaptive Notch Filters to Suppress GNSS Jamming. *IEEE Transactions on Aerospace and Electronic Systems* 56.5 (2020), 3718–3734. DOI: `10.1109/TAES.2020.2982301`.

[42] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* 8 (2020), 165444–165496. DOI: `10.1109/ACCESS.2020.3022294`.

[43] A. Elgamoudi, H. Benzerrouk, G. A. Elango and R. Landry. A Survey for Recent Techniques and Algorithms of Geolocation and Target Tracking in Wireless and Satellite Systems. *Applied Sciences* 11.13 (2021). ISSN: 2076-3417. DOI: `10.3390/app11136079`. URL: `https://www.mdpi.com/2076-3417/11/13/6079`.

[44] Z. Wang, R. Liu, Q. Liu, L. Han and J. S. Thompson. Feasibility Study of UAV-Assisted Anti-Jamming Positioning. *IEEE Transactions on Vehicular Technology* 70.8 (2021), 7718–7733. DOI: `10.1109/TVT.2021.3090403`.

[45] V. Tripathi, W. Elmarissi and S. Caizzone. An ITAR-free Dual Frequency Antenna Array in the ARINC Footprint for Robust Aeronautical Navigation. Oct. 2020, 3686–3696. DOI: `10.33012/2020.17682`.

[46] G. LaMountain and P. Closas. Maneuver Optimization for Synthetic Aperture based DOA estimation of GNSS Jammers. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. 2020, 44–49. DOI: `10.1109/PLANS46316.2020.9110215`.

[47] A. Elgamoudi, H. Benzerrouk, G. A. Elango and R. J. Landry. Quasi-Real RFI Source Generation Using Orolia Skydel LEO Satellite Simulator for Accurate Geolocation and Tracking: Modeling and Experimental Analysis. *Electronics* 11.5 (2022). ISSN: 2079-9292. DOI: `10.3390/electronics11050781`. URL: `https://www.mdpi.com/2079-9292/11/5/781`.

[48] C. Zhou, R. Xiong, H. Zeng, J. Xiao, Y. Wang, P. Jia, J. Ye, T. Zhao and K. Hu. Aerial Locating Method Design for Civil Aviation RFI: UAV Monitoring Platform and Ground Terminal System. *Journal of Intelligent & Robotic Systems* 103 (Oct. 2021), 29. DOI: `10.1007/s10846-021-01479-y`.

[49] P. Borhani Darian, H. Li, P. Wu and P. Closas. Deep Neural Network approach to detect GNSS Spoofing Attacks. Oct. 2020. DOI: `10.33012/2020.17537`.

[50] T. Morehouse, C. Montes, M. Bisbano, J. F. Lin, M. Shao and R. Zhou. Incremental learning-based jammer classification. *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III*. Vol. 11746. International Society for Optics and Photonics. 2021, 117462E.

[51] A. Siemuri, H. Kuusniemi, M. S. Elmusrati, P. Välisuo and A. Shamsuzzoha. Machine Learning Utilization in GNSS—Use Cases, Challenges and Future Applications. *2021 International Conference on Localization and GNSS (ICL-GNSS)*. 2021, 1–6. DOI: `10.1109/ICL-GNSS51451.2021.9452295`.

[52] J. Liu, J.-c. Li, B.-g. Cai and J. Wang. Test and Evaluation of GNSS-based Railway Train Positioning under Jamming Conditions. *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 2020, 1459–1464. DOI: `10.1109/SMC42975.2020.9283279`.

[53] W. Qin and F. Dovis. Situational awareness of chirp jamming threats to GNSS based on supervised machine learning. *IEEE Transactions on Aerospace and Electronic Systems* (2021), 1–1. DOI: `10.1109/TAES.2021.3135014`.

[54] V. J. Michael. *Classification of GNSS Jammers using Machine Learning : Multivariate Time Series and Image Classification Based Approaches*. 2021. URL: `https://hdl.handle.net/11250/2823900`.

[55] C. J. Swinney and J. C. Woods. GNSS Jamming Classification via CNN, Transfer Learning & the Novel Concatenation of Signal Representations. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. 2021, 1–9. DOI: `10.1109/CyberSA52016.2021.9478250`.

[56] K. Lorraine and M. Ramarakula. A Comprehensive Survey on GNSS Interferences and the Application of Neural Networks for Anti-jamming. *IETE Journal of Research* (Aug. 2021), 1–20. DOI: `10.1080/03772063.2021.1953407`.

[57] G.-H. Lee, J. Jo and C. Park. Jamming Prediction for Radar Signals Using Machine Learning Methods. *Security and Communication Networks* 2020 (Jan. 2020), 1–9. DOI: `10.1155/2020/2151570`.

[58] P. Lang, X. Fu, M. Martorella, J. Dong, R. Qin, X. Meng and M. Xie. *A Comprehensive Survey of Machine Learning Applied to Radar Signal Processing*. 2020. DOI: `10.48550/ARXIV.2009.13702`. URL: `https://arxiv.org/abs/2009.13702`.

[59] A. Morrison, N. Sokolova, J. E. Håkegård, T. H. Bryne and L. Ruotsalainen. A Multi-Site Quad-Band Radio Frequency Interference Monitoring Alerting and Reporting System. *2020 European Navigation Conference (ENC)*. 2020, 1–10. DOI: `10.23919/ENC48637.2020.9317522`.

[60] W. Wang, I. A. Sanchez, G. Caparra, A. McKeown, T. Whitworth and E. S. Lohan. A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data. *Sensors (Basel, Switzerland)* 21 (2021).

[61] H. Elyousseph and M. L. Altamimi. UAV RF Fingerprinting with Power Spectra Estimates. *2021 2nd International Conference on Range Technology (ICORT)*. 2021, 1–6. DOI: `10.1109/ICORT52730.2021.9581796`.

[62] H. Elyousseph and M. L. Altamimi. Deep Learning Radio Frequency Signal Classification with Hybrid Images. *2021 IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*. 2021, 7–11. DOI: `10.1109/ICSIPA52582.2021.9576786`.

[63] Y. Liu, J. Wang, J. Li, S. Niu and H. Song. Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey. *IEEE Internet of Things Journal* 9.1 (2022), 298–320. DOI: `10.1109/JIOT.2021.3099028`.

[64] M. L. Psiaki. Navigation using carrier Doppler shift from a LEO constellation: TRANSIT on steroids. *NAVIGATION* 68.3 (2021), 621–641. DOI: `https://doi.org/10.1002/navi.438`. eprint: `https://onlinelibrary.wiley.com/doi/pdf/10.1002/navi.438`. URL: `https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.438`.

[65] B. McLemore and M. L. Psiaki. GDOP of Navigation using Pseudorange and Doppler Shift from a LEO Constellation. *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)* (2021).

[66] B. Mclemore and M. Psiaki. Navigation Using Doppler Shift from LEO Constellations and INS Data. *IEEE Transactions on Aerospace and Electronic Systems* (2022), 1–1. DOI: `10.1109/TAES.2022.3162772`.

[67] M. Neinavaie, J. Khalife and Z. Kassas. Exploiting Starlink Signals for Navigation: First Results. *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)* (2021).

[68] M. Neinavaie, J. Khalife and Z. M. Kassas. Doppler Stretch Estimation with Application to Tracking Globalstar Satellite Signals. *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*. 2021, 647–651. DOI: `10.1109/MILCOM52596.2021.9652890`.

[69] L. Ye, Y. Yang, X. Jing, H. Li, H. Yang and Y. Xia. Dual-Satellite Alternate Switching Ranging/INS Integrated Navigation Algorithm for Broadband LEO Constellation Independent of Altimeter and Continuous Observation. *Remote Sensing* 13.16 (2021). ISSN: 2072-4292. DOI: `10.3390/rs13163312`. URL: `https://www.mdpi.com/2072-4292/13/16/3312`.

[70] E. D. Kaplan and C. J. Hegarty, eds. *Understanding GPS: principles and applications. Principles and Applications*. 2nd ed. Artech House Publishers, 2006. ISBN: 1-58053-894-0.

[71] I. J. Gupta, I. M. Weiss and A. W. Morrison. Desired Features of Adaptive Antenna Arrays for GNSS Receivers. *Proc. IEEE* 104.6 (June 2016), 1195–1206. ISSN: 0018-9219. DOI: `10.1109/JPROC.2016.2524416`.

[72] F. Bastide, D. Akos, C. Macabiau and B. Roturier. Automatic gain control (AGC) as an interference assessment tool. *ION GPS/GNSS 2003, 16th International Technical Meeting of the Satellite Division of The Institute of Navigation*. Portland, United States, Sept. 2003, pp 2042 –2053. URL: `https://hal-enac.archives-ouvertes.fr/hal-01021721`.

[73] M. Foucras, O. Julien, C. Macabiau and B. Ekambi. An efficient strategy for the acquisition of weak galileo E1 OS signals. *ENC 2013, European Navigation Conference*. Vienne, Austria, Apr. 2013, pp xxxx. URL: `https://hal-enac.archives-ouvertes.fr/hal-00937081`.

[74] E. S. Lohan, D. Alonso de Diego, J. A. Lopez-Salcedo, G. Seco-Granados, P. Boto and P. Fernandes. Unambiguous Techniques Modernized GNSS Signals: Surveying the solutions. *IEEE Signal Processing Magazine* 34.5 (2017), 38–52. DOI: `10.1109/MSP.2017.2711778`.

[75] P. Closas, C. Fernandez-Prades and J. A. Fernandez-Rubio. Maximum Likelihood Estimation of Position in GNSS. *IEEE Signal Processing Letters* 14.5 (2007), 359–362. DOI: `10.1109/LSP.2006.888360`.

[76] P. Closas and A. Gusi-Amigo. Direct Position Estimation of GNSS Receivers: Analyzing main results, architectures, enhancements, and challenges. *IEEE Signal Processing Magazine* 34.5 (2017), 72–84. DOI: `10.1109/MSP.2017.2718040`.

[77] S. Zhao and D. Akos. An open source GPS/GNSS vector tracking loop - Implementation, filter tuning, and results. Jan. 2011.

[78] R. Mu and T. Long. Design and Implementation of Vector Tracking Loop for High-Dynamic GNSS Receiver. *Sensors* 21.16 (2021). ISSN: 1424-8220. DOI: `10.3390/s21165629`. URL: `https://www.mdpi.com/1424-8220/21/16/5629`.

[79] G. MacGougan, G. Lachapelle, R. Nayak and A. Wang. Overview of GNSS signal degradation phenomena. *Proceedings of the International Symposium Kinematic Systems and Geodesy, Geomatics and Navigation*. 2001.

[80] P. Puricer and P. Kovar. Technical Limitations of GNSS Receivers in Indoor Positioning. *2007 17th International Conference Radioelektronika*. 2007, 1–5. DOI: `10.1109/RADIOELEK.2007.371487`.

[81] G. D. MacGougan. *High Sensitivity GPS Performance Analysis in Degraded Signal Environments*. 2003. DOI: `10.11575/PRISM/12159`.

[82] J. Marais and B. Godefroy. Analysis and optimal use of GNSS pseudo-range delays in urban canyons. *The Proceedings of the Multiconference on Computational Engineering in Systems Applications*. Vol. 1. 2006, 31–36. DOI: `10.1109/CESA.2006.4281619`.

[83] C. Fouque and P. Bonnifait. Vehicle localization in urban canyons using geo-referenced data and few GNSS satellites. *IFAC Symposium on Intelligent Autonomous Vehicle*. Toulouse, France, 2007, 84. URL: `https://hal.archives-ouvertes.fr/hal-00445268`.

[84] T. Reid, A. Neish, T. Walter and P. Enge. Leveraging Commercial Broadband LEO Constellations for Navigation. *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)*. Sept. 2016. DOI: `10.33012/2016.14729`.

[85] P. A. Iannucci and T. E. Humphreys. Economical Fused LEO GNSS. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. 2020, 426–443.

[86] T. G. Reid, A. M. Neish, T. Walter and P. K. Enge. Broadband LEO Constellations for Navigation. *NAVIGATION* 65.2 (2018), 205–220. DOI: `https://doi.org/10.1002/navi.234`. eprint: `https://onlinelibrary.wiley.com/doi/pdf/10.1002/navi.234`. URL: `https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.234`.

[87] F. Pereira and D. Selva. Exploring the Architecture Trade Space of NextGen Global Navigation Satellite Systems. *2019 IEEE Aerospace Conference*. 2019, 1–13. DOI: `10.1109/AERO.2019.8741849`.

[88] H. Benzerrouk, Q. Nguyen, F. Xiaoxing, A. Amrhar, A. V. Nebylov and R. Landry. Alternative PNT based on Iridium Next LEO Satellites Doppler/INS Integrated Navigation System. *2019 26th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS)*. 2019, 1–10.

[89] H. Ge, B. Li, M. Ge, N. Zang, L. Nie, Y. Shen and H. Schuh. Initial Assessment of Precise Point Positioning with LEO Enhanced Global Navigation Satellite Systems (LeGNSS). *Remote Sensing* 10.7 (2018). ISSN: 2072-4292. DOI: `10.3390/rs10070984`. URL: `https://www.mdpi.com/2072-4292/10/7/984`.

[90] B. Li, H. Ge, M. Ge, L. Nie, Y. Shen and H. Schuh. LEO enhanced Global Navigation Satellite System (LeGNSS) for real-time precise positioning services. *Advances in Space Research* 63.1 (2019), 73–93. ISSN: 0273-1177. DOI:

`https://doi.org/10.1016/j.asr.2018.08.017`. URL: `https://www.sciencedirect.com/science/article/pii/S0273117718306264`.

[91] K. Wyatt and M. Gruber. *Radio Frequency Interference Pocket Guide - RFI Characterization, Location Techniques, Tools and Remediation Methods, with Key Equations and Data*. Institution of Engineering and Technology, 2015. ISBN: 978-1-61353-219-5.

[92] F. Dovis, ed. *GNSS Interference Threats and Countermeasures*. Artech House, 2015. ISBN: 978-1-60807-810-3.

[93] B. R. Elbert. *Radio Frequency Interference in Communications Systems*. Artech House Space Technology and Applications Series. Artech House, 2016. ISBN: 9781608079650.

[94] P. Stavroulakis. *Interference Analysis and Reduction for Wireless Systems*. Mobile Communications Series. Artech House, Inc, 2003. ISBN: 9781580533164.

[95] 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). *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)* (Portland, Oregon). 2011, 430–435.

[96] D. Borio, F. Dovis, H. Kuusniemi and L. L. Presti. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proc. IEEE* 104.6 (June 2016), 1233–1245. ISSN: 0018-9219. DOI: `10.1109/JPROC.2016.2543266`.

[97] 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* 2012 (July 2012). DOI: `10.1155/2012/127072`.

[98] J. A. Klobuchar. Ionospheric Effects on GPS, in Global Positioning System. *Global Positioning System: Theory and Applications, Volume I*. Ed. by J. J. Spilker, J. Penina Axelrad, B. W. Parkinson and P. Enge. Washington: American Institute of Aeronautics and Astronautics INC., 1996. Chap. 12, 485–515.

[99] L. Gupta, R. Jain and G. Vaszkun. Survey of Important Issues in UAV Communication Networks. *IEEE Communications Surveys & Tutorials* 18.2 (2016), 1123–1152. ISSN: 1553-877X. DOI: `10.1109/COMST.2015.2495297`.

[100] EUROCONTROL. *EUROCONTROL Guidelines on a Process for Civil-Military GNSS Interference Testing*. Tech. rep. EUROCONTROL, Aug. 2021. URL: `https://www.eurocontrol.int/sites/default/files/2021-09/eurocontrol-gnss-interference-testing-guid-v1-0.pdf`.

[101] I. C. A. O. (ICAO). *ICAO, Aviation Security, Annex 17*. Tech. rep. International Civil Aviation Organization (ICAO), Aug. 2022. URL: `https://store.icao.int/en/annex-17-security`.

[102] S. M. Kay. *Fundamentals of statistical signal processing (Vol. 2): Detection theory*. Prentice-Hall, 1998. ISBN: 013504135X.

[103] A. Balaei, B. Motella and A. G. Dempster. GPS Interference Detected in Sydney-Australia. *IGNSS conference*. Dec. 2007.

[104] M. Z. H. Bhuiyan, H. Kuusniemi, S. Soderholm and E. Airos. The Impact of Interference on GNSS Receiver Observables – A Running Digital Sum Based Simple Jammer Detector. *Radioengineering* 23.3 (Sept. 2014), 898–906. URL: `https://www.radioeng.cz/fulltexts/2014/14_03_0898_0906.pdf` (visited on 09/2019).

[105] N. Fadaei. Detection, Characterization and Mitigation of GNSS Jamming Interference Using Pre-Correlation Methods. Master's thesis. University of Calgary, 2016.

[106] J. Lehtomäki. Analysis of energy based signal detection. PhD thesis. University of Oulu, Department of Electrical and Information Engineering, 2005.

[107] T. H. Stitz and M. Renfors. Filter-Bank-Based Narrowband Interference Detection and Suppression in Spread Spectrum Systems. *EURASIP J. Adv. Signal Process.* 2004.8 (July 2004). DOI: `10.1155/s1110865704312102`.

[108] K. D. Wesson, J. N. Gross, T. E. Humphreys and B. L. Evans. GNSS Signal Authentication Via Power and Distortion Monitoring. *IEEE Trans. Aerosp. Electron. Syst.* 54.2 (Apr. 2018), 739–754. ISSN: 0018-9251. DOI: `10.1109/TAES.2017.2765258`.

[109] W. Li, Z. JiaQi, L. Yan and P. ShuSheng. Detection of radiometer radio frequency interference with power-law detector. *2017 International Applied Computational Electromagnetics Society Symposium (ACES)*. Aug. 2017.

[110] J. T. Johnson and L. C. Potter. Performance Study of Algorithms for Detecting Pulsed Sinusoidal Interference in Microwave Radiometry. *IEEE Transactions on Geoscience and Remote Sensing* 47.2 (Feb. 2009), 628–636. ISSN: 0196-2892. DOI: `10.1109/TGRS.2008.2003956`.

[111] F. M. Ahmed, K. A. Elbarbary and A. R. H. Elbardawiny. Detection of Sinusoidal Signals in Frequency Domain. *2006 CIE International Conference on Radar*. Oct. 2006. DOI: `10.1109/ICR.2006.343208`.

[112] K. P. Balanda and H. L. MacGillivray. Kurtosis: A Critical Review. *The American Statistician* 42.2 (1988), 111–119. ISSN: 00031305. URL: `http://www.jstor.org/stable/2684482`.

[113] F. D. Nunes and F. M. G. Sousa. GNSS blind interference detection based on fourth-order autocumulants. *IEEE Transactions on Aerospace and Electronic Systems* 52.5 (Oct. 2016), 25740–2586. ISSN: 0018-9251. DOI: `10.1109/TAES.2016.150499`.

[114] G. J. Saulnier and P. Das. Antijam Spread Spectrum Receiver using LMS Adaptive Filtering Techniques. *IEEE Military Communications Conference (MILCOM)*. Vol. 3. 1984, 482–487. DOI: `10.1109/MILCOM.1984.4794898`.

[115] D. Borio, C. O'Driscoll and J. Fortuny. Fast and Flexible. Tracking and Mitigating a Jamming Signal with an Adaptive Notch Filter. *Inside GNSS* 9.2 (March/April 2014), 67–73.

[116] Y.-R. Chien. Design of GPS Anti-Jamming Systems Using Adaptive Notch Filters. *IEEE Syst. J.* 9 (2015), 451–460. DOI: `10.1109/jsyst.2013.2283753`.

[117] D. Alonso. Narrowband interference rejection studies for Galileo signals via Simulink. Master's thesis. Tampere University of Technology, 2015.

[118] V. N. Vapnik. *The nature of statistical learning theory*. Springer-Verlag New York, Inc., 1995. ISBN: 0-387-94559-8.

[119] M. Ajay and M. F. Giles. Multiclass and Binary SVM Classification: Implications for Training and Classification Users. *IEEE Geoscience and Remote Sensing Letters* 5 (2008), 241–245.

[120] S. O'Hara and B. A. Draper. *Introduction to the Bag of Features Paradigm for Image Classification and Retrieval*. 2011. eprint: `1101.3354`.

[121] T. Guo, J. Dong, H. Li and Y. Gao. Simple convolutional neural network on image classification. *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)* (2017), 721–724.

[122] T. Chen and C. Guestrin. XGBoost: A Scalable Tree Boosting System. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. KDD'16. San Francisco, California, USA: ACM, 2016, 785–794. ISBN: 978-1-4503-4232-2. DOI: `10.1145/2939672.2939785`. URL: `http://doi.acm.org/10.1145/2939672.2939785`.

[123] L. Breiman. Random Forests. *Machine Learning* 45.1 (2001), 5–32. ISSN: 0885-6125. DOI: `10.1023/A:1010933404324`. URL: `http://dx.doi.org/10.1023/A%3A1010933404324`.

[124] W. S. McCulloch and W. Pitts. A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics* 5.4 (1943), 115–133.

[125] A. Mucherino, P. J. Papajorgji and P. M. Pardalos. k-Nearest Neighbor Classification. *Data Mining in Agriculture*. New York, NY: Springer New York, 2009, 83–106. ISBN: 978-0-387-88615-2. DOI: `10.1007/978-0-387-88615-2_4`. URL: `https://doi.org/10.1007/978-0-387-88615-2_4`.

[126] J. Furnkranz. Decision Tree. *Encyclopedia of Machine Learning*. Ed. by C. Sammut and G. I. Webb. Boston, MA: Springer US, 2010, 263–267. ISBN: 978-0-387-30164-8. DOI: `10.1007/978-0-387-30164-8_204`. URL: `https://doi.org/10.1007/978-0-387-30164-8_204`.

[127] J. Huillery and N. Martin. Time-Frequency Modeling and Detection of random non-stationary signals for Monitoring Purposes. 11 (May 2006). DOI: `10.2514/6.2006-2261`.

[128] V. Kecman, T.-M. Huang and M. Vogt. Iterative Single Data Algorithm for Training Kernel Machines from Huge Data Sets: Theory and Performance.

Support Vector Machines: Theory and Applications. Vol. 177. May 2005, 605–605. DOI: `10.1007/10984697_12`.

[129] Q. Wu and D.-X. Zhou. SVM Soft Margin Classifiers: Linear Programming versus Quadratic Programming. *Neural Computation* 17.5 (2005), 1160–1187. DOI: `10.1162/0899766053491896`. URL: `https://doi.org/10.1162/0899766053491896`.

[130] R.-E. Fan, P.-H. Chen and C.-J. Lin. Working Set Selection Using Second Order Information for Training Support Vector Machines. *The Journal of Machine Learning Research* 6 (Dec. 2005), 1889–1918. ISSN: 1532-4435. URL: `http://dl.acm.org/citation.cfm?id=1046920.1194907`.

[131] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke and A. Rabinovich. Going Deeper with Convolutions. (2014). DOI: `10.48550/ARXIV.1409.4842`.

[132] K. Simonyan and A. Zisserman. Very Deep Convolutional Networks for Large-Scale Image Recognition. (2014). DOI: `10.48550/ARXIV.1409.1556`.

[133] M. Tan and Q. Le. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. *Proceedings of the 36th International Conference on Machine Learning*. Ed. by K. Chaudhuri and R. Salakhutdinov. Vol. 97. Proceedings of Machine Learning Research. PMLR, June 2019, 6105–6114. URL: `https://proceedings.mlr.press/v97/tan19a.html`.

[134] P. Richter, R. Morales-Ferre and E. S. Lohan. *GATEMAN project – Wide-bandwidth, high-precision GNSS and jammer raw data*. Zenodo. 2019. DOI: `10.5281/zenodo.1161298`.

[135] F. Ramsey and Z. Marek. OneWeb LEO PNT: Progress or Risky Gamble?: *Inside GNSS* 9.2 (September/October 2020), 48–50.

[136] J. Najder and K. Sośnica. Quality of Orbit Predictions for Satellites Tracked by SLR Stations. *Remote Sensing* 13.7 (2021). ISSN: 2072-4292. DOI: `10.3390/rs13071377`. URL: `https://www.mdpi.com/2072-4292/13/7/1377`.

[137] A. B. Jenkin, M. E. Sorge, J. P. McVey, G. E. Peterson and B. Y. Yoo. MEO Debris Environment Projection Study. 2013.

[138] X. Dai, Y. Lou, Z. Dai, C. Hu, Y. Peng, Q. Jing and C. Shi. Precise Orbit Determination for GNSS Maneuvering Satellite with the Constraint of a Predicted Clock. *Remote Sensing* 11 (Aug. 2019), 1949. DOI: `10.3390/rs11161949`.

[139] L. Yang, H. Ruan, Y. Zhang and J. Su. Autonomous Orbit Determination System of Navigation Satellite Based on Spaceborne GPS Technology. *Security and Communication Networks* 2022 (Jan. 2022). ISSN: 1939-0114. DOI: `10.1155/2022/7463315`. URL: `https://doi.org/10.1155/2022/7463315`.

[140] A. Golkar and A. Salado. Definition of New Space—Expert Survey Results and Key Technology Trends. *IEEE Journal on Miniaturization for Air and Space Systems* 1 (2021), 2–9. DOI: `10.1109/JMASS.2020.3045851`.

[141] G. Haibo, L. Bofeng, N. Liangwei, G. Maorong and S. Harald. LEO constellation optimization for LEO enhanced global navigation satellite system (LeGNSS). *Advances in Space Research* 66.3 (2020), 520–532. ISSN: 0273-1177. DOI: `https://doi.org/10.1016/j.asr.2020.04.031`.

[142] G. Curzi, D. Modenini and P. Tortora. Large Constellations of Small Satellites: A Survey of Near Future Challenges and Missions. *Aerospace* 7.9 (2020). DOI: `10.3390/aerospace7090133`.

[143] T. C. Program. *CubeSat Design Specification Rev. 13*. 2014. URL: `https://static1.squarespace.com/static/5418c831e4b0fa4ecac1bacd/t/56e9b62337013b6c063a655a/1458157095454/cds_rev13_final2.pdf`.

[144] N. C. L. Initiative. *CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers*. 2017. URL: `https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf`.

[145] J. C. Springmann. Satellite attitude determination with low-cost sensors. PhD thesis. University of Michigan, 2013.

[146] A. D. Lorrie and F. Lucien. *How Long Does It Take to Develop and Launch Government Satellite Systems?* 2015. URL: `https://www.iceaaonline.com/ready/wp-content/uploads/2014/03/Davis-Satellite-ICEAASoCal-090915.pdf`.

[147] A. Ballard. Rosette Constellations of Earth Satellites. *IEEE Transactions on Aerospace and Electronic Systems* AES-16.5 (1980), 656–673. DOI: `10.1109/TAES.1980.308932`.

[148] J. G. Walker. Satellite Constellations. *Journal of the British Interplanetary Society* 37 (Dec. 1984), 559.

[149] D. Mortari and M. P. Wilkins. Flower constellation set theory. Part I: Compatibility and phasing. *IEEE Transactions on Aerospace and Electronic Systems* 44.3 (2008), 953–962. DOI: `10.1109/TAES.2008.4655355`.

[150] Y. Fun Hu, G. Maral and E. Ferro. Appendix A: Satellite Constellation Design for Network Interconnection Using Non-Geo Satellites. *Service Efficient Network Interconnection via Satellite*. John Wiley & Sons, Ltd, 2001, 215–237. ISBN: 9780470845929. DOI: `https://doi.org/10.1002/0470845929.app1`. eprint: `https://onlinelibrary.wiley.com/doi/pdf/10.1002/0470845929.app1`. URL: `https://onlinelibrary.wiley.com/doi/abs/10.1002/0470845929.app1`.

[151] H. Schaub and J. L. Junkins. *Analytical Mechanics of Space Systems*. Reston, VA: AIAA Education Series, Oct. 2003. DOI: `10.2514/4.861550`.

[152] H. D. Curtis. *Orbital Mechanics for Engineering Students*. Second Edition. Aerospace Engineering. Boston: Butterworth-Heinemann, 2010, 693–699. ISBN: 978-0-12-374778-5. URL: `https://www.sciencedirect.com/book/9780123747785/orbital-mechanics-for-engineering-students`.

[153] S. Cakaj. Practical horizon plane and communication duration for Low Earth Orbiting (LEO) satellite ground stations. *WSEAS Transactions on Communications* 8 (Jan. 2009).

[154] J. Winn, J. Johnson, S. Albrecht, A. Howard, G. Marcy, I. Crossfield and M. Holman. HAT-P-7: A retrograde or polar orbit, and a third body. *The Astrophysical Journal Letters* 703 (Sept. 2009), L99. DOI: `10.1088/0004-637X/703/2/L99`.

[155] Spaceflight101. Israel Launches Advanced Optical Reconnaissance Satellite. *Spaceflight101* (Sept. 13, 2016). URL: `https://spaceflight101.com/israel-launches-advanced-optical-reconnaissance-satellite/` (visited on 04/08/2022).

[156] S. D. Ilcev. Polar Earth Orbits (PEO). *2010 20th International Crimean Conference Microwave Telecommunication Technology*. 2010, 413–415. DOI: `10.1109/CRMICO.2010.5632692`.

[157] L. Riishojgaard. High-latitude winds from molniya orbit - a mission concept for NASA's Earth system science pathfinder program. *International Workshop on the Analysis of Multi-Temporal Remote Sensing Images, 2005*. 2005, 120–124. DOI: `10.1109/AMTRSI.2005.1469853`.

[158] J. Davis, D. Mortari and J. V. McAdams. Reducing Walker, Flower, and Streets-of-Coverage Constellations to a Single Constellation Design Framework. *Advances in the astronautical sciences, Spaceflight mechanics 2012*. Vol. 143. Published for the American Astronautical Society by Univelt, 2012, 697–712. ISBN: 978-0877035817.

[159] M. Guan, T. Xu, F. Gao, W. Nie and H. Yang. Optimal Walker Constellation Design of LEO-Based Global Navigation and Augmentation System. *Remote Sensing* 12.11 (2020). ISSN: 2072-4292. DOI: `10.3390/rs12111845`. URL: `https://www.mdpi.com/2072-4292/12/11/1845`.

[160] J. E. Velazco and J. S. De la Vega. A CubeSat Mission to Demonstrate Omnidirectional Optical Communications. *2020 IEEE Aerospace Conference*. 2020, 1–6. DOI: `10.1109/AERO47225.2020.9172329`.

[161] R. L. Sturdivant and E. K. P. Chong. Systems Engineering of a Terabit Elliptic Orbit Satellite and Phased Array Ground Station for IoT Connectivity and Consumer Internet Access. *IEEE Access* 4 (2016), 9941–9957. DOI: `10.1109/ACCESS.2016.2608929`.

[162] J. E. Draim, P. Cefola and D. Castrel. Elliptical orbit constellations-a new paradigm for higher efficiency in space systems?: *2000 IEEE Aerospace Conference. Proceedings (Cat. No.00TH8484)*. Vol. 7. 2000, 27–35 vol.7. DOI: `10.1109/AERO.2000.879272`.

[163] Spaceref. Space Systems/Loral-Built Satellite for SIRIUS XM Radio Successfully Begins Post-Launch Maneuvers. *Spaceref* (July 2, 2009). URL: `http://www.spaceref.com/news/viewpr.html?pid=28626` (visited on 04/08/2022).

[164] M. P. Wilkins and D. Mortari. Flower constellation set theory part II: Secondary paths and equivalency. *IEEE Transactions on Aerospace and Electronic Systems* 44.3 (2008), 964–976. DOI: `10.1109/TAES.2008.4655356`.

[165] R. H. Ibrahim. Improvement of the Accuracy of the Perturbed Orbital Elements for LEO Satellite by Improving 4th Order Runge–Kutta's Method. *Indian journal of science and technology* 13 (2020), 417–429.

[166] B. Kuiack. Spacecraft Formation Guidance and Control on J2-Perturbed Eccentric Orbits. MA thesis. Carleton University, 2018.

[167] K. I. Khalil and S. Samwel. Effect of Air Drag Force on Low Earth Orbit Satellites During Maximum and Minimum Solar Activity. *Space Research Journal* 9 (Mar. 2016), 1–9. DOI: `10.3923/srj.2016.1.9`.

[168] A. E. Hedin. MSIS-86 Thermospheric Model. *Journal of Geophysical Research: Space Physics* 92.A5 (1987), 4649–4662. DOI: `https://doi.org/10.1029/JA092iA05p04649`. eprint: `https://agupubs.onlinelibrary.wiley.com/doi/pdf/10.1029/JA092iA05p04649`. URL: `https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/JA092iA05p04649`.

[169] C. Ardito, J. Morales, J. Khalife, A. Abdallah and Z. Kassas. Performance Evaluation of Navigation Using LEO Satellite Signals with Periodically Transmitted Satellite Positions. Feb. 2019, 306–318. DOI: `10.33012/2019.16743`.

[170] C. Pinell. Receiver Architectures for Positioning with Low Earth Orbit Satellite Signals. English. Master's thesis. Aalto University. School of Electrical Engineering, 2021, 54. URL: `http://urn.fi/URN:NBN:fi:aalto-2021121910938`.

[171] N. Jardak and Q. Jault. The Potential of LEO Satellite-Based Opportunistic Navigation for High Dynamic Applications. *Sensors* 22.7 (2022). ISSN: 1424-8220. DOI: `10.3390/s22072541`. URL: `https://www.mdpi.com/1424-8220/22/7/2541`.

[172] *Astrocast Constellation Description*. `www.astrocast.com`, accessed on: 04.02.2022. 2022.

[173] Federal Communications Commission (FCC). *BlackSky Global LLC Application for Modification of License To Construct, Deploy and Operate an NGSO Earth Exploration Satellite Service Constellation System*. Tech. rep. BlackSky Global LLC, July 2019. URL: `https://docs.fcc.gov/public/attachments/DA-20-571A1.pdf`.

[174] D. Navarro-reyes, A. Notarantonio and G. Taini. Galileo Constellation: Evaluation of Station Keeping Strategies. 2009.

[175] E. Parliament and D.-G. for Parliamentary Research Services. *Galileo Satellite Navigation System: space applications on earth*. Publications Office, 2019. DOI: `doi/10.2861/684607`.

[176] Globalstar. *Globalstar Overview*. Tech. rep. Globalstar, Dec. 2017. URL: `https://www.globalstar.com/Globalstar/media/Globalstar/Downloads/Spectrum/GlobalstarOverviewPresentation.pdf`.

[177] P. Massatt and M. Zeitzew. The GPS Constellation Design - Current and Projected. 1998.

[178] *ICEYE Overview*. `https://earth.esa.int/eogateway/missions/iceye`, accessed on: 04.02.2022. 2022.

[179] *ICEYE*. `https://www.iceye.com/`, accessed on: 04.02.2022. 2022.

[180] Federal Communications Commission (FCC). *IRIDIUM Next Engineering Statement, Appendix 1*. Tech. rep. Iridium Constellation LLC, July 2013. URL: `https://fcc.report/IBFS/SAT-MOD-20131227-00148/1031348.pdf`.

[181] Federal Communications Commission (FCC). *Application of Kuiper Systems LLC for Authority to Launch and Operate a Non-Geostationary Satellite Orbit System in Ka-band Frequencies: Technical Appendix*. Tech. rep. Kuiper Systems LLC, Nov. 2021. URL: `https://fcc.report/IBFS/SAT-LOA-20211104-00145/13337528`.

[182] Federal Communications Commission (FCC). *Kuiper Systems LLC Request for Experimental Authorization Narrative Statement*. Tech. rep. Kuiper Systems LLC, Nov. 2021. URL: `https://apps.fcc.gov/els/GetAtt.html?id=285359&x=`.

[183] Federal Communications Commission (FCC). *Myriota Pty. Ltd. Petition for Declaratory Ruling Granting Access to the U.S. Market for Non-Voice, Non-Geostationary Satellite System*. Tech. rep. Myriota Pty. Ltd., Dec. 2020. URL: `https://docs.fcc.gov/public/attachments/DA-20-571A1.pdf`.

[184] Federal Communications Commission (FCC). *Amendment to Modification Application for U.S. Market Access Grant for the OneWeb Ku- and Ka-Band System*. Tech. rep. WorldVu Satellites Limited (Oneweb), Apr. 2021. URL: `https://fcc.report/IBFS/SAT-MPL-20210112-00007/3495551.pdf`.

[185] Federal Communications Commission (FCC). *Spacex non-geostationary satellite system, attachment A, technical information to supplement schedule S*. Tech. rep. Space Exploration Holdings, LLC, Apr. 2020. URL: `https://fcc.report/IBFS/SAT-MOD-20200417-00037/2274316.pdf`.

[186] Federal Communications Commission (FCC). *Spacex non-geostationary satellite system, attachment A, technical information to supplement schedule S*. Tech. rep. Space Exploration Holdings, LLC, Aug. 2021. URL: `https://fcc.report/IBFS/SAT-AMD-20210818-00105/12943361.pdf`.

[187] Federal Communications Commission (FCC). *TELESAT Low Earth Orbit non-geostationary satellite system*. Tech. rep. TELESAT, Apr. 2020. URL: `https://fcc.report/IBFS/SAT-MPL-20200526-00053/2378320.pdf`.

[188] G. Dai, X. Chen, M. Wang, E. Fernández, T. N. Nguyen and G. Reinelt. Analysis of Satellite Constellations for the Continuous Coverage of Ground Regions. *Journal of Spacecraft and Rockets* 54.6 (Nov. 2017), 1294–1303. DOI: `10.2514/1.a33826`.

[189] J. Wertz, N. C. for Space Technology (U.S.) and N. R. L. (U.S.) Mission Geometry: Orbit and Constellation Design and Management : Spacecraft Orbit and Attitude Systems. Space technology library. Microcosm Press, 2001, 726. ISBN: 9781881883074. URL: `https://books.google.fi/books?id=aQWPPwAACAAJ`.

[190] S. M. Kay. *Fundamentals of Statistical Signal Processing (vol. 1): Estimation Theory*. Prentice Hall, 1997. ISBN: 0-13-345711-7.

[191] E. S. Lohan. Analytical performance of CBOC-modulated Galileo E1 signal using sine BOC(1,1) receiver for mass-market applications. *IEEE/ION Position, Location and Navigation Symposium*. 2010, 245–253. DOI: `10.1109/PLANS.2010.5507207`.

[192] E. S. Lohan and K. Borre. Accuracy limits in multi-GNSS. *IEEE Transactions on Aerospace and Electronic Systems* 52.5 (2016), 2477–2494. DOI: `10.1109/TAES.2016.150241`.

[193] S. Jaeckel, L. Raschkowski, K. Börner and L. Thiele. QuaDRiGa: A 3-D Multi-Cell Channel Model With Time Evolution for Enabling Virtual Field Trials. *IEEE Transactions on Antennas and Propagation* 62.6 (2014), 3242–3256. DOI: `10.1109/TAP.2014.2310220`.

[194] S. Jaeckel, L. Raschkowski, K. Borner, L. Thiele, F. Burkhardt and E. Eberlein. *QuaDRiGa - Quasi Deterministic Radio Channel Generator, User Manual and Documentation*. Fraunhofer Report. Fraunhofer Heinrich Hertz Institute, 2020. URL: `https://quadriga-channel-model.de/?download=32621` (visited on 02/16/2022).

[195] S. Jaeckel, L. Raschkowski and L. Thiele. *A 5G-NR Satellite Extension for the QuaDRiGa Channel Model*. 2020. arXiv: `2010.01002 [eess.SP]`.

[196] International Telecommunication Union (ITU). *Recommendation ITU-R V.431-8: Nomenclature of the frequency and wavelength bands used in telecommunications*. Tech. rep. International Telecommunication Union (ITU), Aug. 2015. URL: `https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-E.pdf`.

[197] International Telecommunication Union (ITU). *ITU Radio Regulation 2020, Articles, Volume 1*. Tech. rep. International Telecommunication Union (ITU), Aug. 2020. URL: `https://www.itu.int/dms_pub/itu-r/opb/reg/R-REG-RR-2020-ZPF-E.zip`.