UAB
Universitat Autònoma de Barcelona

Feasibility of Snapshot-Based Spoofing Detection Using OSNMA Unpredictable Symbols

Husnain Shahid

ADVERTIMENT. L'accés als continguts d'aquesta tesi queda condicionat a l'acceptació de les condicions d'ús establertes per la següent llicència Creative Commons:  https://creativecommons.org/licenses/?lang=ca

ADVERTENCIA. El acceso a los contenidos de esta tesis queda condicionado a la aceptación de las condiciones de uso establecidas por la siguiente licencia Creative Commons:  https://creativecommons.org/licenses/?lang=es

WARNING. The access to the contents of this doctoral thesis it is limited to the acceptance of the use conditions set by the following Creative Commons license:  https://creativecommons.org/licenses/?lang=en

UAB
Universitat Autònoma de Barcelona

Ph.D. Dissertation

Feasibility of Snapshot-Based Spoofing Detection Using OSNMA Unpredictable Symbols

Author: **Husnain Shahid**

Thesis Advisors: **José A. López-Salcedo**
Gonzalo Seco-Granados

Doctoral Program in Electronic and Telecommunication Engineering

Universitat Autònoma de Barcelona (UAB)

Bellaterra, March 2024

Contents

List of Figures **6**

List of Tables **11**

List of Abbreviations **12**

List of Notations **16**

Abstract **18**

Acknowledgement **19**

1 Introduction **22**
1.1 Research Objectives 23
1.2 Research Scope 24
1.3 Thesis Organization 25

2 Overview of GNSS **28**
2.1 Operating Principles of GNSS 28
2.1.1 Description of Constellations 28
2.1.2 GNSS Signals 30
2.1.3 GNSS System Description 31
2.1.3.1 Space Segment 31
2.1.3.2 Ground Segment 32
2.1.3.3 User Segment 33
2.1.4 GNSS Receiver Architecture & Signal Processing . . . 34
2.1.4.1 Link Budget 35
2.1.4.2 Intermediate Frequency (IF) Signal Processing: 36
2.1.4.3 Signal Acquisition 37
2.1.4.4 Signal Tracking 38
2.1.4.5 Navigation Solution 40
2.1.4.6 Weighted Least Squares (WLS) 43

2.2 Security Concerns on GNSS 45
2.2.1 Motivation 45
2.2.2 OSNMA Fundamentals 45

3 Spoofing Attacks and Countermeasures 49
3.1 Types of Attacks to GNSS Receivers 49
3.1.1 Jamming 49
3.1.2 Meaconing 50
3.1.2.1 Important Features of Meaconing Attack . . . 51
3.1.3 Spoofing 51
3.1.3.1 Simplistic Attack 52
3.1.3.2 Intermediate Attack 52
3.1.3.3 Sophisticated Attack 53
3.2 State of the Art of Anti-Spoofing Techniques 53
3.2.1 Antenna-Level Techniques 54
3.2.1.1 Array Processing 54
3.2.1.2 Polarization Discrimination 56
3.2.2 Pre-Correlation Techniques 58
3.2.2.1 Absolute Power Monitoring 58
3.2.2.2 Power Variation 59
3.2.2.3 Dual Frequency Power Comparison 61
3.2.3 DSP Post-Correlation Techniques 61
3.2.3.1 Multi-Peak Detection 62
3.2.3.2 Signal Quality Monitoring 64
3.2.3.3 Consistency Checks 68
3.2.3.4 Observable Jumps 70
3.2.3.5 Clock Monitoring 70
3.2.3.6 Multiple Constellation/Frequency Redundancy 71
3.2.4 External Aiding 72
3.2.4.1 Assisted GNSS 73
3.2.4.2 Server-Assisted Processing of GNSS Encrypted Signals 75
3.2.5 OSNMA Anti-Spoofing Techniques for SCER Attacks . 75

4 Snapshot OSNMA: Concept and Feasibility 81
4.1 Snapshot OSNMA 82
4.1.1 OSNMA Unpredictable Symbols 83
4.1.2 Snapshot OSNMA System Architecture 85
4.2 Feasibility and Boundary Conditions of Snapshot OSNMA . . 87
4.2.1 Signal model at the spoofer's side 87
4.2.2 Signal model at the user's side 88

4.2.3 Unpredictable symbol errors induced by a simple spoofer 89
4.2.4 Unpredictable symbol errors due to a sophisticated spoofer 90
4.2.5 Symbol errors due to user's receiver noise 91
4.2.6 Symbol errors due to the overlap of authentic and spoofed signals at the user's receiver 92
4.2.7 Symbol errors due to multipath 95
4.2.8 Symbol errors due to synchronization errors at the user's receiver 97
4.3 Symbol errors due to signal fading 100
4.4 Detection of Spoofed Unpredictable Symbols 102
4.4.1 Proposed Detector 103
4.4.2 Statistical Characterization 103
4.4.3 Threshold Settings 104
4.5 Performance Evaluation in Open Sky Environment 105
4.6 Performance Evaluation in Urban and Sub-Urban Environment 111
4.7 Statistical Characterization of Snapshot OSNMA Spoofing Detector 116
4.8 Performance Evaluation 119
4.9 Practical Implementation Aspects 121
4.9.1 Relative time delay between visible satellites 122
4.9.2 Clock offset affecting the wake up time 124

5 Detection Performance Under Time and Symbol Errors 127
5.1 Signal model 129
5.1.1 Signal model for the sequence of received symbols . . . 130
5.1.2 Symbol error rate for typical working scenarios 131
5.2 Proposed snapshot spoofing detection 132
5.2.1 Detector Formulation 132
5.2.2 Probability of Detection 134
5.2.3 Probability of False Alarm 135
5.3 Simulation Results 135
5.3.1 Goodness of the Theoretical Expressions for P_{d} and P_{fa} 135
5.3.2 Probability of Detection as a Function of P_{e} 137
5.3.3 Probability of Detection vs Probability of False Alarm 138
5.4 Conclusions 140

6 Experimental Analysis of Snapshot OSNMA 141
6.1 Experimental Processing 141
6.1.1 Signal Generation: 142
6.1.1.1 Authentic Signal 143
6.1.1.2 Spoofed Signal 143

6.1.2 IQ Files Processing with FGI-GRX Software Receiver: 147
6.1.3 Snapshot OSNMA Spoofing Detection 152
6.1.4 Conclusion 156

Publications and Other Supports **156**

Bibliography **158**

List of Figures

2.1 GNSS System Architecture: space segment, ground control segment and user segment. 32
2.2 Block diagram of GNSS receiver processing. 37
2.3 The basic principle of signal acquisition. 38
2.4 The basic principle of signal tracking [1]. 39
2.5 Signal tracking with FGI-GSRx software receiver, illustrating PLL, FLL locks on real-like Galileo E1B signal. 40
2.6 Depiction of GNSS positioning principle. 41

3.1 Basic workflow of meaconing in GNSS [2]. 50
3.2 Scenario that illustrates the working of spoofing in GNSS. . . 51
3.3 (a) Different geometry of authentic satellite signals impinging with a dual antenna receiver compared to a point transmitter on ground acting as a spoofer. (b) Phase differences for 7 satellite signals with the lack of angular diversity, entitled from same transmitter [3]. 55
3.4 Polarization Diagram (a) Authentic (b) Spoofing transmitter [4]. 57
3.5 (a) Probability of detection vs probability of false alarm under different Total Spoofing Power (TSP) (b) Signal to Interference and Noise Ratio (SINR) vs TSP for authentic and spoofed signals [5]. 59
3.6 Relationship between variations in AGC and variations in C/N_0 in nominal conditions (upper right hand side corner), in the presence of RF interference (lower left hand side corner) and in the presence of spoofing (lower right hand side corner) [6]. 60
3.7 The search space in the presence of spoofer (showing in terms of two peaks, one is authentic while other is spoofed) [7]. . . 62
3.8 Explanation of width threshold for detecting the presence of spoofers [8]. 63

3.9 Interaction of a counterfeit signal with an authentic one, initially separated apart (upper plot), but gradually approaching (middle plot) until the authentic signal is captured and the aggregated correlation peak is distorted (bottom plot) [8]. 65
3.10 ROC curves for different values of p_s [9]. 66
3.11 Detection results for overpowered attack with a spoofer appearing between time 150 and 200 seconds (left plot) versus the matched power attach (right plot) with a spoofer appearing between time 150 and 200, as well as 250 and 300 seconds, when using the GoF test (upper plot) or the sign test (bottom plot). [10] 67
3.12 Time evolution for the simple ratio SQM metric (upper plot) and for the very early/late correlators (bottom plot) in the presence of a spoofing attack. [11] 68
3.13 ROC curves for individual SQM metrics and various metric combinations [12]. 68
3.14 The AGC detection metric based on jump in position fix [13]. 70
3.15 The clock bias (up) and clock bias rate (down) for a spoofed and an authentic (i.e. "clean") signal [10]. 71
3.16 The GLONASS signal is ahead of GPS due to spoofing manipulation (Left). An example of the resulting phase error (Right) [14]. 72
3.17 Location Service requests [15]. 73
3.18 Example of an A-GNSS architecture [16] 74
3.19 Spreading code transmission (left). Remote processing authentication (right). 76
3.20 Bit error probability of the spoofer (left) and gain reduction at the receiver (right) as a function of the time the spoofer spends in observing the unpredictable bits. [17] 77
3.21 Detection probability of all proposed detectors in [18] with 5dB advantage for spoofer (Left). Detection probability for the LMS channel (Right). 78
3.22 Performance for time varying attacks on Galileo E1 signal using LRT (left) and GLRT (right) for unpredictable bit detection [19]. 79

4.1 (a) I/NAV nominal odd page for Galileo E1-B, where the "Reserved 1" field containing the OSNMA data is highlighted. (b) OSNMA unpredictable symbols position (see green cells) within the I/NAV nominal odd-page already encoded and interleaved, that is, as received by the user [20]. 84

4.2 High-level architecture of the proposed snapshot OSNMA spoofing detector. 85
4.3 Probability of having at least one error in a set of Q unpredictable symbols estimated by the spoofer with probability of error p_s. 90
4.4 Impact of thermal noise in terms of Bit Error Rate (BER). . . 92
4.5 SER due to the destructive overlapping of the authentic and spoofed signals at the user's receiver as a function of the signal to spoofer ratio (SSR). Dashed lines represent the values of SSR that lead to an excessive SER (i.e. $> 10^{-3}$), and thus are likely to be avoided by a potential spoofer in order to remain unnoticed. 94
4.6 Worst SER for different C/N_0 values of the authentic signal at the user's receiver when a single-ray reflection is present, using SMR = 4.5 dB as specified in ([21], Appendix A3.3). . . 96
4.7 SER degradation, defined, as a loss in C/N_0 measured in dB, due to residual carrier phase estimation errors at the user's receiver. For the sake of completeness, the minimum C/N_0 for detecting a Galileo E1-B satellite with probability of detection 0.9 and probability of false alarm 10^{-6} is indicated in each curve by the '$\circ$' marker. 99
4.8 Cumulative distribution function (cdf) of SER in the presence of shadowing and blockage effects in urban and suburban environments, for different satellite elevation angles and a user at vehicular or pedestrian dynamics at a nominal $C/N_0 = 45$ dBHz. 102
4.9 AUC for the proposed spoofing detector when the spoofer has 3dB power advantage in perfect LOS conditions than the authentic signal and the probability of error of the spoofer is $p_s = 0.1$ (upper) and $p_s = 0.01$ (lower). 107
4.10 Probability of detecting the spoofer as a function of time when $p_s = 0.1$ (upper) and $p_s = 0.01$ (lower) for $C/N_0 = 38$ dBHz at the user's receiver and with the spoofer operating at -3, 0 and +3 dB more of C/N_0. 109
4.11 AUC for spoofer at 3dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 112
4.12 AUC for spoofer at 5dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 112
4.13 AUC for spoofer at 10dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 112

4.14 AUC for spoofer at 3dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 114
4.15 AUC for spoofer at 5dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 114
4.16 AUC for spoofer at 10dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right). 114
4.17 AUC when the spoofer has 5dB power advantage in perfect LOS conditions with $p_s = 0.01$ (upper) and Empirical ROC curve for a spoofer with 5dB power advantage in perfect LOS with $p_s = 0.1$ and $Q = 100$ (lower). 117
4.18 The empirical PDFs using Monto Carlo simulation and theoretical PDFs using Biomial distribution representing the AUC´s three regions (Blue, Green and Yellow) in terms of symbol errors under $\mathcal{H}_0$ and $\mathcal{H}_1$, when (a) AUC < 0.5, (b) AUC > 0.5 and (c) when AUC $= 0.5$. 118
4.19 P_{D} for a spoofer with 5dB power advantage in perfect LOS conditions with $p_s = 0.01$ (Left) and $p_s = 0.1$ (Right). 120
4.20 (Upper) Probability density function (pdf) of the time delay difference between satellites, with respect a reference one, using real satellite data. (Lower) Cumulative density function (cdf) corresponding to the upper one. 123
4.21 Mean number of unpredictable symbols for each satellite in view as a function of snapshot length 125

5.1 Illustration of the symbols received by the user due to the time uncertainty caused by the clock offset and the satellites different propagation times. 128
5.2 Comparison between the empirical and theoretical P_{d} for $P_{e,1} = 0.1$ (left), as well as P_{fa} for $P_{e,0} = 0.001$ (right), as a function of the unpredictable symbols L_s, using $\gamma = \{0, 1\}$. 137
5.3 Probability of detection as a function of the probability of symbol error, $P_{e,1}$, for $L_u = 20$ symbols with $\gamma = 0$ (left) and $\gamma = 1$ (right). 138
5.4 Youden index for the proposed detector in various working conditions for $P_{e,0} = \{0.001, 0.01, 0.1\}$, $P_{e,1} = \{0.5, 0.1, 0.01\}$, and time uncertainty of $L_u = 20$ symbols. 139

6.1 The experimental scheme for spoofing detection system incorporating Snapshot OSNMA capabilities. 142
6.2 Skydel GSG-8 Advanced GNSS Simulator [22] 142
6.3 Illustration of Skydel generating Galileo E1 authentic signal . 143

6.4 Illustration of Skydel modifying unpredictable bits in I/NAV message using NMM function 144
6.5 Erroneous Unpredictable bits using Skydel 145
6.6 The symbol error analysis before and after interleaving to see the impact of additional symbol errors 146
6.7 A snapshot of Galileo E1B time, frequency domain plots . . . 148
6.8 (a) BPSK constellation after acquisition stage affected Doppler and phase discontinuity. (b) The phase discontinuity between the consecutive symbols visible by phase jumps. (c) The phase continuity between the consecutive symbols visible by negligible phase jumps. 149
6.9 The BPSK constellation with Phase continuity, Doppler removed, and Phase offset of (a) 0 degree, (b) 90 degrees and (c) 180 degrees. 150
6.10 MATLAB commands to estimate and remove the Doppler from prompts. 151
6.11 The aggregation of authentic and spoofed signal with 3dB power advantage and relative phase offset 180°, where spoofing starts at time = 3 seconds and ends at 6 seconds represented in red. 152
6.12 The preamble identification to detect the even and odd pages, where the index for instance, 219, 221, 244 are the first subframes for respective satellites in view. 153
6.13 The 3rd unpredictable symbol of 1st snapshot is inverted by spoofer (left).The 3rd unpredictable symbol of 2nd snapshot is inverted by spoofer (right). 154
6.14 The 2nd unpredictable symbol of 3rd snapshot is inverted by spoofer (left).The 3rd unpredictable symbol of 4th snapshot is inverted by spoofer (right) 154
6.15 The impact of time uncertainty on the position of unpredictable symbol sequence. 155
6.16 Functional flow of the software developed for the emulation of the snapshot OSNMA concept. 158

List of Tables

2.1 The description of GNSS constellations 30
2.2 The general overview of the GNSS signal operating frequencies 31

4.1 Time delay estimation jitter in a snapshot receiver processing a snapshot of L Galileo E1-B symbols, operating at the minimum detectable C/N_0 100
4.2 The computation of threshold for snapshot length $L = 8$. . . . 106
4.3 The time required to detect the spoofing attack under different conditions 110

6.1 The overall parameters configuration to process IQ files through FGI-GRX software receiver. 148

List of Abbreviations

A-GNSS	Assisted GNSS
AER	Authentication Error Rate
AGC	Automatic Gain Control
AmpM	Amplitude Combination Mode
AOA	Angle Of Arrival
AWGN	Additive White Gaussian Noise
AUC	Area Under the ROC curve
BER	Bit Error Rate
BI	Bit Index
BOC	Binary Offset Carrier
BPSK	Binary Phase Shift Keying
BSC	Binary Symmetric Channel
CAF	Cross-Ambiguity Function
CAS	Commercial Authentication Service
CBOC	Composite Binary Offset Carrier
CDF	Cumulative Density Function
CI	Coherent Integration
CNR	Carrier to Noise Ratio
CRLB	Cramer Rao Lower Bound

DD	Distance Decreasing
DLL	Delay Lock Loop
DSP	Digital Signal Processing
DSSS	Direct-Sequence Spread Spectrum
EC	Expected Content
EM	Electromagnetic Field
ESA	European Space Agency
EU	European Union
FFT	Fast Fourier Transform
FLL	Frequency Lock Loop
FSPL	Free Space Path Loss
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GS	Ground Segment
GoF	Goodness of Fit
I	In-Phase
IF	Intermediate Frequency
IGSO	Inclination Geosynchronous Orbit
I.I.D	Independent and Identically Distributed
IoT	Internet of Things
KL	Kullback Leibler
LHCP	Left Hand Circular Polarization
LNAs	Low-Noise Amplifiers
LMS	Land Mobile Satellite
LOS	Line Of Sight

LR	Likelihood Ratio
LS	Least Square
LTE	Long Term Evolution
MAC	Message Authentication Code
MAP	Maximum A Posteriori
MEE	Multipath Error Envelope
MEO	Medium Earth Orbit
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
NCI	Non-Coherent Integration
NF	Noise Figure
NMA	Navigation Message Authentication
NMM	Navigation Message Modification
NTP	Network Time Protocol
NWPR	Narrow-band Wide Band Power Ratio
OS	Open Service
OSNMA	Open Service Navigation Message Authentication
PDF	Probability Density Function
PfaM	Probability of False Alarm combination Mode
PLL	Phase Lock Loop
PNT	Position Navigation and Timing
POI	Point Of Interest
PPS	Pulse-Per-Second
PRS	Public Regulated Service
PRN	Pseudorandom Noise

PVT	Position Velocity and Time
Q	Quadrature
RF	Radio Frequency
RHCP	Right Hand Circular Polarization
ROC	Receiver Operating Characteristic
SBAS	Satellite-Based Augmentation Systems
SCER	Security Code Estimation and Replay
SDR	Software-Defined Radio
SER	Symbol Error Rate
SINR	Signal to Interference and Noise Ratio
SMR	Signal to Multipath Ratio (SMR)
SN	Snapshot Number
SNR	Signal to Noise Ratio
SQM	Signal Quality Monitoring
SS	Space Segment
SSR	Signal to Spoofer Ratio
TESLA	Timed Efficient Stream Loss Tolerant Authentication
TQM	Time Quality Module
TSP	Total Spoofing Power
UNMM	Update Navigation Message Modification
US	User Segment

List of Notations

$\oplus$	XOR operator
$(C/N_0)_{a,u}$	C/N_0 of authentic signal at the user's receiver
$(C/N_0)_{s,u}$	C/N_0 of spoofed signal at the user's receiver
$\arg\min_x f(x)$	Value of x that minimizes function $f(x)$
ϵ_τ	Time delay estimation error
$\{\cdot\}_m$	Circular rotation of values by m positions
erfc	Complementary error function
ln	Natural logarithm
min$\|.\|$	Minimum of norm
SHA-256	Hash function
sign (r)	Take signs of vector r
ϕ	Carrier phase
$\sum_{i=0}^{N-1} x_i$	Sum of values of x_i for $i = 0$ to $N-1$
ξ	Estimation error
$B(m,p)$	Binomial distribution for m trials with success probability p
C/N_0	Carrier to Noise Ratio
g''	Second derivative
G_t	Receive gain

G_t	Transmission gain
L	Snapshot length
P_d	Probability of detection
P_n	Noise power
p_s	Probability of error by spoofer
P_t	Transmission power
P_{fa}	Probability of false alarm
$p_{u,0}$	Symbol error rate due to signal impairments
$p_{u,1}$	Symbol error rate due to spoofer and signal impairments
$R_c(t', v')$	Coherent correlation output
$R_c(t', v', k)$	Non-coherently accumulated correlation output
$S \not\subset X$	S is not a subset of X
$S \subset X$	S is a subset of X
t'	Time delay
v'	Frequency shift
$x \to 1$	The variable x approaches to 1
$X \sim f(x)$	The random variable X follows the distribution by the pdf $f(x)$
$\mathbf{A}^T$,$\mathbf{A}^{-1}$	Transpose and Inverse of matrix $\mathbf{A}$ respectively
$\mathbf{s}\in \{\pm 1\}$	Binary vector with $+1$s and -1s
$\text{var}(\epsilon_\theta)$	Variance of phase estimation error

Abstract

Global Navigation Satellite System (GNSS) signal authentication and anti-spoofing are receiving an increasing interest among the GNSS community as key enablers for the deployment of GNSS-based applications and services with safety-critical and liability-critical implications. To this end, Galileo is providing the Galileo Open Service Navigation Message Authentication (OSNMA) in its E1-B signal component, which conveys a set of cryptographic data with the purpose of authenticating the content of the Galileo I/NAV message. Some of these data symbols are unpredictable to the users, and therefore they cannot be known in advance and used to generate a counterfeit signal, thus introducing an additional protection level against potential spoofers. Despite being unpredictable, spoofers could still estimate these symbols on the fly and use them to retransmit a counterfeit signal to forge the user's navigation solution.

In response to these attacks, this dissertation sets to present a novel idea of a snapshot-based spoofing detector at symbol level that makes use of only the OSNMA unpredictable symbols. The technique is intended to be implemented in snapshot GNSS receivers widely adopted in smartphones and Internet of Things (IoT) devices, where the continuous processing of GNSS signals is not feasible due to high computational load and battery consumption. Therefore, the proposed technique is referred as *snapshot OSNMA*. It is envisaged following a client-server approach whereby the user gathers a snapshot of the Galileo E1-B signal, extracts a few unpredictable symbols and sends them to a remote server where their authenticity is analyzed and reported back to the user. The problem is formulated using an equivalent Binary Symmetric Channel (BSC) interpretation, where the performance is determined by the probabilities of error at the spoofer and the user sides.

In particular, this document extends the discussion to derive the theoretical foundation of this client-server based *snapshot OSNMA*, evaluates the feasibility of this concept and validates the detector employing real-like GNSS signals. Intricately, the overall study comprises of four main components. The first component is about the boundary conditions that refer to

the study of sources of symbol errors other than spoofer for instance, signal impairments such as thermal noise, multi-path, synchronization errors, shadowing and blockage in urban and suburban environments, time uncertainties. The study of these conditions helps identify either the contribution of symbol errors from these impairments or the spoofer and thereby develop a lower bound at which the detector would be able to work efficiently. Second component corresponds to characterize the statistical properties of *snapshot OSNMA*. This results in further optimizing the detection performance of the proposed detector. Third component comprehensively focuses on the impact of time uncertainties in detecting the spoofing attack at symbol level. These time uncertainties could appear as a result of various factors such as receiver clock offset or satellite clock offset, etc., and have an impact on overall detection performance. While the fourth component explicitly performs the experimental analysis by generating the real-like Galileo E1-B signal using GNSS simulator i.e., Skydel GSG 8 and then employing these signals to validate the performance of *snapshot OSNMA*. The performance results state that the approach is robust to detect sophisticated attacks even in favorable conditions at the spoofer side. Therefore, it becomes a valuable candidate for the exploitation of OSNMA in GNSS receivers where neither continuous processing of the GNSS signal nor OSNMA-enabled capabilities are implemented.

Keywords: OSNMA, anti-spoofing, snapshot receivers

Acknowledgement

This Ph.D. journey was actually a high speed roller coaster ride which comes to an end in the form of valuable Ph.D. dissertation. In fact, this is not the end; it is just a beginning to excel into professional career with the capabilities that I accomplished during my Ph.D. The output is not just the Ph.D. dissertation but a competent person with the accomplishments of excelling into market, taking things in critical ways and in all other perspectives of life.

In this crafted journey, I would like to express my gratitude to Prof. José A. López-Salcedo for his contribution throughout who supported me from my relocation in Ph.D. to the end. I am truly grateful for those explanatory technical emails that he used to write with the valuable suggestions and assist me understanding the concepts by correlating them with the daily life examples which helped me to take research problems in ultra-critical ways. His efforts on improving my academic writing capabilities is exemplary as well. Moreover, I am thankful to Prof. Gonzalo Seco-Granados for supervising this work and the colleagues who are always up for the discussions of research problems.

Taking into account the technical contributions, I am thankful to our former colleague Sergi for his contribution on the Symbol Error Rate (SER) for the cases in urban and sub-urban environment. I also appreciate my colleague Alda for assisting me in the administrative process due to language barrier. Moreover, I am grateful to the Qascom team, in particular Carlo Sarto and Luca Canzian, for proposing to investigate the *snapshot OSNMA* concept in the framework of the EUSPA-funded OSNMA+ project[1], which provided a professional framework where this research could be applied. Also, to Ignacio Fernandez-Hernandez (DG-DEFIS, EC) for his valuable suggestions on the

[1]This work was supported in part by the OSNMA+ project funded by the European Union Agency for the Space Programme (EUSPA) under contract GSA/GRANT/03/2019/02, and in part by the Spanish Agency of Research (AEI) under the Research and Development projects PID2020-118984GB-I00/ and PDC2021-121362-I00/AEI/10.13039/501100011033.

snapshot OSNMA concept.

Last but not least, I am obliged to my family especially mother, father and siblings back in Pakistan and my spouse who supported me emotionally since living abroad without family for a long period and visit them only after years is really tough. Despite all the odds, they supported and motivated me to accomplish my goals. I am grateful to my friends living and working in different countries for being available any time whenever I need them regardless of problem either to solve the technical research problems or daily life problems which is actually a massive support from them.

Chapter 1

Introduction

Services relying on Global Navigation Satellite Systems (GNSS) are widely present in many market segments ranging from consumer solutions, road transportation and automotive, aviation, maritime, emergency response, agriculture and critical infrastructures, just to mention a few [23]. With the potential of providing the precise positioning and time information, and the widespread availability of GNSS-enabled products, such as smartphones, wearables, and other tracking devices, GNSS has become an integral part of our daily lives. What's more, GNSS has become a vital component of the internet of things (IoT) and smart cities, bringing forth location-based services for connected devices and improving urban infrastructure management. Despite the fact that GNSS is an essential part of such applications and services, security is crucial to fortify the reliability and integrity of location-based services. In this context, spoofing is becoming an increasing threat to GNSS signal integrity, whereby an attacker intends to imitate an authentic GNSS signal to ultimately alter the user's navigation solution. It consists of broadcasting slightly overpowered GNSS-like signals, precisely aligned with the authentic satellite ones, with the intention of taking charge of the Position, Velocity and Time (PVT) solution and eventually forge the user's navigation solution by forcing the user's receiver to lock onto the spoofed signal. Among spoofing attacks, sophisticated ones are difficult to detect since these contain high probability of successful attack due to precisely designed by spoofer. In that sense, the lack of signal authentication poses serious concerns to safety- and liability-critical applications, thus hindering the deployment of GNSS in key emerging sectors.

It is true that the GNSS community is aware of such threat and countermeasures have been proposed at all levels, from the user's terminal to the system level to detect and prevent such attacks. At user terminal, these countermeasures predominantly include using the advanced signal process-

ing algorithms by exploiting the properties of the GNSS signals whereas at system level, Galileo has been the first GNSS to implement a protection mechanism to its open-service signal, the so-called Open Service Navigation Message Authentication (OSNMA). This mechanism is relied on the use of cryptographic data to verify the authenticity of the navigation message (I/NAV) broadcast on the Galileo E1-B signal component. OSNMA is based on the Time Efficient Stream Loss Tolerant Authentication (TESLA) protocol, where the authentication data is conveyed in a set of predictable and, most importantly, unpredictable symbols. During the sophisticated attack, the spoofer attempts to estimate these unpredictable symbols before sending them towards the victim receiver since it can not be known in advance. Nevertheless, the spoofer may incur symbols errors with a non-negligible probability during estimating these unpredictable symbols. Therefore, the key observation is about investigating such unpredictable symbols that can effectively help in identifying a counterfeit signal.

This dissertation investigates the feasibility of signal authentication and spoofing detection by exploiting these unpredictable symbols readily present in the I/NAV message of Galileo E1-B signal component. The concept underlying the spoofing detection is that the attacker strives to estimate the unpredictable symbols in advance and replay the signal towards the user´s receiver. However, during the estimation of these symbols, spoofer could be vulnerable to make errors in symbol estimation. Therefore, a statistical detector is designed which will be able to detect the sophisticated spoofing attack by exploiting these unpredictable symbols. The proposed technique follows a client-server approach whereby the user receiver is responsible for gathering the snapshots of the Galileo E1-B signal, extracts the unpredictable symbols and sending them to a remote trusted server where access to the authentic unpredictable symbols is available, and then comparing both the received and the expected sequences to detect the potential mismatches. The technique is intended to be implemented in snapshot GNSS receivers widely adopted in smartphones and IoT devices, where the continuous processing of GNSS signals is not feasible due to high computational load and battery consumption.

1.1 Research Objectives

Considering the signal integrity and spoofing detection realm, the following objectives are intended to achieve throughout the study.

- Explore the feasibility of leveraging the OSNMA unpredictable symbols for spoofing detection in a snapshot mode.

- Identify and study the factors other than spoofer as boundary conditions that could have analogous impact on the unpredictable symbols because it may impose constraints on detection performance.
- Design a snapshot-based spoofing detector with the statistical characterizations while keeping those boundary conditions into account to detect the spoofing attack under different environments.
- A thorough analysis to examine the performance of proposed snapshot-based spoofing detector and ascertain the shortcomings.
- Investigate the practical aspects of the proposed snapshot-based spoofing detector using open source satellite data to design the wake up strategy for snapshot receiver.
- Validate the proposed detector with experimental data generated using an RF GNSS simulator.

1.2 Research Scope

Spoofing detection in GNSS is gradually becoming a paramount requirement due to the significant increase of occurrence of this type of attacks, which compromise the signal integrity and security. The proposed research technique has a remarkable scope for devices where continuous processing of GNSS signals is not feasible, due to either high computational load or battery consumption. For instance, smartphones, IoT devices and other smart wearables. To counter this problem in most handheld receivers, the proposed technique enables the receiver front-end to periodically switch on for a few hundreds of milliseconds, aiming at reducing the power consumption, and gather a batch of OSNMA unpredictable symbols for spoofing detection, whereas it remains in sleep mode for the rest of time. This is usually referred to as snapshot processing. Since the technique would make use of OSNMA unpredictable symbols, it is therefore named as *snapshot OSNMA*.

Moreover, in the context of OSNMA, the availability of OSNMA data or, in general, I/NAV data, is a concern in spoofing detection techniques that make use of such data provided by existing mass-market receivers. This is due to the fact that, as reported in [24], the availability of I/NAV data in those receivers is currently below 10%, in the best case. It is for the reason that snapshot receivers are thus well-suited for the implementation of the proposed OSNMA based spoofing detection technique, since they circumvent many of the limitations and constraints of conventional receivers that try to

fully decode the whole I/NAV message. Instead, snapshot receivers can focus on collecting just the short pieces of signal where unpredictable symbols are present.

1.3 Thesis Organization

The overall thesis is structured in following manners:

Chapter 2: This chapter provides a concise introduction to the fundamental mechanism and operational principles of GNSS and newly develop OSNMA service especially designed to counter the spoofing attacks. But before delving into the spoofing , it is essential to comprehend the architecture of GNSS in order to identify the modules where the spoofing attacks can be instigated. Primarily, this chapter particularly comprises of overview of the GNSS signals while emphasizes on Galileo E1-B signal along with encompasses a brief description of the different GNSS complementary segments, for instance, GNSS space segment, GNSS user segment or the processing of GNSS signal at the user receivers and GNSS ground control segment. It also explores the process of estimating the navigation solution in the GNSS receivers. Afterwards, the discussion leads towards introducing the OSNMA fundamentals and mechanism while emphasizing the signal authentication.

Chapter 3: This chapter is dedicated to examining different types of spoofing attacks and accessing their level of dominant impact on the navigation solution to eventually take over the receiver. Subsequently, a very comprehensive literature review is conducted to explore the state-of-the-art anti-spoofing techniques that have been proposed in detecting the variety of spoofing attacks. Ultimately, a special attention is given on the discussion of Security Code Estimation and Replay (SCER) attacks that are known due to their high degree of accuracy which makes challenging to detect these attacks. In response to these attacks, an explanatory overview of OSNMA is instigated in order to highlight how this recently introduced OSNMA technique is capable to counter these kind of replay attacks by employing the unpredictable information, making them more challenging to execute.

Chapter 4: This chapter is inspired from the OSNMA and proposes a client server-based snapshot OSNMA technique which operates at symbol level. This technique aims to detect the sophisticated spoofing attacks by utilizing the unpredictable symbols embedded into I/NAV message of Galileo E1-B signal. To instigate the replay attacks in this realm, the attacker tracks

the signals from the satellites and performs an estimation of the unpredictable symbols, and then send to the victim's receiver. During the estimation process, the spoofer ends up with incurring in a non-negligible probability of error. Therefore, the detection metric of snapshot OSNMA detector relies on comparing the unpredictable symbols received by user receiver with the unpredictable symbols present in the database of trusted server at a given position and time. In essence, at first, this chapter formulates the boundary conditions which intends to analyze the factors other than spoofer that could also be incurred the errors with non-negligible probability. These factors may hinder the detector´s ability to identify weather symbol errors are caused by the spoofer or the other signal impairments. In this aspect, the boundary conditions provide the insights to all the potential impairments, for instance, symbol errors due to receiver noise, overlap of authentic and spoofed signals, multi-path, synchronization errors and the errors due to signal fading, etc. Therefore, examining these contributions of incurring the errors is worthwhile to assess if the proposed detection metric is feasible enough to be opted for detecting the spoofing attack.

After examining the boundary conditions, this chapter comprises on three modules. The first and second module delves into a comprehensive study that performs the feasibility analysis of snapshot OSNMA in the open sky and the urban environment, respectively. The third module focuses on conducting a profound statistical characterization of the proposed detector. This formulation aims to further improve the detection performance by optimizing the statistical properties of the detector even under challenging conditions.

Chapter 5: This chapter further extends the detection performance of the proposed detector by taking into account the timing and symbols errors, where timing errors appear due to various factors, for instance satellite and receiver clock offsets, satellites different propagation times and also the timing errors due to A-GNSS since snapshot OSNMA acquires position and timing information through A-GNSS. All these factors have implications on the synchronization of received unpredictable symbols and the ones present at the server side and thereby overall detection performance

Chapter 6: This chapter investigates the practical like implementation of the snapshot OSNMA by using the simulated signals generated by the Skydel simulator. It conducts simulation of scenarios to validate the snapshot OSNMA formulated in previous chapters and evaluates the spoofing detection with realistic simulated signals considering the RF simulator limitations in the aspects of symbol level spoofed signal.

Conclusion

This chapter provided the brief introduction to *snapshot OSNMA* concept for spoofing detection that mainly proposed in this dissertation. It involved the motivation behind the main idea, research scope of this concept in mass market and the research objectives that are being achieved throughout the document. After all, a comprehensive discussion is instigated about how this dissertation is structured to introduce ease of navigating the desire information of the proposed concept.

Chapter 2

Overview of GNSS

The dependence on GNSS emerges with the highest level of precision than ever in the enormous expanse of the modern world, where location and navigation are crucial. From here, this chapter is mainly focused on understanding the working principles of GNSS, delving into the system's foundations, constellation configurations, and signal features, especially the Galileo E1-B signal component [25]. The core of GNSS is its capacity to provide precise global position, velocity, and time synchronization to users. At the center of this technology, is a network of satellites carefully circling our planet, sending messages that user receivers loyally collect and process. These networks, known as GNSS constellations, act as a framework for location, navigation, and timing services, constructing a global network of connection [26].

2.1 Operating Principles of GNSS

This section, at first, provides valuable insights into the overall GNSS system, enhancing the understanding of its fundamental operational principles and the processing stages to ultimately acquired the reliable navigation solution. The second part delves into the OSNMA fundamentals in order to understand the signal authentication paradigm. This discussion is actually pivotal in identifying the attributes which snapshot OSNMA exploits to counter the spoofing attacks.

2.1.1 Description of Constellations

This subsection explains four main GNSS constellations utilized worldwide: GPS, GLONASS, Galileo, and BeiDou. Each constellation possesses its unique qualities, amplifying their overall efficacy and global scope. The GPS

constellation, consisting of 31 satellites (24 operational satellites, 95% of the time), is meticulously managed by the US Department of Defense. These satellites, stationed in six orbital planes, circle the Earth at an approximate height of $20,200$ kilometers. GPS is broadcasting signals in the L1, L2, and L5 frequency bands, provides positioning accuracy between 5 and 10 meters at the widely used L1 frequency (1575.42 MHz), while L2 and modernized signal L5 signal operates at the frequencies 1227.60 MHz and 1175 MHz with the accuracy of 1 to 2 meters and 30 centimeters to 1 meter respectively. This accuracy makes the later one highly suitable for precise positioning applications [23].

GLONASS, a Russian GNSS, proudly boasts its constellation of approximately 24 active satellites [23]. These satellites, arranged in three orbital planes at a height of approximately $19,100$ kilometers, transmit signals in the L1 and L2 frequency bands. The L1 frequency (1602 MHz) provides positioning accuracy on par with GPS, making GLONASS a robust global coverage provider, primarily catering to Russia and its surrounding regions, with expanding reach through international cooperation.

The European Union (EU) and European Space Agency (ESA) join forces to bring forth Galileo, an independent GNSS system. With a mission to provide worldwide positioning services of unparalleled precision and reliability, Galileo's signals span across various frequency bands, including E1, E5, and E6 [27]. Its constellation comprises over 24 satellites in full service, elegantly distributed in Medium Earth Orbit (MEO). The E1 frequency (1575.42 MHz), akin to GPS L1, serves as a vital component in positioning applications. Galileo sets itself apart with advanced features such as enhanced accuracy, robustness against interference, and authentication capabilities, propelling GNSS technology to new horizons.

China's contribution to the GNSS realm comes in the form of the BeiDou Navigation Satellite System, commonly known as BeiDou. Its constellation, a synergy of MEO and Geostationary Earth Orbit (GEO) satellites and Inclination Geosynchronous Orbit (IGSO), aspires to achieve global coverage. BeiDou encompasses a diverse array of satellites tailored for positioning, regional coverage, and Satellite-Based Augmentation Systems (SBAS). Operating in the B1, B2, and B3 frequency bands, BeiDou signals find their position. The B1 frequency (1561.098 MHz), much like GPS L1, is dedicated to non-military purposes. BeiDou, with an invincible devotion to growing global coverage, principally provides location and navigation services throughout China and the Asia-Pacific area [28, 29].

As these GNSS constellations intertwine, users are provided with a profusion of satellite signals, elevating precision, availability, and dependability. Receivers have the ability to connect multiple constellations simultaneously,

enhancing performance and resilience, particularly in challenging environments overwhelmed by obstacles or signal interference. Each constellation's distinctive properties contribute to the variety of GNSS capabilities, enabling an extensive array of applications across the globe. These satellite signals, the essence of GNSS, carry critical data essential for navigation and positioning. Distinguished by their modulation techniques, frequency bands, and structural characteristics, these signals exhibit a remarkable depth. They comprise a carrier wave modulated by a spreading code, facilitating precise temporal synchronization and enabling receiver differentiation among multiple satellites. In a multi-satellite constellation environment, spreading codes provide each signal with a distinct profile, allowing the receiver to discern and track individual spacecraft. But these transmissions do not stop at modulation alone; they carry within them vital navigational data. This data, an enormous information, includes time corrections, satellite ephemeris, and other critical parameters required for exact user position determination. The GNSS receiver majorly depends on this abundance of information to discover the secrets of exact locating and precise tracking time. The detailed description of GNSS constellations are provided in Table 2.1.

Table 2.1: The description of GNSS constellations

Parameters	GPS	GLONASS	Galileo	BeiDou
No. of Satellites	31	24	24	35
Orbit(s)	MEO	MEO	MEO	MEO, GEO, IGSO
Orbital Planes	06	03	03	06
Inclination Angle	55 °	65 °	56 °	55 °
Altitude	20,200 km	19,100 km	23,222 km	21530, 35786,35786 km,
Time Scale	GPST	GLONASST	GST	BDT
Coordinate System	WGS 84	PZ90	GTRF	CGCS 2000

*GPST = GPS Time, GLONASST = GLONASS Time, GST= Galieo Time, BDT= BeiDou Time,

WGS= World Geodetic System, PZ= Parametry Zemli, GTRF= Galileo Terrestrial Reference Frame, CGCS= China Geodetic Coordinate System.

2.1.2 GNSS Signals

Amongst the several group of GNSS signals, as discussed in preceding subsection, Galileo E1 signal emerges with a noteworthy significance. Therefore, the main focus of this dissertation revolves around the Galileo E1-B Open Service (OS) signal, is recently modified with the Navigation Message Authentication (NMA) scheme in the I/NAV message. However, to broaden

the view, the overview of other GNSS signals are also briefly discussed in Table 2.2. Operating within the GPS L1 frequency range, Galileo E1 signal is composed of three channels: A, B, and C. E1-A offers a Public Regulated Service (PRS), accessible to government users therefore, it is a restricted access signal as its ranging codes and navigation data are encrypted. The other component is E1-B which represents the data signal since it is modulated by the navigation data and hence NMA is being provided in this component while the third component represents the data-free signal E1-C, also called a pilot signal. It is made of a ranging code only, not modulated by a navigation data stream. The E1 signal is characterized by a code length of 4092 with 1023 MHz chipping rate resulting in a repetition rate of 4 ms. For the pilot signal, an additional secondary code of length 25 chips extends the repetition interval to 100 ms [25]. Notably, leveraging Composite Binary Offset Carrier (CBOC) modulation which is a combination of BOC(1,1) and BOC(6,1) modulations, E1 signal exhibits enhanced resilience against interference and multipath, fortifying its integrity amidst the noise of the world.

Table 2.2: The general overview of the GNSS signal operating frequencies

No.	GPS	GLONASS	Galileo	BeiDou
1	L1 C/A (1575.42 MHz)	L1 CA (1602 MHz)	E1 (1575.42 MHz)	B1I (1561.09 MHz)
2	L2C (1227.60 MHz)	L2 C (1246 MHz)	E5a (1176.45 MHz)	B2I (1207.14 MHz)
3	L2 P (1227.60 MHz)	L3 OC (1202 MHz)	E5b (1204.17 MHz)	B3 (1268.52 MHz)
4	L5 (1176.45 MHz)	N/A	E5 AltBoc (1191.79 MHz)	B1C (1575.42 MHz)
5	N/A	N/A	E6 (1278.75 MHz)	B2a (1176.45 MHz)

2.1.3 GNSS System Description

The Space Segment (SS), Ground Segment (GS), and the User Segment (US) make up three primary segments of the GNSS. Each component is essential to the GNSS system's smooth operation and precision positioning capabilities. This subsection elaborates these primary segments as given in Figure 2.1, enhances comprehension of the operating mechanism of GNSS.

2.1.3.1 Space Segment

The constellation of satellites that circle the Earth and provides ranging signals and data messages to user terminal, ultimately useful to provide navigation, is referred to as the space segment. It comprises of numerous satellites

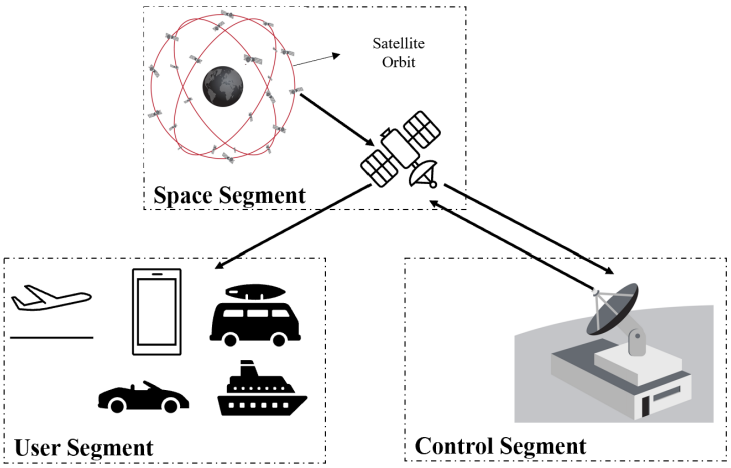


Figure 2.1: GNSS System Architecture: space segment, ground control segment and user segment.

that are carefully positioned in orbit to offer worldwide coverage [30]. The space segment's salient features include:

- **Satellite Constellation**: Every GNSS, including GPS, GLONASS, Galileo, and BeiDou, has its own constellation of satellites. In order to maintain continuous coverage, these constellations often include several satellites in different orbital planes as discussed in preceding subsection in Table 2.1.
- **Satellite Orbits**: The GNSS satellites follow precise orbital planes and altitudes as they round the Earth. For instance, although GLONASS and BeiDou employ a combination of MEO and GEO satellites, GPS and Galileo use MEO.
- **Satellite Construction**: GNSS satellites are built to resist the harsh conditions of space and maintain accuracy over long periods of time. They have onboard sensors for orbital determination, precise atomic clocks for exact timing, and communication systems for signal transmission to user receivers on Earth.

2.1.3.2 Ground Segment

The management and oversight of the GNSS satellites are carried out via network of control centers, ground-based tracking stations, and related equipment, together referred to as the ground segment [31]. Its essential parts consist of:

- **Control Centers**: The operation of the satellites is monitored and managed by control centers. They oversee operations like satellite configuration, orbit calculation, synchronization of the clocks, and satellite uploading of navigational data.
- **Tracking Stations**: To receive signals from the GNSS satellites, ground-based tracking stations are placed in key locations all over the world. The positions of the satellites, the strength of the signal, and other factors required for accurate positioning computations are tracked and observed by these stations.
- **Data Processing Centers**: Tracking stations and control centers deliver the collected data to data processing centers. To produce accurate navigation data, they carry out data analysis, orbit determination, clock adjustments, and other calculations. The satellites then receive this data for broadcast to user receivers.

2.1.3.3 User Segment

The user segment of the GNSS system encompasses the GNSS receivers utilized by individuals, land and air-transport, IoT and various other applications to receive and process signals from GNSS satellites are included in the user segment [32]. The user group consists of:

- **User Receivers**: Systems or devices that receive and process GNSS signals are reffered as user receivers. They may be handheld gadgets, receivers installed on vehicles, or components designed into other machinery. In order to determine the position, velocity, and time of the received signals, user receivers process algorithms and perform specific procedures.
- **Antennas**: Antennas are a crucial component of user receivers and are in charge of GNSS signal reception. They concurrently collect signals from several satellites and send the signals to the receiver for further processing.
- **Applications**: The user segment includes a wide range of GNSS-related applications. These include precision agriculture, timing synchronization, location-based services, surveying and mapping applications, and navigation systems for air, sea, and land vehicles [33].

For the GNSS system to operate properly, interaction between the space segment, ground segment, and user segment is essential. The ground segment

monitors, controls, and distributes data to assure the accuracy and availability of the signals, which are transmitted by satellites in the space segment. In order to establish precise locations and other pertinent information, the user segment receives and processes the signals. Global users now have access to precise positioning and navigational capabilities thanks to this cooperative effort [34].

2.1.4 GNSS Receiver Architecture & Signal Processing

The user segment is mostly comprised of GNSS receiver that are responsible for processing the received GNSS signals in order to calculate the navigation solution. The architecture of a GNSS receiver consists of multiple components that actually collaborate to perform different operations to process those received signals. A GNSS receiver's antenna, RF front-end, and baseband processing are its essential elements [35, 36].

Antenna: A GNSS receiver's antenna is an initial component that engages with GNSS signals. Its primary function is to catch the signals transmitted by satellites. The antenna concurrently collects signals from several satellites and transforms those signals into electrical impulses. A GNSS antenna's essential features include:

- **Multiband Operation**: In order to receive signals from several GNSS constellations, GNSS antennas are sometimes built to function over numerous frequency bands (e.g. E1 and E5, or L1 and L2).
- **Gain and Radiation Pattern**: The gain of an antenna dictates how well it can pick up the radio wave signals, while the radiation pattern affects how sensitive the antenna is to signals coming from various directions.
- **Multipath and anti-jamming techniques**: Modern GNSS antennas use filtering and nulling techniques to reduce the impacts of interference, jamming, spoofing and multipath. The comprehensive discussion about spoofing detetction at antenna level is provided in forthcoming chapter.

RF Front-End: The Radio Frequency (RF) front-end is in charge of handling the electrical signals that the antenna sends out. It carries out a number of crucial tasks, such as:

- **Amplification**: To make the weak electrical impulses from the antenna strong enough for processing, the RF front-end amplifies them.

- **Filtering**: To make sure that only the GNSS signals of interest are analyzed, it filters away undesired signals, noise, and interference.
- **Frequency Down conversion**: To make baseband processing of the RF signals easier, the RF front-end down converts the RF signals to a lower frequency range.

Additionally, Low-Noise Amplifiers (LNAs), filters, mixers, and frequency synthesizers are typical parts of the RF front-end.

2.1.4.1 Link Budget

Prior to delving into signal processing of GNSS signals and to understand the performance of satellite signal reception in GNSS receivers, it is essential to understand the link budget. This term takes into account the performance gains and losses along the entire signal transmission path, from the satellite to the receiver. The link budget examines the effects of noise and interference on the received signal quality, and thus helps in determining the received signal strength [37, 38].

The main components of the link budget are:

- **Transmit Power (P_t)**: Transmit Power measures the strength of the satellite's signal transmission. The value of this parameter is often classified.
- **Free Space Path Loss (FSPL)**: Satellite signals lose strength as they travel through space as they travel longer distances. The inverse square law governs this loss, also known as the free space path loss. The FSPL is represented by the following equation, based on the distance between the satellite and the receiver r.

$$\text{FSPL} = \left(\frac{\lambda}{4\pi r}\right)^2 \tag{2.1}$$

- **Antenna Gain (G_t and G_r)**: The ability of satellite and receiver antennas to focus and direct transmitted and received signals is called antenna gain. Better link performance and reception is a result of higher antenna gain.
- **Cable Loss and System Loss**: The power loss that occurs when a signal traverses the transmission cable between the antenna and receiver is called cable loss. For instance, losses in connectors, filters, and other system components are considered system losses.

- **Atmospheric Loss**: As the signal passes through the Earth's atmosphere, it is further attenuated by atmospheric gases, precipitation, and other weather-related variables. The frequency and environment of infection influence these losses.

- **Receiver Noise Figure (NF)**: This statistic indicates how much noise the receiver mixers and amplifiers add to the system. High sensitivity and low noise contribution to the received signal are indicated by a low noise figure.

- **Signal-to-Noise Ratio (SNR)**: SNR measures the strength of the received signal compared to background noise. It indicates the quality of the signal and can be estimated by the ratio of signal power P_s and P_n and noise power given in the following equation.

$$\text{SNR} = \frac{P_s}{P_n} \tag{2.2}$$

- **Carrier to Noise Ratio (C/N_0)**: The carrier to noise ratio is another parameter to measure the strength of received GNSS signals. Unlike communication system, this metric is often preferred over SNR in GNSS system. This is because SNR relies on the receiver bandwidth B, but the bandwidth of a GNSS receiver is not fixed, which makes it as a confusing metric to compare the performance from difference receivers. In contrast, the C/N_0 compensates this bandwidth factor and therefore solves this difficulty. The C/N_0 can be computed as,

$$C/N_0 = \text{SNR} \cdot B \tag{2.3}$$

The link budget takes into account these variables to determine the received signal power and C/N_0 at the receiver. If the received signal power exceed well better than the noise level and meets the SNR threshold required for signal demodulation, the receiver can effectively analyze the signal and extract navigation data.

2.1.4.2 Intermediate Frequency (IF) Signal Processing:

The received RF signals are further processed and analyzed at the baseband processing level in order to derive pertinent data for positioning and navigation. It entails the crucial operations such as signal acquisition, signal tracking, decoding of navigation data and finally provide the Position Navigation and Timing (PNT) solutions as shown in Figure 2.2.

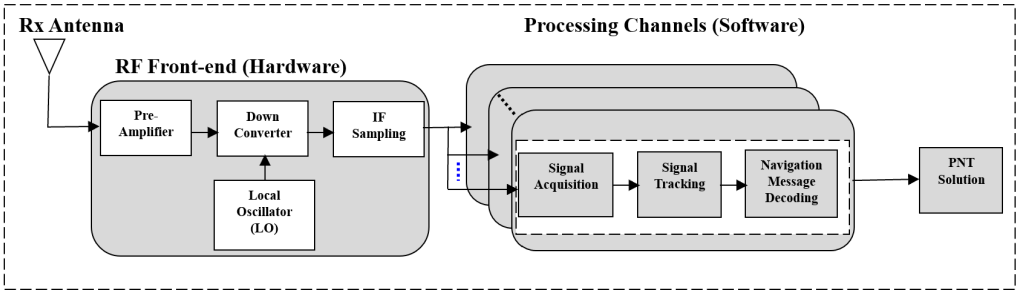


Figure 2.2: Block diagram of GNSS receiver processing.

In order to initiate these operations, the typical received discrete-time signal at the GNSS receiver after sampled and quantization can be written as [39].

$$r[n] = \sqrt{C}x[n-t]e^{j(2\pi vn+\theta)} + w[n] \tag{2.4}$$

where C is the bandpass or RF received power, the exponential term represents the In-Phase (I) and Quadrature (Q) components of the received signal, while t and v correspond to the time delay and the sum-up frequency error including Doppler effect and the clock offset of local oscillator respectively and θ is carrier phase.

2.1.4.3 Signal Acquisition

In order to recognize and synchronize with the GNSS signals, the baseband processor module performs signal acquisition. Acquisition is the first stage of signal processing in GNSS when the receiver detects a satellite signal and attempts to latch on to it. This entails locating GNSS signals, coarsely determining their characteristics (such as carrier frequency and code phase) by correlating the received signal samples $r[n]$ with its local counterpart $c[n]$ using tentative time delay t' and frequency shifts v' which gives a matrix of time-frequency corresponding to all tentative values whereas the maximum of this time-frequency search matrix gives the correlation peak. The general mechanism of signal acquition and thereby correlation peak, is depicted in Figure 2.3

In case, the received signal power is too low, increasing the correlation time has some implications and is essential to be able to detect the signal since longer observation time improves the energy and therefore, enhance the ability of signal to be detected. This increment in the correlation time is referred as Coherent Integration (CI) i.e. $R_c(t', v')$. However, keep extending

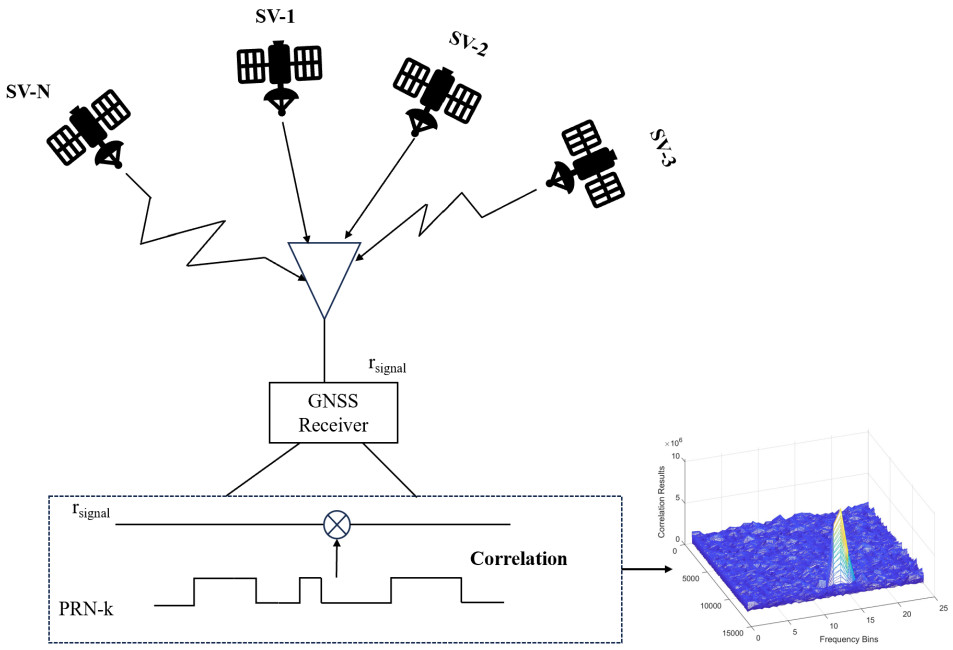


Figure 2.3: The basic principle of signal acquisition.

the correlation time for a long period suffers from constraints can not be extended due to some bounds, for instance the presence of data modulating bits which restrict this time to the bit period. Otherwise, it may face the presence of bit transitions [39].

To avoid such constraints, rather than observing signal for such a long time, the total correlation time can be split into N shorter coherent correlations i.e. $R_c(t', v', k)$, where $k = 1, 2....N - 1$ that are non-coherently accumulated. The resultant energy or power measurement is compared to a specified detection threshold to assess whether a signal is there. Non-Coherent Integration (NCI) is less sensitive and precise than coherent acquisition in estimating signal attributes, but it needs less processing complexity.

2.1.4.4 Signal Tracking

The process whereby a GNSS receiver takes the output from the acquisition stage, and constantly fine tunes such coarsely estimated parameters is referred as the tracking of a GNSS signal. A detailed description of the tracking process as follows and depicted in Figure 2.4

- **Input Parameters**: To start tracking, the receiver must first acquire the information of coarsely estimated parameters such as Doppler fre-

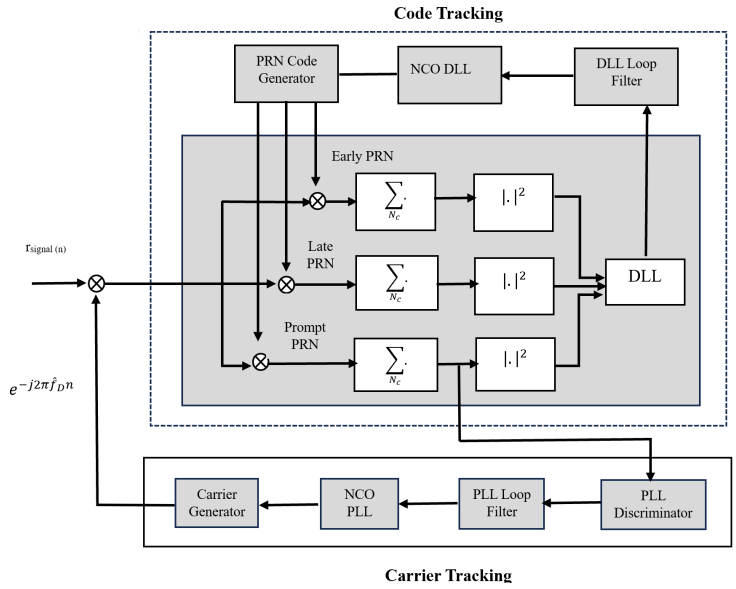


Figure 2.4: The basic principle of signal tracking [1].

quency and code delay from the acquisition stage. This information is obtained from the previous acquisition stage, and enables the receiver to start tracking on an initial signal lock.

- **Code Tracking**: After the receiver acquires the signal, it enters the code tracking phase. Pseudo-random code sequences, often called spreading codes, are accurately tracked by the receiver during code tracking. Each satellite has a unique spreading code that allows the receiver to identify and separate signals from multiple satellites. To track the code phase, the receiver makes a local copy of the spreading code and compares it with the received signal. The code phase of the local replica is continuously adjusted by the receiver's Delay Lock Loop (DLL) to keep it synchronized with the received signal. This tracking technique compensates for code phase variations caused by receiver motion, satellite motion, and signal propagation effects, etc.

- **Carrier Tracking**: In addition to code supervision, receivers perform carrier tracking. Carrier tracking requires carrier frequency locking and tracking to maintain coherent demodulation of navigation data. To determine the carrier phase and frequency, the receiver creates a local carrier replica and compares it with the received signal. To keep it synchronized with the received signal, the carrier tracking loop changes the phase and frequency of the local carrier replica using the Phase

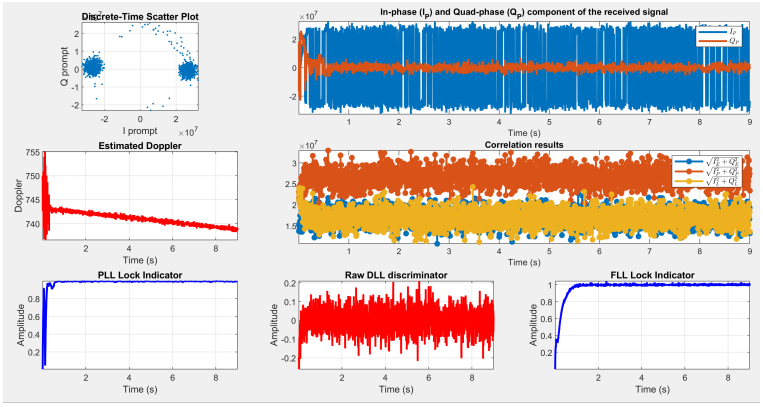


Figure 2.5: Signal tracking with FGI-GSRx software receiver, illustrating PLL, FLL locks on real-like Galileo E1B signal.

Lock Loop (PLL) and Frequency Lock Loop (FLL). Carrier tracking compensates for carrier phase variations caused by atmospheric effects, Doppler shifts caused by satellite movement, and other sources.

- **Data Demodulation**: Once the code and carrier tracking loops are established, the receiver can demodulate and extract the navigation data encoded in the satellite signals. Navigation data consists of information such as clock corrections, satellite ephemeris, and other system-related data. The receiver uses the demodulated navigation data to finally calculate precise position, velocity and time solution.

The tracking process requires continuous monitoring and correction to account for variations in the received signal caused by factors such as signal strength, multi-path interference, atmospheric conditions, and receiver dynamics. It uses advanced tracking techniques and algorithms such as adaptive filtering and signal quality measurements to improve tracking performance and reduce the effects of signal degradation [40, 41] By stable tracking multiple satellite signals, GNSS receivers can pinpoint the position reliably. It is important to note that GNSS receiver tracking mechanisms are sophisticated and involve complex algorithms and control loops. The signal tracking by GNSS receiver as shown in Figure 2.5 by processing real-like Galileo signal with FGI-GSRx software receiver.

2.1.4.5 Navigation Solution

After locking on the signal at the tracking stage and decoding the navigation data, the forthcoming step is to estimate the navigation solution in terms

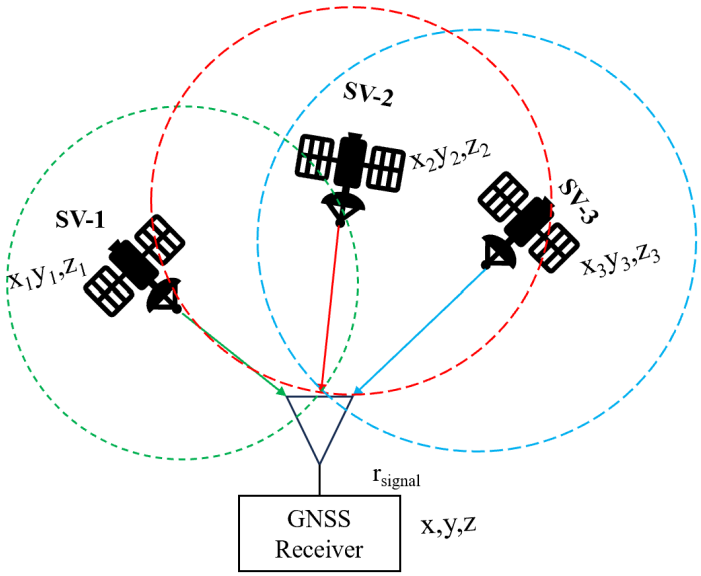


Figure 2.6: Depiction of GNSS positioning principle.

of position coordinates which can be acquired using Trilateration and Least Square (LS) methods. Since GNSS positioning is nothing but actually based on the measurement of distances between a user and numerous satellites to establish the user's actual position. In this essence, Trilateration, unlike its close relative, triangulation, which requires the measurement of angles, is focused on the measurement of ranges or pseudoranges [42, 43]. Delving into the depths, trilateration can be generally illustrated in Figure 2.6 and follows the steps as:

- **Conceptual Foundation**: The intersection of circles (in two dimensions) or spheres (in three dimensions) is the underlying principle of trilateration. Each satellite works as a beacon, emitting a signal to offer the user a range measurement. This trilateration approach is based on the user's position being at the intersection of these range circles or spheres.

- **Range Measurements**: The user receiver gets range data from numerous satellites during trilateration. These data, which indicate the estimated range between the user and each satellite, can be expressed as distances or pseudo-ranges. The pseudo-ranges are commonly calculated by multiplying the time it takes the signal to travel from the satellite to the receiver by the speed of light.

- **Mathematical Formulation**: Trilateration involves determining a series of equations to identify the user's location. A minimum of three satellites is necessary for two-dimensional trilateration, whereas a minimum of four satellites is necessary for three-dimensional trilateration. The equations can be written down as follows with no clock bias for simplicity, as depicted in Figure 2.6

  For two-dimensional trilateration:

$$\begin{aligned} r_1^2 &= (x - x_1)^2 + (y - y_1)^2 \\ r_2^2 &= (x - x_2)^2 + (y - y_2)^2 \\ r_3^2 &= (x - x_3)^2 + (y - y_3)^2 \end{aligned} \tag{2.5}$$

  For three-dimensional trilateration:

$$\begin{aligned} r_1^2 &= (x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2 \\ r_2^2 &= (x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2 \\ r_3^2 &= (x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2 \\ r_4^2 &= (x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2 \end{aligned} \tag{2.6}$$

  In these equations, (x, y, z) represents the unknown user position coordinates, (x_i, y_i, z_i) denote the known satellite positions and r_i signifies the range measurement, or pseudo-range, from the user to the $i - th$ satellite.

- **Solving the Equations**: The set of equations is simultaneously solved to establish the user's position, which requires finding the intersection point(s) of the circles or spheres created by the range measurements. In practice, this is achieved through numerical techniques such as iterative algorithms or linearization techniques.

- **Position Estimation**: After solving these system of equations, the user's location shows as the coordinates x_{final}, y_{final} (for two-dimensional) and $x_{final}, y_{final}, z_{final}$ (for three-dimensional) where the circles or spheres connect. It is the sought-after jewel, a representation of trilateration's achievement.

- **Accuracy Considerations**: While trilateration is a powerful method for determining the user's position, but comes up with challenges such as measurement errors, satellite geometry, atmospheric effects, and receiver biases can all introduce uncertainties and reduce the precision

of the estimated position. Responsively, various techniques such as error mitigation algorithms and advanced positioning methods, are used to mitigate these factors and improve the accuracy of the trilateration solution.

2.1.4.6 Weighted Least Squares (WLS)

The WLS method of position solution is a tremendously powerful approach used in GNSS to precisely calculate the user's location based on multiple measurements from a profusion of satellites. This method uses the weighted least squares idea to minimize the sum of squared residuals between the measured and computed ranges, or pseudo-ranges, resulting in an accurate and dependable location estimation [44, 45]. The complexities of the WLS method:

- **Measurement Equations**:

  The range of pseudo-range measurement from the receiver to each astronomical satellite can be mathematically defined as a function of the user's position (x, y, z) and the satellite positions (x_i, y_i, z_i) in the context of GNSS. These measurement equations provide the relationship between the user's position and the observed pseudo-ranges, and they may be expressed for each satellite as follows:

  $$\text{range}_\text{i} = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} + b_i + e_i \tag{2.7}$$

  where range_i represents the measured range or pseudo-range to the $i - th$ satellite, b_i denotes the ever-elusive receiver clock bias or other beguiling systematic errors and e_i depicts the mischievous measurement noise or error term that attempts to obfuscate our estimation efforts.

- **WLS Objective**: The core of the problem, since the least squares method seeks to minimize the sum of squared residuals between the measured and computed ranges in an artistic way. This goal sets the stage for an exquisite optimization problem that tries to reveal the mysteries of the user's specific position.

- **Linearization**: A bit of mathematical derivation can be used to explain the complexities of the optimization problem. Here comes linearization, a first-order Taylor series approximation wonderfully calibrates the measurement formulas, provide an easier path towards the possible solutions. The linearized equation is written as:

$$\Delta\text{range}_\text{i} \approx (x - x_i)\frac{\partial\text{range}}{\partial x} + (y - y_i)\frac{\partial\text{range}}{\partial y} + (z - z_i)\frac{\partial\text{range}}{\partial z} + \Delta b_i + e_i \tag{2.8}$$

where Δrange_i embodies the residual or the intriguing difference between the measured and computed range, $\frac{\partial\text{range}}{\partial x}$, $\frac{\partial\text{range}}{\partial y}$ and $\frac{\partial\text{range}}{\partial z}$ represent the partial derivatives of the range equation to the user's position coordinates, Δb_i signifies the residual receiver clock bias or systematic error.

- **Matrix Formulation**: An excellent matrix formulation is used to overcome mathematical obstacles and to move forward. Linearized equations are properly rebuilt as matrices, revealing their fundamental concept:

$$\Delta\mathbf{range_i} = \mathbf{A}\Delta\mathbf{P} + \Delta\mathbf{b_i} + \mathbf{e} \tag{2.9}$$

where $\mathbf{A}$, the design matrix, $\Delta\mathbf{P}$, a vector of position corrections, offers a glimmer for precise estimation.

- **WLS Solution**: For each epoch, the least squares approach is used to calculate the receiver coordinates derived from the pseudoranges. This approach can provide an approximation of the receiver coordinates at a given location. The main tasks is to reduce the sum of squared residuals. It can be stated mathematically as:

$$\min\|\boldsymbol{\Delta}\text{range} - \mathbf{A}\boldsymbol{\Delta}\mathbf{P} + \boldsymbol{\Delta}\mathbf{b}\|^\mathbf{2} \tag{2.10}$$

Unlocking this solution involves solving the normal equation:

$$(\mathbf{A^T A})\boldsymbol{\Delta}\mathbf{P} = \mathbf{A^T}(\boldsymbol{\Delta}\text{range} - \boldsymbol{\Delta}\mathbf{b}) \tag{2.11}$$

In this equation, the transpose of matrix A, denoted as A^T, plays a key role in the quest.

- **User Position Estimation**: The user's position can then be accurately predicted. The actual location can be found by applying the computed position corrections to the initial user position estimate:

$$\begin{aligned} x_{final} &= x_{initial} + \Delta P_x \\ y_{final} &= y_{initial} + \Delta P_y \\ z_{final} &= z_{initial} + \Delta P_z \end{aligned} \tag{2.12}$$

Here,ΔP_x,ΔP_y, and ΔP_z represents the computed position corrections in the x, y, and z directions, respectively.

The WLS approach eliminates measurement errors and unveils the complex user position, conquering the global field of GNSS location. Other elements such as satellite geometry, atmospheric impacts, and receiver biases can be accounted for in the least squares solution in actual circumstances to increase position estimation accuracy and precision.

2.2 Security Concerns on GNSS

2.2.1 Motivation

The discussion so far is intended to understand the GNSS fundamentals and working principles emphasizing on Galileo E1-B signal. However, there is an important concern that has gained increased interest in the recent years, and it is the fact that conventional GNSS signal lack any security mechanism. This makes GNSS signals vulnerable to spoofing attacks, which have become more and more frequency due to the facilities for implementing spoofing devices using Software-Defined Radio (SDR) technology. The high occurrence of actual attacks, as reported in the recent literature, has pushed for a rapid and decided development of security countermeasures for future GNSS signals. This is the case of Galileo, where two civil authentication services are being deployed: the OSNMA on the Galileo E1B signal and the Commercial Authentication Service (CAS) implementing spreading code encryption of the Galileo E6C signal. In this chapter we will focus on the former, the OSNMA protocol, whose first experimental tests with the signal-in-space was began in mid February 2021, and which is actually the cornerstone of the present thesis.

2.2.2 OSNMA Fundamentals

OSNMA is the Navigation Message Authentication (NMA) deployed for the Galileo Open Service (OS). This scheme pursues a two-fold objective: firstly, to verify the signal origin and to protect the navigation message from spoofers by using cryptographic methods; secondly, to preserve the same navigation performance to data authenticated users and standard non-authenticated user in terms of multiple factors including time to first fix, accuracy and availability, even in difficult conditions [46]. OSNMA is based on the continuous transmission of cryptographic data that the receiver can use to authenticate the received signal. While this is done at bit level by implementing a series of crytographic operations, the unpredictability of these bits can also be used at signal level to detect the authenticity of the received signal as well. This

is proposed in [17, 47] and further discussed next.

OSNMA is a message authentication protocol and as such, a key or signature is needed to encrypt the message before it is transmitted to the receiver. In general terms, there are two possible ways to do so either by following a symmetric or an asymmetric scheme:

- **Symmetric**: It is based on sharing a secret key by both transmitter and receiver, and being a "secret" key, the receiver must store it into a security module, which becomes a serious concern in case the receiver is lost.
- **Asymmetric**: It is based on a private key that is only known and used by the transmitter for authenticating the message and a public key that is distributed publicly and used by the receiver to verify the message authenticity.

Asymmetric schemes are clearly preferred to avoid security concerns at the receiver side, since the latter does only need to have access to the public key. In particular, OSNMA follows a hybrid symmetric/asymmetric approach based on the TESLA protocol. The main properties of the TESLA protocol are [46]:

- Low computation overhead for the generation and validation of authenticated data.
- Low communication overhead.
- Strong robustness to data loss, which is convenient for GNSS receivers in reduced visibility environments.
- Optimal for multicast transmissions (one-to-many) as it is the case of GNSS.

Based on this properties, the principle behind the TESLA protocol is based on the transmission of the so-called "Message Authentication Code" (MAC) to authenticate a message, and on the delayed transmission of the key used to compute such MAC. The delay between the transmission of the MAC and the key should ensure that the key is unknown until the message and MAC is already received, and therefore it cannot be used by a spoofer to generate the MAC in advance.

The key used to compute the MAC belongs to a chain generated through a one-way function denoted herein as "F". The chain starts with a random seed key K_n, which is secret, and ends with a root key K_0, which is public and can be obtained from any random seed as $K_0 = F^n(K_n)$. That is, by recursively

applying the one-way function "F". For improved security, the symmetry of the recursions can be broken by adding additional information (e.g. a counter or a time tag) to the hashing process. Furthermore, the key size can be reduced by truncating the hash output to reduce the communication overhead. An example of a one-way function is a hash function (e.g. $SHA-256$), so the chain can be constructed by hash in the previous elements.

For the TESLA protocol to operate successfully and provide security, two main requirements must be fulfilled:

- The receiver must be loosely synchronized with the transmitter in order to properly process the message, MAC and keys.
- Another authentication system is needed at start-up, so the receiver is required to have an authentication root key.

Based on these principles and requirements, the OSNMA authentication carried out at the receiver is based on the following steps [48, 49]:

- The receiver receives the navigation data and MAC on which TESLA protocol is based, to authenticate the plaintext message.
- Later, the receiver receives the key that was used to generate the MAC.
- The receiver authenticates the key with the previous key from an authentic chain, or from the root key by recursively applying the one-way function "F".

The specific features of the TESLA protocol that has been applied to GNSS through the OSNMA protocol are:

- A single one-way chain is used for all satellites, in contrast to the standard TESLA approach where each satellite would use a different one-way chain.

The reasons to use a single chain for all satellites are:

- To drastically reduce the Authentication Error Rate (AER).
- To reduce the communication overhead.
- To help in the initialization, as only one root key is needed for all satellites. This is particularly useful when one or a few satellites are received in good condition while all the rest are received in poor conditions due to low elevation, multipath, blockage, etc.

- Several MACs can be associated with each key, thus allowing cross-authentication of some satellites by others.

In the coming chapters, the unpredictability conveyed in some of the OSNMA data symbols will be exploited as a way to eventually detect potential spoofers. This technique is by no means a by-pass of the actual OSNMA protocol, but just a simple way for snapshot receivers (i.e. receivers only capable of gathering a very short piece of GNSS signal) to have some degree of protection against spoofing attacks, without the need of processing all the many-seconds-long OSNMA data. The technique will be described in detail in Chapter 4.

Conclusion

To delve into the insights of spoofing and the corresponding anti-spoofing techniques, it is first needed to have some basic knowledge on the GNSS stages and working principles at which spoofing could be instigated and detected. From this perspective, this chapter overviewed the operating principles of GNSS that includes the description of GNSS constellations in space and the corresponding GNSS signals especially E1-B. In turn, the GNSS system description comprises the space, ground and user segments. And finally, the focus has been placed on the GNSS receiver architecture and its working stages, in particular the signal acquisition, signal tracking, and navigation stages. This will help us in understanding the signal processing stages that, later on, could be exploited to detect the potential spoofing attacks. Additionally, this chapter instigated the discussion on how E1-B signal is being evolved by introducing OSNMA framework in supporting authentication against spoofing. This is important to know since snapshot OSNMA exploits OSNMA unpredictable information to detect the spoofing attacks.

Chapter 3

Spoofing Attacks and Countermeasures

The wide adoption of GNSS has enabled location-based services worldwide. However, as the society's dependence on GNSS grows, so does the concerns about spoofing and disruptions to satellite signals. Unfortunately, security was not a built-in feature on GNSS, as already discussed in the preceding chapter. Therefore, and despite some attempts to incorporate security countermeasures in future GNSS evolutions, intentional interference, jamming and spoofing still constitute nowadays a major security concern with the potential for severe economic and defense impacts. By transmitting noise or counterfeit signals within GNSS bands, jammers can entirely immobilize satellite reception over a local area. Therefore developing strategies to detect and mitigate attacks is critical for navigation security [50]. A review of the possible types of attacks and potential countermeasures to mitigate them, will be discussed in this chapter.

3.1 Types of Attacks to GNSS Receivers

This forthcoming subsections provide insights about the type of intentional attacks that are threaten to the widely growing navigation services.

3.1.1 Jamming

Jamming refers to the actions deliberately taken by the attacker to disrupt or block the reception of GNSS signals leading to denial of navigation services. In simpler scenarios, criminals can use jammers to block trucking fleet tracking and cargo surveillance systems for theft. Even inexpensive jamming

devices purchased online can cut off GNSS to any target if sufficient actions to overcome are not available at the user receiver. Defending against jamming first requires effective detection capabilities. For instance, monitoring signal strength and noise can reveal jamming, but subtle attacks may avoid obvious giveaways [51, 52]. Directional antennas can nullify some jammers and can prevent denial-of-service attacks. Additionally, combining GNSS with inertial sensors, celestial navigation, and other augmentation systems provides backup if satellite signals are compromised [53].

3.1.2 Meaconing

The term "meaconing" refers to a procedure where the attacker captures and rebroadcast the delayed authentic satellite signals towards the victim receiver. This ability to record and replay satellite signals with unplanned delays grants meacons harmful control over a victim's perception of location and time. For example, a delayed signal could slowly inject errors in a satellite navigational system, which could distort the timing of a cell phone network or disrupting communications [2, 13]. Meaconing is a serious threat to the security of navigation and communication systems. It can cause significant damage to critical infrastructure, including transportation, emergency services, and military operations. The basic illustration of meaconing is shown in Figure 3.1.

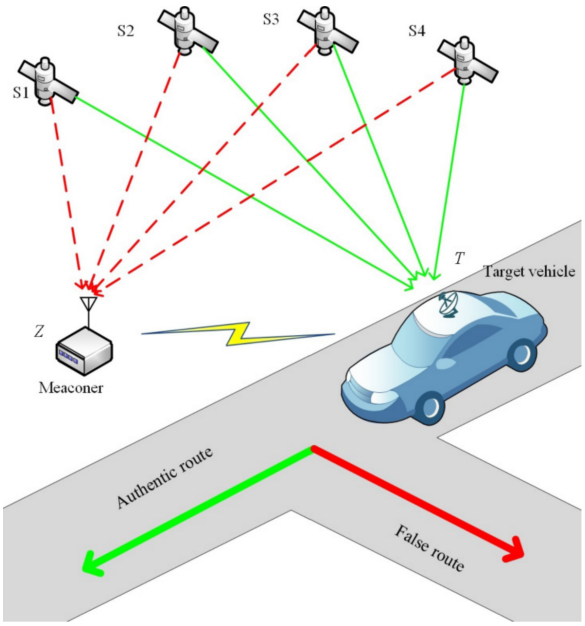


Figure 3.1: Basic workflow of meaconing in GNSS [2].

3.1.2.1 Important Features of Meaconing Attack

- Reception, delay, and rebroadcast of radio-navigation signals.
- It cannot arbitrarily control the PVT of target receivers. Instead, target receivers will be in confusion and see the position and velocity of the meacon and a time in arrears of the actual time.
- It is easy to execute; it needs few RF components without specific software developments.
- It may be possible to detect if the raised delay is not constant due to receiver clock drift.

3.1.3 Spoofing

Spoofing in GNSS refers to the transmission of counterfeit GNSS-like signals, consciously to produce a false position within the victim receiver without disrupting GNSS operations. Figure 3.2 shows the scenario of spoofing attack that sends the false signals at certain power through a GNSS receiver. After that, this spoofed signal combined with the original GNSS signals that tracked from satellites in space at the user´s receiver to take over the victim.

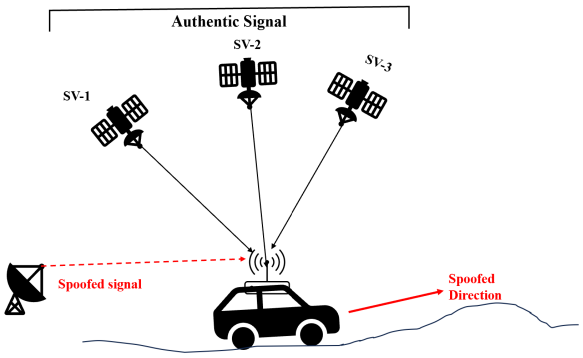


Figure 3.2: Scenario that illustrates the working of spoofing in GNSS.

In GNSS, spoofing attacks fall into three categories: simplistic, intermediate (or shadowed), and sophisticated. However, references may use different names and arrangements based on specific features. These three categories of spoofing attacks provide a general classification based on implementation complexity for each type of threat, including technical details and possible variants. In the following subsections, the three categories are elaborated upon.

3.1.3.1 Simplistic Attack

A simplistic spoofing attack refers to the basic attacks, where spoofer generates counterfeit signal with inconsistencies or within constraint environment, therefore, generally not able to make an attack consistent or time synchronized with the real signal or initiate the attack with high power. More about the discrepancies, it can be affected by rough variations in navigation message or it may only contain information about the satellites that are not visible at the victim receiver at the moment. Taking into account these shortcomings, simplistic spoofing attacks can be easy to tackle and mitigate with simple countermeasures [2]. The important characteristics of the simplistic spoofing attacks and their impact on victim receiver are follows,

- **Hardware Requirement**: The signal simulator combined with power amplifier and RF transmitting front-end.
- **Impact on Victim Receiver**: Counterfeit signal appear as noise and do not sync with real signal. This spoofing attack can cause the receiver to lose its lock frequently in the tracking mode or experience re-acquisition issues.
- **Implementation Limitations**: Use confined signal simulator or commercial component with the limited software developments to perform the attack

3.1.3.2 Intermediate Attack

Intermediate attacks require more expertise and resources than elementary spoofing to execute and properly manipulate authentic GNSS signals. Rather than recklessly broadcasting signals, unlike simplistic attack, the spoofer extracts position, time and satellite information from the signal, align at least the code-phase with the authentic one and then lock over the authentic signal with making slightly overpower the counterfeit signal to successfully implement the intermediate level attack. The important characteristics of the simplistic spoofing attacks are follows,

- **Hardware Requirement**: The custom device specially designed for spoofing or as an alternative modified signal simulator combined with power amplifier and RF transmitting front-end.
- **Impact on Victim Receiver**: The counterfeit correlation peak is aligned with the authentic signal correlation peak. The power of fake signal is then gradually increased to gain control of the victim receiver.

- **Implementation Limitations**: Sophisticated software must be in place at the spoofer side to design the successful attack.

3.1.3.3 Sophisticated Attack

The sophisticated attacks involve the use of multiple coordinated and synchronized receivers to generate the counterfeit signal that comprises of closely resemble with the authentic signal with high accuracy. These coordinated receivers having the potential to generate and transmit the counterfeit signal with the centimeter level precision of position information about their´s and the victim receiver antenna phase centers, making them more challenging to even defeat the complex countermeasures. Hence, cryptography-based authentication techniques are the most effective defense against these coordinated attacks. Since cryptographic measures comprises of security code information that can not be known in advance to the spoofer, however, advanced spoofer could still forge the victim receiver. This is done by preemptively estimating the unknown information in advance and then replay the signal along with the estimated information to gain over the control on victim receiver. This attack is pertained as SCER attack.

This dissertation mainly focused to provide the countermeasures to detect the SCER attacks while the comprehensive discussion about proposed spoofing detector is provided in later sections. The important characteristics of the sophisticated spoofing attacks are follows [2],

- **Hardware Requirement**: Multiple coordinated and synchronized receivers.
- **Impact on Victim Receiver**: At first, the counterfeit signal is accurately aligned with the authentic signal and then the power of fake signal is then gradually increased to gain control of the victim receiver similar to intermediate spoofing attack.
- **Implementation Limitations**: Complex implementation and the effectiveness region is limited.

3.2 State of the Art of Anti-Spoofing Techniques

In the recent years there has been an increasing interest in deriving and developing anti-spoofing techniques for GNSS receivers. The most relevant techniques are briefly summarieed here to further identify their capabilities

and limitations from a spoofing detection perspective. The techniques are classified here depending on the feature or stage of the receiver where they are applied.

3.2.1 Antenna-Level Techniques

Antenna-level techniques can be classified into two main categories. The first one is based on the use of antenna arrays for exploiting the spatial information of the signals arriving to the user's receiver. The second one is based on exploiting the different polarization between authentic and spoofed signals.

3.2.1.1 Array Processing

There are basically two possible strategies that can be opted in the general context of array processing:

1) Combining the antenna outputs at pre-correlation level, using the signal directly coming from the antenna.

2) Combining the antenna outputs at post-correlation level, processing the signal coming from antenna after correlation with the local replica of the satellite of interest. This is the approach best suiting the application of spoofing detection, because GNSS signals are buried below the noise floor and it is not until the correlation with the local replica is done, that they become detectable.

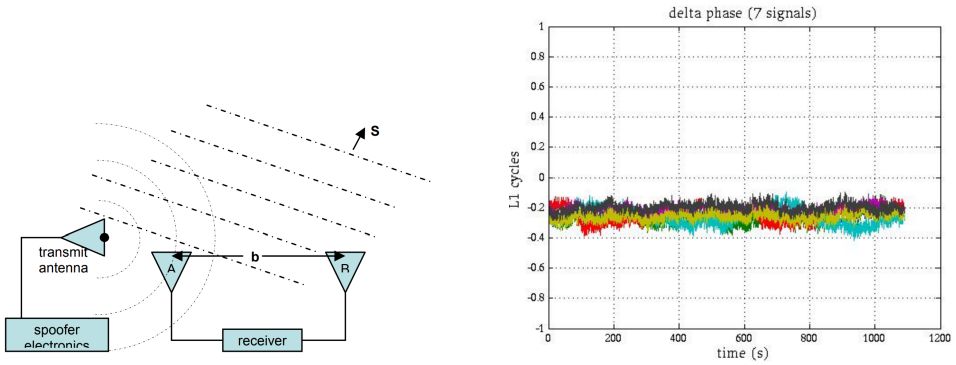
In the context of post-correlation, there are two possibilities could be instigated to detect the spoofing attack:

`Signal-level detection:` Apply beamforming by creating a beam that points towards the direction of a particular satellite of interest while minimizing the power from potential interference/spoofing sources. A deterministic design can be implemented to reduce the contribution coming from low elevation angles, where spoofed signals are likely to come. Alternatively, adaptive designs can also be considered to automatically steer the beam. However, this has the problem that unlike most interference signals, spoofing signals are like satellite signals thus making them two correlated random variables. It is for this reason that it becomes challenging for beamforming techniques to discriminate one from the other unless additional a-priori information is provided.

`Observable-level detection:` This approach involves using the output observables provided by a GNSS receiver when processing the signal coming from different antennas. The most widely adopted case is that of using carrier phase observables. In particular, the difference of carrier phase observables

between antenna pairs for a given satellite under analysis. Such carrier phase difference is composed of two main contributions. The first one contains a phase bias that is specific to the chosen antenna pair. The second one contains a phase term that depends on the angle of arrival of the satellite being processed. The first term is constant for all satellites but the second one varies from satellite to satellite due to their different angles of arrival at the antenna array. It is for this reason that comparing the carrier phase difference between antenna 1 and antenna 2 for all satellites in view, one would expect the result to vary from one satellite to another due to their different angle of arrival. For a spoofed signal this is not the case because all satellite signals are likely to arrive to the antenna array with the same angle of arrival, and thus the carrier phase difference between antenna pairs does not vary but remains constant, thus suggesting the lack of angular diversity in the received satellite signals.

In view of the aforementioned properties, array processing techniques have been proven to be very effective for detecting spoofed signals. However, these techniques are difficult to implement in practice due to the cost and complexity that they involve and are reserved to high-end professional receivers operating in key specific applications. Simpler approaches are possible by restricting the receiver to operate with a simple two-elements antenna array (i.e., a so-called dual antenna receiver) or using the observables coming from multiple single antenna receivers.



(a) (b)

Figure 3.3: (a) Different geometry of authentic satellite signals impinging with a dual antenna receiver compared to a point transmitter on ground acting as a spoofer. (b) Phase differences for 7 satellite signals with the lack of angular diversity, entitled from same transmitter [3].

In [3], for instance, a spoofing detection technique is developed by using

a dual antenna receiver which is based on exploiting the Angle Of Arrival (AOA) of the signals impinging onto the receiver array, as shown in Figure 3.3(a). It can be seen that the satellite signals transmitted by a spoofer arrive at the dual antenna receiver with the same AOA and therefore the aforementioned carrier phase differences must overlay each other except for multipath and phase noise as shown in Figure 3.3(b).

3.2.1.2 Polarization Discrimination

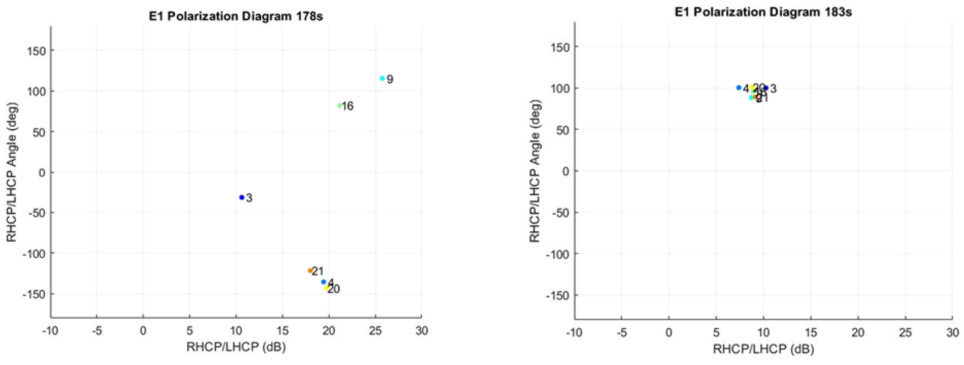
It is well known that GNSS satellites transmit Right Hand Circular Polarization (RHCP) signals and consequently, antennas receiving GNSS signals must be designed accordingly, being RHCP as well. However, the presence of a non-RHCP contribution can provide valuable information on the presence of spoofed signals. On the one hand, some spoofers make use of conventional linearly polarized transmit antennas as those used by many terrestrial wireless communication systems. Such linear polarization could be detected and used to infer the presence of a potential spoofer. On the other hand, even if the spoofer is able to use a RHCP antenna the Electromagnetic Field (EM) associated to RHCP witnesses some degradation. Two different degradations are possible. The first one is due to multipath or reflection factors that cause a non-negligible Left Hand Circular Polarization (LHCP) contribution referred to as cross-polar component. The second one appears when the signal propagates through low elevation angles and causes the circular polarization to be deformed into a close to linear polarization. In any case, the departure from a pure RHCP in the received signal helps in detecting authentic signals (i.e., with pure RHCP) from spoofed ones (i.e., with non RHCP, either LHCP or linear). Such discrimination could be exploited using multiple ways:

`Post Correlation Level:` By using a dual RHCP/LHCP antenna and a GNSS receiver capable of tracking both the RHCP and LHCP signals. Even though authentic signals may be affected by a degradation/deformation of their polarization, such effect is expected to be different for each satellite owing to the fact that each satellite signal arrives at the user's receiver from a different direction, and thus experiencing different propagation effects. In contrast, spoofed satellite signals coming from the same single transmitter do experience all the same propagation effects, and thus the very same degradation/deformation of their polarization. It is for this reason that monitoring the randomness of the RHCP vs LCHP ratio on the received satellite signals becomes an effective tool for inferring the presence of spoofed signals.

`Pre-Correlation Level:` By comparing the power levels coming from a each of the ports of a dual vertical/horizontal antenna that could be rotating

to capture the expected RHCP contribution, but at the same time, gathering the independent vertical/horizontal contributions, separately. In this case one could monitor the power at each of these linearly polarized channels and check whether the corresponding polarization is aligned with the orientation of the spoofed signal polarization or not. If there is spoofed signal, one of these linearly polarized channels would contain most of the power and the other channel would reduce or even loose the signal.

An example of the first approach introduced above on post-correlation level techniques is provided in [4]. A dual polarized antenna having two RF outputs RHCP and LHCP ports is used together with a dual antenna GNSS receiver with two RF input ports. By default, the receiver independently acquires and tracks the signal from each antenna input. However, when used for dual polarization applications, the receiver fails to permanently monitor the LHCP signal because its SNR is often too low to be tracked. Hence, to overcome this limitation, it is proposed to synchronously process both the RHCP and LHCP signals rather than having independently tracking of both components. In order to test this scheme for spoofing detection, [4] implements an intermediate matched power timing attack in which the spoofed signal initially matches the authentic signal but having slightly higher power to take over the loop. Then, the timing of the spoofer is gradually delayed and taking away the tracking loops. In order to detect the spoofing attack, the receiver will compute the correlation values for each signal. The respective polarization vector which is a correlation ratio of RHCP and LHCP is used to visualize the diagram having magnitude and phase along the horizontal and vertical coordinates respectively.



(a) (b)

Figure 3.4: Polarization Diagram (a) Authentic (b) Spoofing transmitter [4].

Based on the polarization vector, it can be seen from Figure 3.4(a), the

large spread of phase and amplitude represents the authentic signals that comes from different directions and the ratios are all uncorrelated while in case of spoofing shown in Fig.3.3(b), it's highly correlated and clustered at one point leading to the successful detection.

3.2.2 Pre-Correlation Techniques

Pre-correlation techniques are intended to detect the spoofing attack before performing the correlation, and they are mainly dependent on power monitoring and variation. Based on it, multiple power-based techniques are discussed which contribute to detect spoofing attacks.

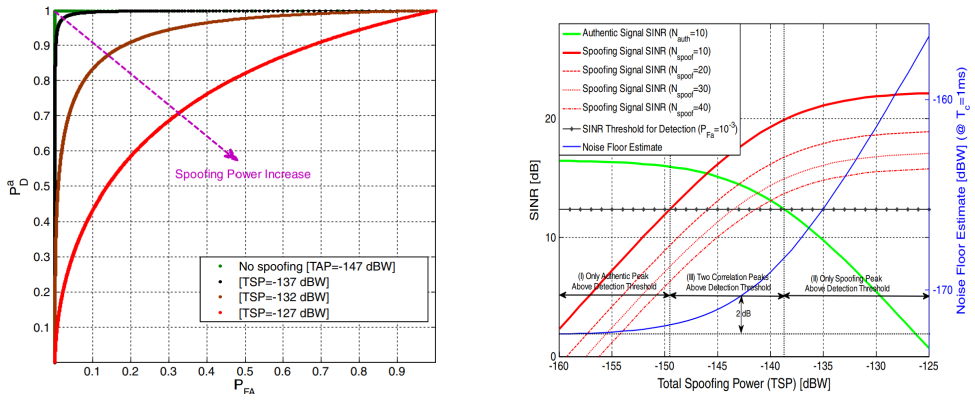
3.2.2.1 Absolute Power Monitoring

The received GNSS signal has a power subject to a predefined link budget that takes into account the power transmitted by the GNSS satellites, the different transmit/receive antenna gains and the losses experienced from the free space propagation. This key feature can be used to recognize the presence of spoofed signals. The reason is that spoofers typically generate signals with a much higher power in comparison with authentic signals in order to take over the tracking loops of the victim's receiver. Hence absolute power observables become a powerful tool that can help in detecting spoofing attacks.

An example is found in [54] where the received signal power monitoring is used to detect counterfeit signals. The starting hypothesis is that the receiver has acquired the authentic signal at first. Based on that, a threshold is computed in terms of reasonable power upper limit that serves to declare a spoofing attack. However, it is are not very reliable because the received power could increase or decrease due to multi-factors including radio frequency interference as well as multipath, obstacles, etc.

Another contribution on absolute power monitoring is provided in [5] where spoofing countermeasures are based on measuring the signal strength and noise power, as a complement to C/N_0 measurements. The main assumption is that the presence of spoofed signals may not significantly change the C/N_0 when they are closely aligned to the authentic signal, but when the signal power and the noise floor are separately monitored, in absolute terms, they can be seen to exhibit a significant change when the spoofed signal appears. Not only because of a higher signal power when the receiver turns to be aligned with the spoofed signal, which is typically of much higher power than authentic signals, but also because even when the receiver is not

aligned with the spoofed signal, the presence of the latter can be perceived as an increase in the overall noise floor.



(a) (b)

Figure 3.5: (a) Probability of detection vs probability of false alarm under different Total Spoofing Power (TSP) (b) Signal to Interference and Noise Ratio (SINR) vs TSP for authentic and spoofed signals [5].

However, spoofing signals are much stronger than authentic signals and therefore their resulting noise floor could easily exceed the ambient noise floor level and thus easily be detected. This can be seen in the blue curve in Figure 3.5(b) where the noise floor estimate is shown as a function of the TSP, which is divided into three regions.

The first one ranges from -160 to -150 dBW of TSP where no spoofing is barely present and the conditions remain the nominal ones. In the second region the TSP ranges from -150 to nearly -140 dBW and it is here where the correlation peak of the spoofed signal starts to be visible. In this region the estimated noise floor is 2-3 dB higher than the nominal one, so the spoofer could be detected by noticing this fact. Finally, the third region ranges for TSP values from nearly -140 to -125 and here the receiver is captured by the spoofed signal. As can be seen, the SNIR in this region has a rather flat behaviour compared to the noise floor, which has a linear increase and thus serves well for the purpose of detecting the presence of a spoofer.

3.2.2.2 Power Variation

Power variation is another factor that could be able to detect spoofing attacks by closely monitoring the variability of power while taking the other interference factors into consideration. By monitoring the variability trend

of power helps the victim to detect the spoofing attack as already discussed in the literature and summarized below.

Power variations can be introduced by spoofers but also due to multipath effects and RF interferences, so the discrimination of these different sources of variations is key to make sure that the threat of interest is being detected. In order to do so and enhance the detection performance, a technique based on the combination of multiple metrics including Automatic Gain Control (AGC), C/N_0 variation as well as multiple correlators is employed in [6] for spoofing detection. That work also provided insights to distinguish between RF interference and spoofing using AGC and C/N_0 variations.

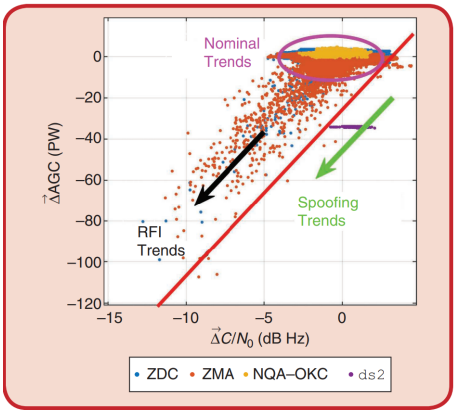


Figure 3.6: Relationship between variations in AGC and variations in C/N_0 in nominal conditions (upper right hand side corner), in the presence of RF interference (lower left hand side corner) and in the presence of spoofing (lower right hand side corner) [6].

The key differentiator factor between RF interference and spoofing is that when a spoofed signal is present, the AGC tends to decrease due to the higher power of the spoofer but the C/N_0 is not so severely affected, experiencing only mild fluctuations around their nominal value as seen in the purple horizontal dots on the right-hand side of Fig.3.6. In contrast, when RF interferences are present, not only the AGC decreases due to the higher power of the interference but also the C/N_0 dramatically drops as shown in the left-hand side of Fig.3.6. Such a different behaviour of the pair (AGC, C/N_0) variations can therefore be used to infer the presence of spoofing attacks.

3.2.2.3 Dual Frequency Power Comparison

Multi-frequency GNSS receivers are starting to be widespread deployed, not only for L1+L2 operation in GPS but also for E1+E5 operation in Galileo, with the advantage that they can resolve the ionospheric contribution and thus provide a cleaner and more accurate position solution to the end user. The availability of an additional frequency can also be used as an additional degree of freedom for spoofing detection, since it is unlikely that spoofers are able to simultaneously spoof in more than one frequency band. Some works in the literature propose to take advantage of the predefined power level difference between GNSS signals in different frequency bands. For instance, the received signal power is not expected to exceed -155.5 dBW and -153.0 dBW, respectively, for the P(Y) and C/A signal components of the L1 band, nor -158.0 dBW for either signal on the L2 band. Such power differences are proposed to be exploited in [55] since most spoofers may only be able to generate a spoofed signal in one frequency band, typically in L1. As consequence, measuring the received signal power in L1 and cross-checking with the signal power level in L2 can provide information on whether the signal being received in L1 is authentic or not. The power comparison can be made by monitoring in multiple ways including absolute power of each carrier, monitoring the signal power changing rate as well as monitoring the relative powers.

An alternative approach proposed in [55] is to cross-correlate the received signal in L1 with the received signal in L2, since they both share at least one signal component, either the C/A or the P(Y). In this way the cross-correlation of the L1 and L2 received signals should provide a correlation peak with a known relative time shift due to the know group delay between both signals. Counterfeiting this property would require the spoofer to simultaneously spoof in both bands and with a specific delay, which is unlikely to be possible for most conventional spoofing devices.

3.2.3 DSP Post-Correlation Techniques

In this section, Digital Signal Processing (DSP) techniques implemented after the correlation of received signal with local replica will be reviewed. These techniques can be classified into multiple categories depending on type of spoofing attack, utilization of observables and their corresponding responses to particular spoofing attack. The most relevant ones are discussed in detail next.

3.2.3.1 Multi-Peak Detection

It is well known that GNSS receivers need to implement the correlation of the received signal with the locally generated replica in the acquisition stage of the receiver and the local replica is generated for a collection of tentative code delays and frequency shift values, seeking for the pair of values that maximizes the correlation output and thus better matches with the actual code delay and frequency shift of the received signal as discussed in previous chapter. This correlation output appears as a peak large enough to exceed by some orders of magnitude the noise floor, thus becoming clearly visible. The orthogonality of the GNSS spreading codes guarantees that in nominal working conditions, there will be only one peak in the acquisition search space because the rest of received satellites are perceived as some background noise from the point of view of the satellite of interest. This unique feature can easily be exploited for spoofing detection because the presence of a spoofed signal, thus having the same spreading code as the satellite of interest, will result in a second correlation peak somewhere in the search space, there were the tentative code delay and frequency shift coincide with those of the spoofed signal. This abnormal situation with two (or more) correlation peaks in the acquisition search space is what the so-called multi-peak detection technique focus on. An example of this latter situation is shown below in Figure 3.7.

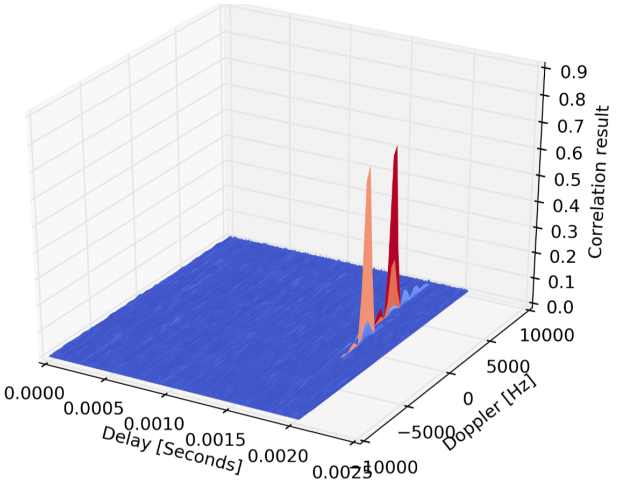


Figure 3.7: The search space in the presence of spoofer (showing in terms of two peaks, one is authentic while other is spoofed) [7].

There are numerous contributions in the literature exploiting the presence of multiple peaks in the acquisition search space. For instance, the work in [8] considers the case where the spoofed signal, when present, can be near or far

away from the authentic correlation peak. When near to the authentic peak, the spoofed peak overlaps the authentic one and leads to an increase of the correlation amplitude since the spoofed power is often much higher than the authentic signal power. When the spoofed peak is far away from the authentic one then it is easy to be identified because there are clearly two correlation peaks visible. Both situations correspond to the case "spoofer present". The second situation corresponds to the case "spoofer absent" where there is only one correlation peak, with the expected height and width. Finally, the third situation corresponds to the case "noise only" where there is neither spoofer nor authentic signal but only noise.

It may be the case that the power of both signals is closed so it leads to overlap the both signals which gives one peak but changes the width of correlation. In order to overcome this limitation, a width threshold is evaluated by using a power threshold and the maximum expected value of the correlation, as visually explained in Figure 3.8.

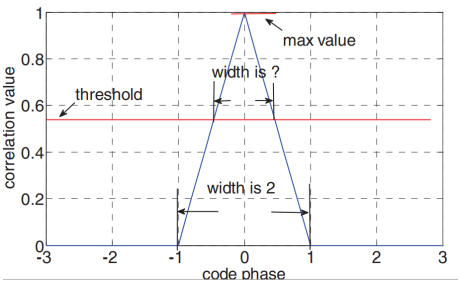


Figure 3.8: Explanation of width threshold for detecting the presence of spoofers [8].

Multi-peak detection can also be combined with other detection metrics such as monitoring the Cross-Ambiguity Function (CAF), i.e., the time-frequency correlation function, as well as the AGC gains, as proposed in [56]. In case of spoofing attack, it is clear that the search space will contain two correlation peaks corresponding to the spoofed and authentic signals, however, there is a side-effect caused by the presence of a high-power spoofer that needs to be accounted for. In particular, as the spoofed signal power gradually increases, the cross-correlation between the spoofed signal and the local replica of the authentic signal start to interfere and gradually exceed the floor noise. This effect is similar to the near-far problem experienced in indoor GNSS applications and it hinders the detection of the correlation peak of the authentic signal, leading to an undetectable zone or even creating false high correlation peaks in other cells of the search space different from the true one. Fortunately, the AGC gains from receiver RF front end can be

used to detect the presence of high-power input signals and assist the spoofing detection mechanism. In summary, combining the multi-peak detection with the AGC gains helps to improve the detection of overpowered attacks.

To conclude, multi-peak detection appears as one of the simplest while most effective techniques for detecting the presence of spoofed signals, particularly for snapshot GNSS receivers that do operate in acquisition mode only. Multi-peak detection has been implemented and tested in practice, and has gained a renewed interest in the recent years as confirmed in [57]. It is therefore becomes one of the strong candidates of anti-spoofing technique to be implemented in this of the present activity.

3.2.3.2 Signal Quality Monitoring

Signal Quality Monitoring (SQM) is considered as one of the most efficient techniques to detect spoofing while having a very low computational cost. The underlying principle of SQM techniques is to monitor the shape of the correlation peak in order to detect potential deformations that could indicate the presence of a spoofed signal overlapping with the authentic one. These techniques have their origins in civil aviation, where it is of paramount importance to monitor the quality of the received GNSS signals due to the criticality of the underlying application. In that case the potential deformations are typically due to propagation effects such as multipath, or to a spureous malfunctioning of the GNSS satellite payload. The latter is very infrequent but can momentarily cause what it is often referred to as "evil waveform", a signal distortion that can introduce persistent errors of a few meters without the receiver loosing lock. The very same principle of monitoring the shape of the correlation peak is applicable to spoofing detection as well, as already pointed out in previous sections. The reason is that the presence of a spoofed signal with very close delay and doppler shift to those of the authentic signal results in an overlap of both correlation peaks, giving rise to an aggregated correlation peak with a distorted shape, as shown in Figure 3.9 This effect is actually the same as the one experienced in the presence of multipath. Actually, multipath replicas arriving at the user's receiver can be seen as an unintentional and spontaneous form of spoofing. It is for this reason that many of the SQM techniques proposed in the literature for multipath detection can be applied to spoofing detection as well.

When the counterfeit signal interacts with the authentic signal, the phase and power of the signal admixture significantly fluctuates at this stage, as well as during the period when the spoofed signal moves away from the authentic signal. Such fluctuation creates the deformation of the complex correlator shape and this abnormality can be used for spoofing detection.

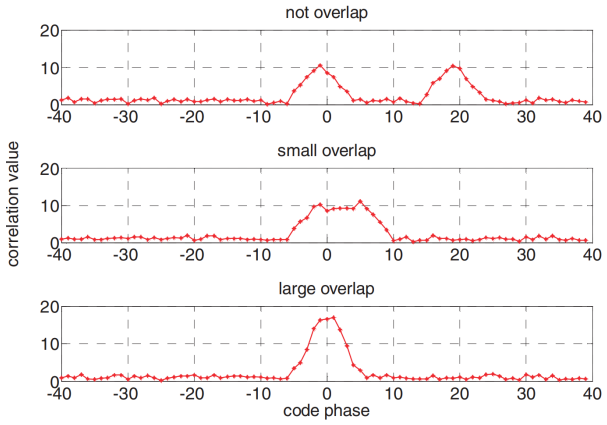


Figure 3.9: Interaction of a counterfeit signal with an authentic one, initially separated apart (upper plot), but gradually approaching (middle plot) until the authentic signal is captured and the aggregated correlation peak is distorted (bottom plot) [8].

Ratio-test SQM: The work in [9] concentrates in the sum ratio where the numerator is taken as the sum of the early and late correlators while the denominator is taken as the prompt correlator multiplied by a scaling factor. The result is referred in this paper as "ratio test", which is a well-known SQM metric whose effectiveness has been widely discussed and demonstrated, but whose application to spoofing detection is addressed in [9]. Ratio metric is defined over non-coherent DLL and the spoofing detection is formulated using a binary testing hypothesis based on the Neyman–Pearson criterion in the absence of noise, in order to focus on the signal content of the early/late/prompt correlators, so that it can be distinguished between the spoofer absent and the spoofer present cases. The first hypothesis is labeled as the ratio test in the absence of spoofing and noise while the second hypothesis is set to be ratio test in the presence of only spoofing signal. In general, a NP decision strategy is based on the computation of the Likelihood Ratio (LR) to be compared against a threshold. In order to evaluate the performance the ROC curve between the probability of detection (P_D) and probability of false alarm (P_{FA}) is visualised, and it can be seen in Figure 3.10. The p_s parameter is the difference in mean of the Ratio test between each hypothesis, normalized to the noise variance. This parameter is therefore an indicator of how close or how far the two hypotheses (i.e. spoofer absent or spoofer present) are.

Goodness of Fit (GoF) SQM

A validation of two statistical tests namely Chi Square GoF and sign

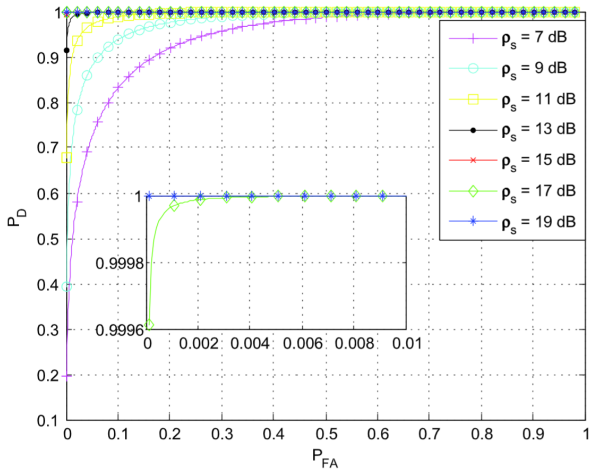
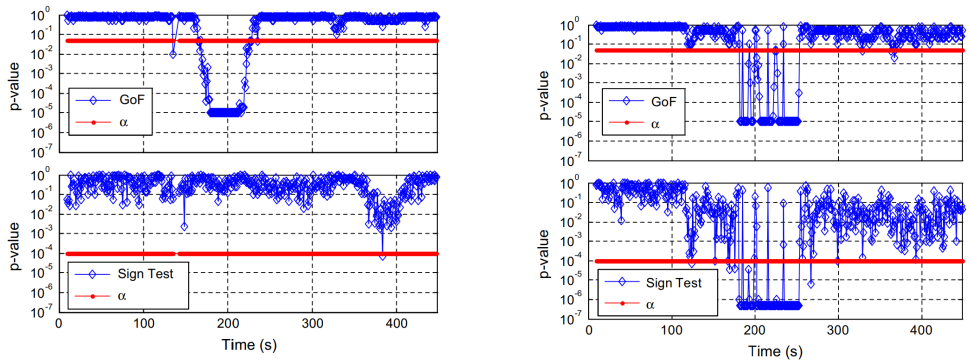


Figure 3.10: ROC curves for different values of p_s [9].

test is presented in [10] where the performance is assessed by means of the well-known TEXBAT dataset comprising five different kinds of spoofing attacks. The main detector analyzed in [10] is the GoF based on the difference between the early and late correlators. Ideally, these two correlators should be identical in the absence of spoofer, so that their difference should become zero. More precisely, when thermal noise is added, the difference should become a zero mean Gaussian random process. The GoF test is therefore comparing whether the measurements available on the difference of early and late correlators fits to this zero mean Gaussian distribution (i.e. no spoofer present) or not, in which case an alarm is raised on the presence of a spoofer. The sign test also considered in [10] tries to ascertain whether the mean of the difference of early/late correlators is zero or not. Both tests are validated on multiple spoofing case in order to assess their performance. The sign test, was unable to detect the overpowered attacks, as shown in the bottom plot on the left hand side of Figure 3.11, because it just checks whether the difference between the early and late correlators is equal to zero. In overpowered attacks, though, the early and late correlators remain aligned and this makes spoofer to be unnoticeable for the difference SQM metric. In other cases where the spoofer does not have a power advantage, the sign test is also able to detect the spoofing as shown in the right hand side of Figure 3.11

Combination of SQM metrics and use of very-early/very-late correlators

It is often difficult to cover all possible spoofing attacks by using just one single SQM metric. Even though using its moving variance can slightly improve the performance, as shown in [58], a more robust approach is proposed



(a) (b)

Figure 3.11: Detection results for overpowered attack with a spoofer appearing between time 150 and 200 seconds (left plot) versus the matched power attach (right plot) with a spoofer appearing between time 150 and 200, as well as 250 and 300 seconds, when using the GoF test (upper plot) or the sign test (bottom plot). [10]

in [11] using the combination of different SQM metrics. It addresses the problem that when spoofed alarm is raised, the spoofer has already captured the user's receiver or at least, already caused negative effects on its normal working condition. Therefore, the detection alarm should better be raised as early as possible for a prompt spoofer detection. To do so, [11] introduces a multi-correlator technique that introduces two sets of correlators are placed beside the real correlation peak, thus helping to detect the counterfeit signal well before its correlation peak aligns with the authentic one as shown in Figure 3.12.

A combination of SQM metrics is also proposed in [12] to account for the fact that no single SQM metric is able to succeed in detecting spoofers for all possible carrier phase offsets and code delay offsets between the spoofed signal and the authentic one. Two different modes named as Amplitude Combination Mode (AmpM) and probability of false alarm combination mode (pfaM) are proposed. The first one consists in combining the values of different SQM metrics to obtain a new (combined) SQM metric. The second one consists in declaring the presence of spoofer whenever one of the individual SQM metrics exceeds its own threshold.

The statistical properties are formulated using the combination of both metrics while in case of pfaM mode, two probability of false alarms are combined for both metrics while the spoofing presence decsion is made as long as one metric exceeds its threshold. It is interesting to see in Figure 3.13, the best performance is obtained with the pfaM combination, that is, combining

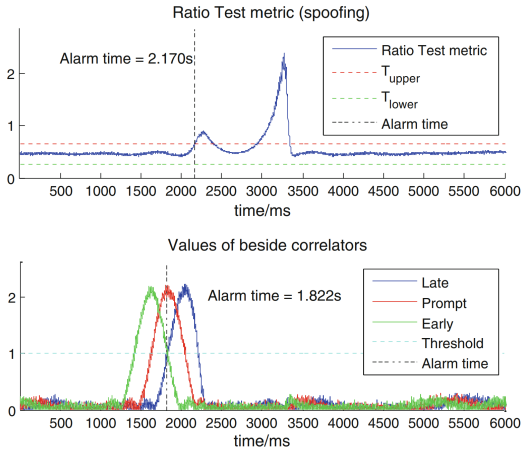


Figure 3.12: Time evolution for the simple ratio SQM metric (upper plot) and for the very early/late correlators (bottom plot) in the presence of a spoofing attack. [11] .

the individual SQM decisions similarly to a hard-decision approach.

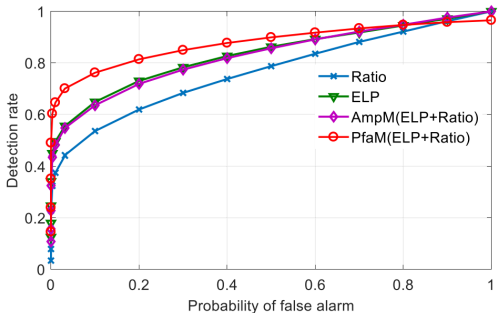


Figure 3.13: ROC curves for individual SQM metrics and various metric combinations [12].

3.2.3.3 Consistency Checks

Code-carrier phase consistency

Code and carrier phase are the two key output observables provided by GNSS receivers. In case of an authentic signal, both code and carrier phase show a consistent behaviour as both are affected by the very same relative motion of satellite and receiver [5]. While code alignment is relatively easy for a spoofer to be achieved, carrier phase alignment is much more difficult and challenging, and therefore it can be used to infer the potential presence of a spoofed signal. In case of a spoofing attack it is likely that the two

observables are not consistent within a given observation window. On one hand, the spoofer has to align the correlation peak with the authentic signal by appropriately shifting the code phase while on the other hand the spoofer has to keep its carrier frequency shift almost the same as that of the authentic signal, as well as the carrier phase as much as possible to prevent the aggregated correlation peak to significantly distort. Monitoring their consistency is one of the techniques proposed in the literature for spoofing detection, as done for instance in [59]. Nevertheless, there are few techniques based on this strategy that have been formulated in detail and discussed widely in the literature.

Doppler consistency

An alternative approach making use of consistency checks is to compare the carrier Doppler meaured by the receiver with the one expected according to the satellites velocities, as proposed in [60]. The latter can be calculated by the receiver based on the ephemeris that can be downloaded from an assistance server, to prevent using the broadcast navigation message in case it had been spoofed. In principle the measured Doppler and the expected one should have the same trend, since otherwise, it might be an indication that the received signal is being spoofed.

Pseudorange consistency (RAIM)

Receiver Autonomous Integrity Monitoring (RAIM) is a technique widely adopted in the civil aviation domain that is based on the consistency check of the redundancy present in the range measurements, in order to guarantee the integrity of the position solution. There are many different RAIM implementations such as that based on the range comparison, on the parity method, the least-squares residuals, or the separation solution [60]. Despite its wide adoption in many critical applications, RAIM has some limitations that pose concerns on its applicability to the case of spoofing detection, as discussed in [61]. For instance, RAIM works at position level using the pseudorange measurements which means that it operates at the very last stage of the receiver chain and therefore it incurs in some latency. Also in [62], it is discussed that during the position determination stage, RAIM could be able to detect abnormalities based on the range residuals. However, once the receiver is fully controlled, the range residuals might be too small to trigger an alarm. Also, more sophisticated spoofers could change the PVT solution without making the receiver to detect the anomalies.

Later on, in [63], the idea of using RAIM with signals of opportunity (e.g. eLoran, multiple GNSS or communication signals), to validate the consistency is proposed but just superficially, without a detailed discussion about the design, implementation and performance. This is a promising approach but requires a significant added complexity for processing.

3.2.3.4 Observable Jumps

This approach is based on the fact that there is usually a transition from the receiver tracking the authentic signal to the receiver being captured by the spoofed signal. Such transition often involves a degradation of the receiver observables when the spoofed signal overlaps with the authentic one and it is in the process of taking over the tracking loops. Once this is done, the output observables follow a different trend imposed by the spoofer's will and therefore one can see that there has been a jump in the receiver output observables before and after the spoofer intervention. Such jumps can be detected by using change detection techniques such as those proposed in [64]. One of the methods reported in [13], based on monitoring positon fixes and the AGC values from the receiver RF front end'. The experiment is conducted using a vehicle having a GPS antenna mounted on it. Also, a repeater implementing a simple attack is conducted. At first, the vehicle starts out of the range of the spoofer repeater while GPS receiver is powered on. Then, the vehicle drives towards the spoofer at constant speed and a sudden change in the position fix is experienced at time instants from 135 to 170 seconds, as shown in Figure 3.14. At the same time the AGC values abruptly jumped, further indicating that a spoofer attack was being suffered.

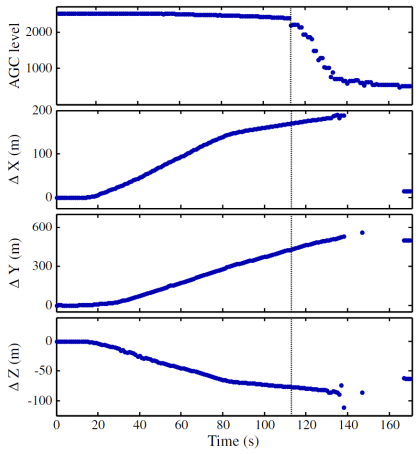


Figure 3.14: The AGC detection metric based on jump in position fix [13].

3.2.3.5 Clock Monitoring

The basic idea of GNSS localization and timing is trilateration, which relies on the known location of the GNSS satellites and the distance between satellite and user measured by the user's receiver. The navigation message

transmitted by each satellite contains the ephemeris and almanac data along with time of transmission. Besides, the distance between the satellite and users provide the pseudorange information. However, the pseudorange is not the exact distance between the satellite and the user because the receiver and satellite clocks are both biased to some extent, and propagation effects introduce additional errors. While the satellite clock bias can be known, the receiver clock bias can not and must be therefore estimated. In a normal scenario, the receiver clock bias changes smoothly, which mainly depends on the quality of the local crystal oscillator. In a spoofing attack, though, the estimated clock bias may abruptly change as a result of the inconsistencies introduced by the spoofer at the observable level, which propagate through the navigation equations and end up affecting the estimated clock bias as well. It is for this reason that clock monitoring becomes an interesting technique to detect spoofing attacks as shown in Figure 3.15. During the spoofing attack, if the spoofer causes the receiver clock bias to change too rapidly, then it could be easily detected by the victim's receiver. It could also be monitored the clock drift rate and compared with reference values for similar types of oscillator (e.g. TCXO, OCXO, Rubidium oscillator, Hydrogen maser etc).

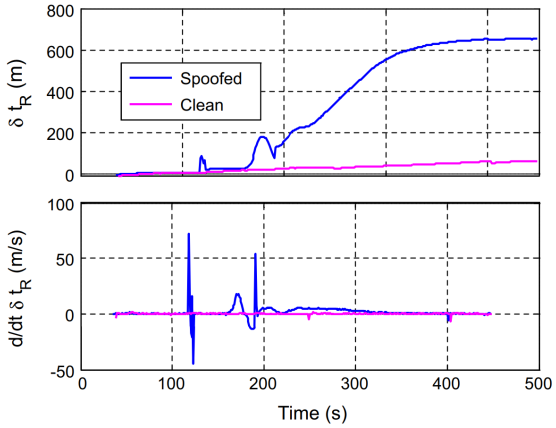
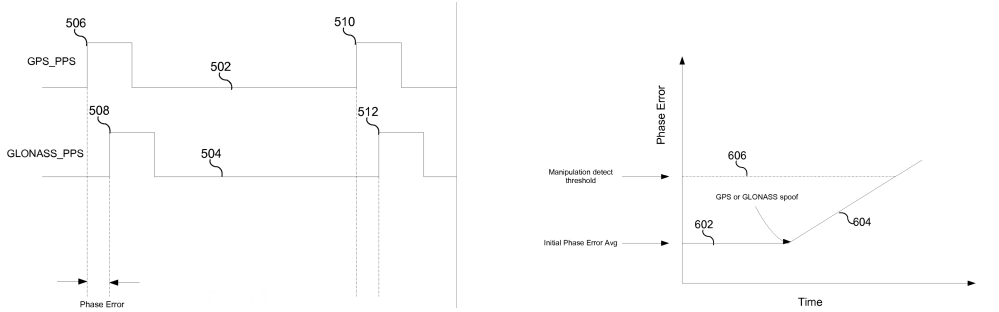


Figure 3.15: The clock bias (up) and clock bias rate (down) for a spoofed and an authentic (i.e. "clean") signal [10].

3.2.3.6 Multiple Constellation/Frequency Redundancy

Multi-Constellation is the usage of multiple GNSS such as GPS, Galileo, BeiDou and GLONASS in order to get a combined PVT solution. The consistency of having multiple constellations increases the probability of spoofing detection, as the spoofer has to be very sophisticated to properly counterfeit

such a big amount of GNSS signals and their interdependent parameters. A system based on multi-constellation spoofing detection has been patented in [14] to detect the time signal manipulation. The strategy is based on the usage of the GNSS time reference signal such as Pulse-Per-Second (PPS) signal by means of a so-called Time Quality Module (TQM) that monitors the phase error between the time reference as derived from two constellations such GPS and GLONASS, or more. Whenever the phase error between the time signals of two or more of the constellations exceeds a predefined threshold, such difference would to be declared as spoofing. An example can be seen in Figure 3.16 (left) where the rising edge of the GLONASS time signal is ahead of the GPS time and the phase error is shown in Figure 3.16 (right).



(a) (b)

Figure 3.16: The GLONASS signal is ahead of GPS due to spoofing manipulation (Left). An example of the resulting phase error (Right) [14].

3.2.4 External Aiding

So far, spoofing detection techniques relying on sources internal to the GNSS receiver have been discussed. However, in addition to these solutions, it is also possible to detect spoofing attacks by making use of external sources that provide independent information to that provided by the GNSS receiver. For instance, "Network Assisted" in which the information comes from a central facility connected to the GNSS receiver through a communication network, in order to support the processing of the GNSS signals. Such processing may be performed either at the receiver side or at the central facility side. The network assisted anti-spoofing techniques further comprises on following two classes.

- Assisted GNSS (A-GNSS)
- Server-assisted processing of GNSS encrypted signals.

	Supported Mode		
Processing step	**A-GNSS Terminal-assisted**	**A-GNSS Terminal-based**	**GNSS Standalone**
Baseband processing	Positioning Module	Positioning Module	Positioning Module
Pseudo range calculation	Positioning Module	Positioning Module	Positioning Module
Position calculation	Central Facility	Positioning Module	Positioning Module
Decoding of Satellite data	Central Facility	Central Facility	Positioning Module
Selection of Satellites	Central Facility	Central Facility	Positioning Module

Figure 3.17: Location Service requests [15].

3.2.4.1 Assisted GNSS

In A-GNSS, the GNSS receiver exchanges information with a server through a network, in order to support the processing of GNSS signals. A-GNSS has mainly been designed to improve the startup performance (i.e., the time to first fix) of smartphones, indeed its development has been supported by the U.S. FCC's 911 requirement to make cell phone location data available to emergency call dispatchers. Figure 3.17 shows Location Service requests [15], taken from the ETSI Technical Specification [15], shows where the different processing steps are done in a GNSS standalone architecture and in two different A-GNSS architectures:

- **GNSS Standalone**: In standalone, the receiver has to search for the available GNSS satellites, acquire and track the GNSS signals, decode the navigation messages, estimate the pseudoranges and compute the position.
- **A-GNSS Terminal-Based**: In terminal based A-GNSS, the receiver gets the list of satellites from a central facility and the associated satellite data (e.g., ephemeris, clock corrections, etc.), and it explore this information to acquire the GNSS signals, estimate the pseudoranges and compute the position.
- **A-GNSS Terminal-Assisted**: In this scenario, the receiver gets the list of satellites from a central facility and additional information (e.g., the Doppler search windows) in order to acquire the GNSS signals and estimate the pseudoranges. These pseudoranges are then transmitted to the central facility that computes the receiver position, which is sent back to the receiver.

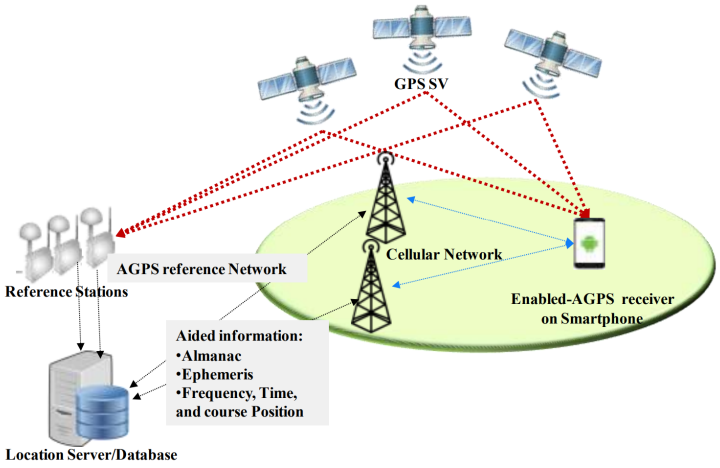


Figure 3.18: Example of an A-GNSS architecture [16] .

In both A-GNSS architectures the receiver does not need to decode the navigation messages and not even to continuously track the GNSS signal, instead it can employ a snapshot-based approach to estimate the pseudoranges at regular time interval. These features are desirable in many smartphone applications because they allow to improve the time to first fix and the power consumption. The idea proposed in this dissertation follows the identical snapshot based assisted GNSS approach to support the processing and detection of spoofing attacks.

A-GNSS has not been designed as an anti-spoofing technique, however it implicitly protects from data-level spoofing attacks, because the satellite data is coming from the central facility but not the data carried within the received (potentially spoofed) GNSS signals. An example of an A-GNSS system architecture is depicted in Figure 3.18. It is made of the following elements [16]:

- **Reference Stations**: GNSS receivers placed in different locations, with the goal of monitoring the operational GNSS satellites in view in different areas and extracting the associated navigation data.
- **Location Server / Database**: A central facility collecting the information extracted from the reference stations and disseminating to the A-GNSS receivers aiding data, possibly computing the positions of A-GNSS receivers in case of A-GNSS Terminal-assisted architecture.
- **Communication Networks**: The networks used to disseminate the information, including the network from the reference stations to the

central facility, and the network connecting the central facility to final A-GNSS receivers.

It is important to remark that A-GNSS protects against data-level spoofing attacks as long as A-GNSS system itself is protected. Considering the widespread of applications exploiting A-GNSS based positioning, A-GNSS systems may be considered as important infrastructures that need specific protection mechanisms. In particular, it is recommended to embark authentication mechanisms, such as OSNMA, and other anti-spoofing techniques within the A-GNSS reference stations, to enhance the robustness and security of the collected data that are subsequently disseminated to the A-GNSS receivers.

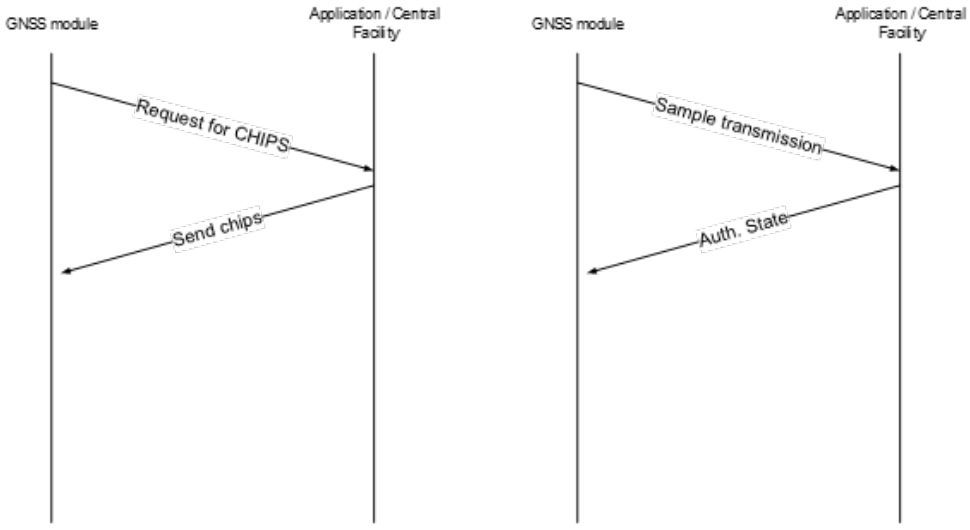
3.2.4.2 Server-Assisted Processing of GNSS Encrypted Signals

Encrypted GNSS signals can be exploited to perform signal authentication checks and hence protecting against signal-level spoofing. The usage of such signals for a receiver not possessing the associated crypto-module requires the support of a central facility having the crypto-module. Two architectures are foreseen depending on where the authentication check is performed:

- **Spreading Code Transmission**: In this scenario, the central facility sends snapshots of encrypted PRN to the positioning terminal, which correlates them with the received signal to perform an authentication check. The central facility may send the snapshots of encrypted PRN either to a specific terminal after an explicit request (client-server architecture, as shown in 3.19 (left)), or to all connected terminals at regular time intervals (multi-cast architecture).
- **Remote Processing Authentication**: In the remote processing authentication, the snapshots of raw IQ samples are collected by the terminal and sent to the central facility, which performs the authentication check and send back to the terminal as shown in 3.19 (right). Motivating this remote processing authentication approach, this dissertation follows the identical protocols for spoofing detection exploiting OSNMA unpredictable properties.

3.2.5 OSNMA Anti-Spoofing Techniques for SCER Attacks

The techniques described so far are intended to detect the presence of a spoofed GNSS signal under the assumption that the GNSS signal has no



(a) (b)

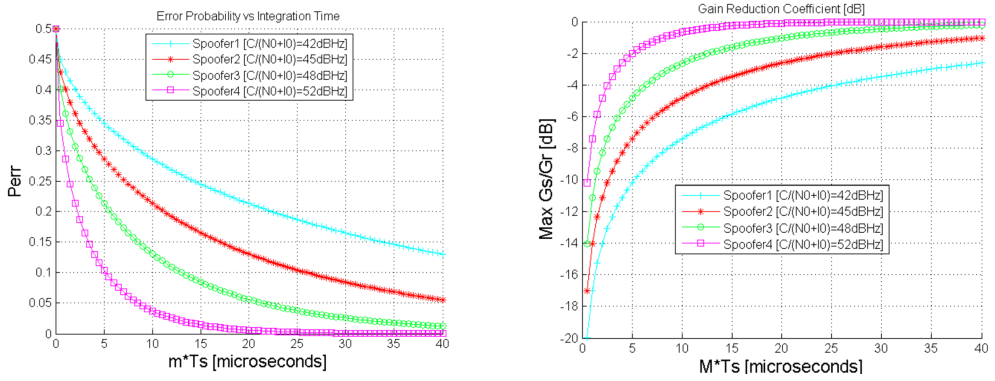
Figure 3.19: Spreading code transmission (left). Remote processing authentication (right).

security countermeasures by itself, meaning that it is an open signal with no encryption nor authentication capabilities but this is not the case in OSNMA. Therefore, this subsection highlights the countermeasures against SCER attacks by exploiting the OSNMA authentication properties since SCER attacks are considered the most sophisticated attacks that can be implemented by a spoofer in order to alter the victim's PVT solution. In this attack, the spoofer receives the authentic signals from the GNSS satellites, estimates the observables with very high accuracy and replays the signal to the victim's receiver in order to take over the tracking loops and then gradually alter the position fix. OSNMA provides an interesting countermeasure against SCER attacks by means of the unpredictable bits that it introduces into the authentication navigation message. However, a spoofer could always try to estimate such bits and replay them with a zero or negligible delay. Actually, there are two different types of SCER attacks:

- **Zero latency SCER attacks:** The delay of the spoofed signal is considered to be zero at the beginning of the attack and then gradually increased to spoof the pseudorange and hence the position, avoiding effects easily noticeable at the tracking loops of the victim.
- **Non-Zero latency SCER attacks:** A significant delay is present in the spoofer-generated signal. In order to avoid being detected due to

the jump in the tracking loops of the victim's receiver, at the beginning of the attack, the spoofer may try to generate jamming signals that could temporarily "blind" the victim's receiver. Details about SCER attacks and protection techniques against them are receiving an increasing interest.

The work in [17] provides insights about the NMA unpredictability and its protection role against replay attacks by considering a zero latency SCER attack. The victim's receiver could take advantage of the NMA unpredictable bits to detect whether the received signal is authentic or not. To do so, the receiver should store the first N_C chips of the received pseudorandom code for each of the N_U unpredictable symbols over a given interval. The receiver would then accumulate $N_C N_U$ chips in total. Once the N_U unpredictable symbols are received and authenticated, the receiver generates the corresponding local replica and correlates it with stored signal samples. The analysis carried out in [17] measures how difficult can be for the spoofer to estimate the unpredictable bits so that it could replay them to the victim's receiver. That is to say, what the probability of bit error is as a function of the time interval that the spoofer observes each unpredictable bit and the C/(N0+I0) of the received signal at the spoofer, as shown in the left hand side of Figure 3.20.

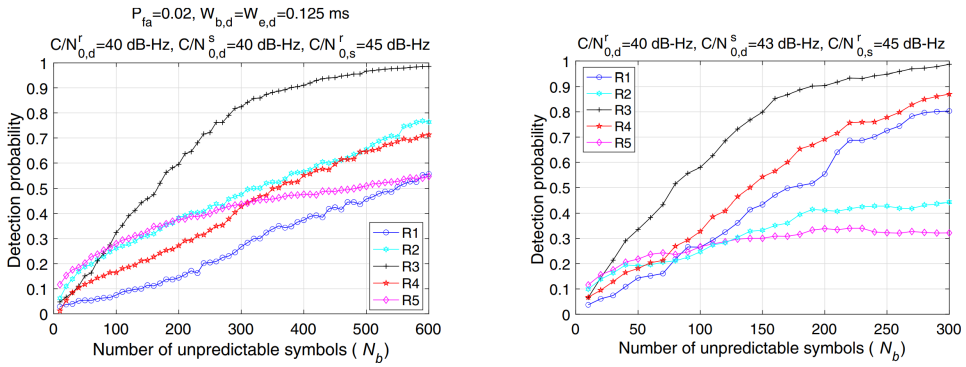


(a) (b)

Figure 3.20: Bit error probability of the spoofer (left) and gain reduction at the receiver (right) as a function of the time the spoofer spends in observing the unpredictable bits. [17]

The analysis in [17] also determines the gain obtained by the victim's receiver when accumulating $N_C N_U$ chips in total, either when the received signal is authentic or when it is spoofed. In the latter case, the gain would

be lower and depends on the spoofer's probability of successfully estimating the bits, which depends on the time the spoofer takes to observe the unpredictable bits before a decision on that bit is issued. For instance, if the spoofer observed only the first 5 chips of the unpredictable symbols, there would a gain reduction of 7 dB at the receiver compared to the case when the authentic signal is tracked. The results can be seen in the right hand side plot of Figure 3.20



(a) (b)

Figure 3.21: Detection probability of all proposed detectors in [18] with 5dB advantage for spoofer (Left). Detection probability for the LMS channel (Right).

The idea proposed in [17] for the receiver to correlate and accumulate pieces of the unpredictable bits is further extended in [18]. In particular, five detectors based on the partial correlation of the received signal are proposed. Such correlation is done using the initial part of the current unpredictable symbol and the end of the same unpredictable symbol, in order to exploit potential inconsistencies that might appear due to the efforts of the spoofer to determine the sign of such symbol at the time of replaying it. Among the five detectors, the first one referred to as R1 involves the computation of the absolute ratio of two metrics, the initial and last partial correlation. For the second detector referred to as R2, the absolute value of the ratio used in detector R1 minus one is investigated, indicating no spoofing attack is present if the result is close to zero. The third detector referred to as R3 is based on computing the mean of the difference between the correlation at the beginning and the end of the unpredictable bit. The R4 detector compares the measured C/N_0 at the beggining and the end of the unpredictable bit, where the C/N_0 is estimated using the Narrow-band Wide Band Power Ratio (NWPR). Finally, the last detector referred to as R5 is designed on the basis of the phases difference between the initial and the last partial correlation

of the unpredictable bit. Apart from benign working conditions, the Land Mobile Satellite (LMS) channel is also considered for assessing the impact of multipath. The performance of all five detectors is evaluated in multiple environments as shown in Figure 3.21, showing that the R3 detector based on the mean of the two partial correlations outperforms all other detectors.

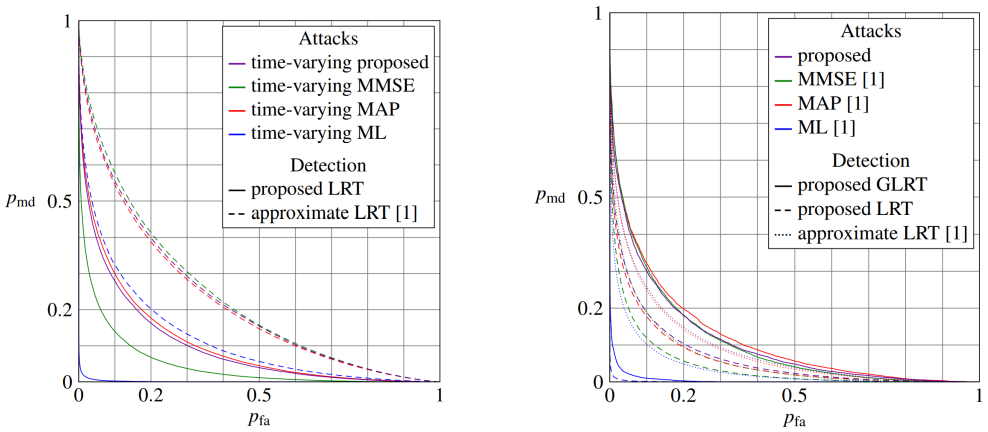


Figure 3.22: Performance for time varying attacks on Galileo E1 signal using LRT (left) and GLRT (right) for unpredictable bit detection [19].

Another work addressing anti-spoofing techniques relying on OSNMA is the one in [47]. As in any zero delay SCER attack, the spoofer needs to replay the received signal before it can actually know the value of the unpredictable bit, since it takes a while for it to be determined. During this uncertainty period, the spoofer can replay a random bit and then switch to the correct bit once it is determined. The very same principle is considered in [47] with the exception that the unpredictable bit is replayed in advance, before its starting time, in order to introduce a signal advance at the victim's receiver instead of a delay, as usual. This strategy is known as Distance-Decreasing (DD) attack because advancing the replayed signal means that the victim's receiver perceives a shorter distance from that spoofed signal. According to [47], this has the advantage that the clock bias at the receiver can be maintained more easily without incurring in an abrupt delay, which would be otherwise easily detected. Finally, the work in [19] reviews the problem of SCER attacks and formulates the problem as a binary testing problem where different detection strategies can be implemented for deciding the unpredictable bits. Three strategies are considered, two of them are time invariant i.e., Maximum Likelihood (ML) and Maximum A Posteriori (MAP) estimators, and

one of them is time-varying, the Minimum Mean Square Error (MMSE) estimator. The bit detectors are optimized by minimizing the Kullback-Leibler (KL) divergence between the authentic and the spoofed signal. The performance analysis among classical attacks and detection strategy metrics and the proposed attacks and detection strategy is shown in Figure 3.22

Conclusion

This chapter comprised of two significant sections. The first section is focused on characterizing the nature of spoofing attacks i.e. from simpler attacks to the sophisticated ones that are threaten to the widely growing navigation services. The other section is about the discussion of the variety of state-of-the-art anti-spoofing techniques at all levels that are rigorously applied and studied in literature to detect the variety of spoofing attacks. This assists in identifying how the anti-spoofing techniques are evolved towards OSNMA in the recent years.

Chapter 4

Snapshot OSNMA: Concept and Feasibility

Heretofore, a comprehensive discussion has been carried out concerning a different types of spoofing attacks and the most relevant anti-spoofing techniques to counter these attacks. Taking into account the significance of GNSS signal integrity in the literature, one can see how important becomes the study of signal authentication and anti-spoofing within the GNSS community, as key enablers for the deployment of GNSS-based applications and services.

Among the variety of spoofing attacks discussed in the previous chapter, SCER attacks stand out as particularly concerning. They require substantial attention because the lack of signal authentication and the gradual increase of potential attacks, pose a serious threat for the practical use and deployment of GNSS. To counter these challenges, endeavors has been taken by introducing the OSNMA paradigm as a means of authenticating navigation message, as discussed in a prior. Specifically, Galileo is providing the OSNMA framework in its E1-B signal component, which conveys a set of cryptographic data with the purpose of authenticating the content of the Galileo I/NAV message. Some of these data symbols are unpredictable to the users, and therefore they cannot be known in advance and used to generate a counterfeit signal, thus introducing an additional protection level against potential spoofers.

Recent publications described novel sophisticated attack mechanisms that might be used to circumvent the protection provided by the navigation message authentication. That is, by tracking the received signal from the Galileo satellites in view, estimating the OSNMA unpredictable symbols and retransmitting a replica of the Galileo signal with these estimated unpredictable symbols to the victim receiver, in order to gradually take over the victim's

tracking loops. All these steps would be carried out by incurring into a negligible delay, which makes this attack being often referred as a zero-delay SCER attack. Nevertheless, in execution of the attack and specifically, in the process of estimating the OSNMA unpredictable symbols to be re-transmitted to the victim's receiver, the spoofer may incur in non-negligible probability of error leading to ultimately inverting the sign of some symbols. This introduces some uncertainty at symbol level that beccomes the Point Of Interest (POI) to be investigated at the user's side for detecting the presence of a potential spoofer.

4.1 Snapshot OSNMA

Contrary to the existing contributions, this chapter briefly proposes a symbol-level remote-server anti-spoofing technique intended to be implemented in snapshot GNSS receivers. That is, those widely adopted in smartphones and IoT devices, where the continuous processing of GNSS signals is not feasible due to high computational load and battery consumption. In these circumstances the receiver cannot have access to the whole OSNMA data and thus cannot implement the full OSNMA functionalities. Furthermore, no pages of the I/NAV message can be retrieved because just a portion of a page is available on the snapshot of received signal.

This is a limitation that snapshot receivers face and that the proposed technique intends to circumvent by providing a certain degree of protection against spoofing attacks. This is be done by using just a portion of the Galileo I/NAV message, where OSNMA unpredictable symbols are transmitted. This is possible because the position where unpredictable symbols are transmitted onto the I/NAV navigation message is known in advance, and thus the user's receiver could be scheduled to wake up at predefined time intervals. It is for this reason that the proposed technique is referred to as *snapshot* OSNMA. Once the receiver is triggered to wake up, it gathers a snapshot of Galileo E1-B signal, retrieves the unpredictable symbols, computes the position and time through A-GNSS framework, and sends these time-tagged and geo-tagged estimated unpredictable symbols to the remote server. It is important to highlight here that not only position, but also time, is computed using the received snapshot of GNSS samples. Time information provides an additional degree of protection because, if the user's receiver local time is a trusted one, then comparing the estimated time with the trusted one can unveil the presence of excessive time offsets. Such offsets could be incurred by spoofers when trying to estimate the unpredictable symbols.

Once the time-tagged and geo-tagged symbols are sent to the remote

server, the latter takes these received unpredictable symbols, and compares them with the authentic unpredictable symbols that the user should have at that particular position and time. Since no OSNMA data is decoded at the user terminal, this approach circumvents the problems due to the low availability of decoded I/NAV data at the user terminal, which has been reported to be typically less than 10% in most of the existing Android smartphones [24].

The rest of the chapter provides comprehensive details of the transmission of unpredictable symbols within the I/NAV message and its relation with snapshot OSNMA. Additionally, it is envisaged, apart of potential spoofer, there may be other factors that could contribute in incurring the symbol errors such as intense signal impairments. Therefore, the feasibility of working at symbol level is thoroughly examined in terms of the so-called boundary conditions. Subsequently, the detector to be implemented at the server side is designed taking into account the boundary condition introduced .

4.1.1 OSNMA Unpredictable Symbols

As previously mentioned, Galileo incorporates OSNMA features that are intended to assist the user's receiver in the verification of the received message authenticity, and thus the mitigation of potential spoofing attacks that may alter the content of the I/NAV message. OSNMA follows an approach based on the TESLA protocol, which relies on the transmission of a MAC to authenticate the message, and a delayed transmission of keys used to compute such MAC [46], as comprehensively discussed in previous chapter. The delay between the transmission of MAC and the key is made in such a way that the key is unknown to the user until the message and the MAC is received. Therefore, a potential spoofer cannot used the keys to generate the MAC in advance.

The OSNMA data is conveyed in the 40 bits of the "Reserved 1" field available in nominal odd pages of the I/NAV message transmitted on the Galileo E1-B signal component, as shown in Figure 4.1. Each page, even and odd, has a duration of one second, so one full page spans for a total of two seconds. Then 15 full pages are grouped into one sub-frame, which lasts for 30 seconds, and 24 of these sub-frames are grouped into one frame, which is the largest structure of the I/NAV message and lasts for 720 seconds. The OSNMA data are included in odd pages of the I/NAV message, which has a bit rate of 120 bit per second. Since the I/NAV bits are convolutionally encoded with coding rate of 1/2 which means that each bit is encoded into two symbols with a total of 240 symbols per page. Additionally, 10 synchronization symbols are added at the beginning of each page, which makes a

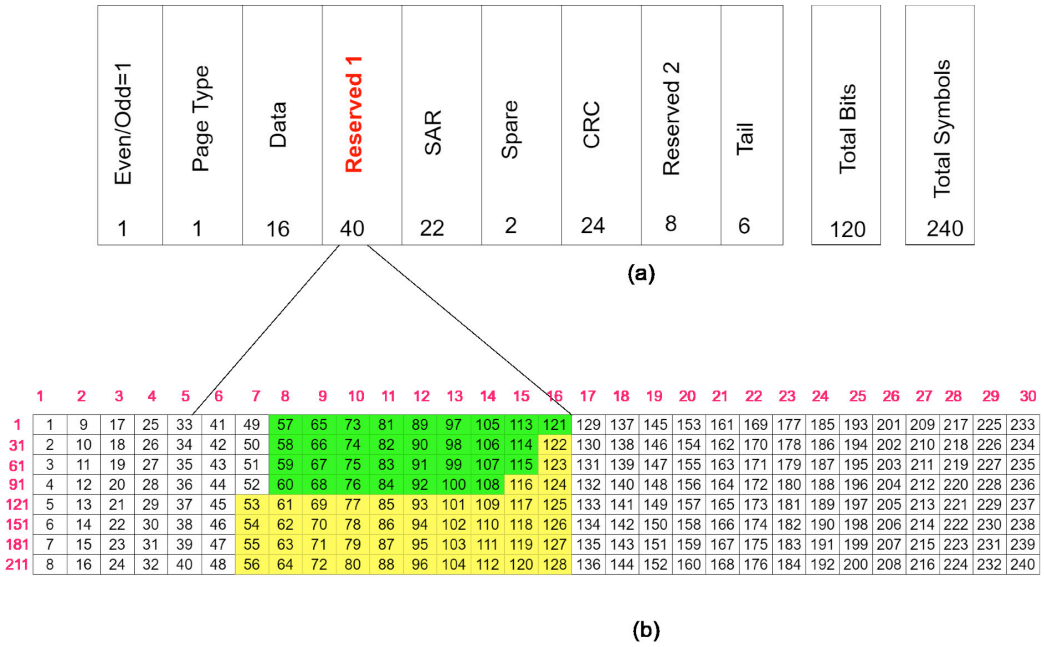


Figure 4.1: (a) I/NAV nominal odd page for Galileo E1-B, where the "Reserved 1" field containing the OSNMA data is highlighted. (b) OSNMA unpredictable symbols position (see green cells) within the I/NAV nominal odd-page already encoded and interleaved, that is, as received by the user [20].

total of 250 symbols per page, transmitted in one second. This means that the symbol period for Galileo E1-B is therefore 4 ms.

Once the bits have been encoded into symbols, the latter are interleaved by writing them column-wise in blocks of 8 symbols and reading them row-wise. This is indicated in Figure 4.1, where one can see that the cells are filled using a sequential numbering per column, meaning that their content is written column-wise. However, the contents are read row-wise, and this is indicated by the sequential numbering appearing in red in the top of the symbols matrix. The row-wise symbols are what users actually receive, and what the proposed detector actually have to work with. Unpredictable symbols are highlighted in green in Figure 4.1(b) [20]. For illustrative purposes, it is assumed that the 32 bits of the MAC and Key (MACK) section are all unpredictable, which is not the case for all pages. Yet, the principles of this work still hold in other cases. As can be seen, when unpredictable symbols are present, a receiver operating in snapshot mode can collect between 7 to 9 consecutive unpredictable symbols per snapshot. The analysis presented in this chapter will provide answers to key questions related to the design of

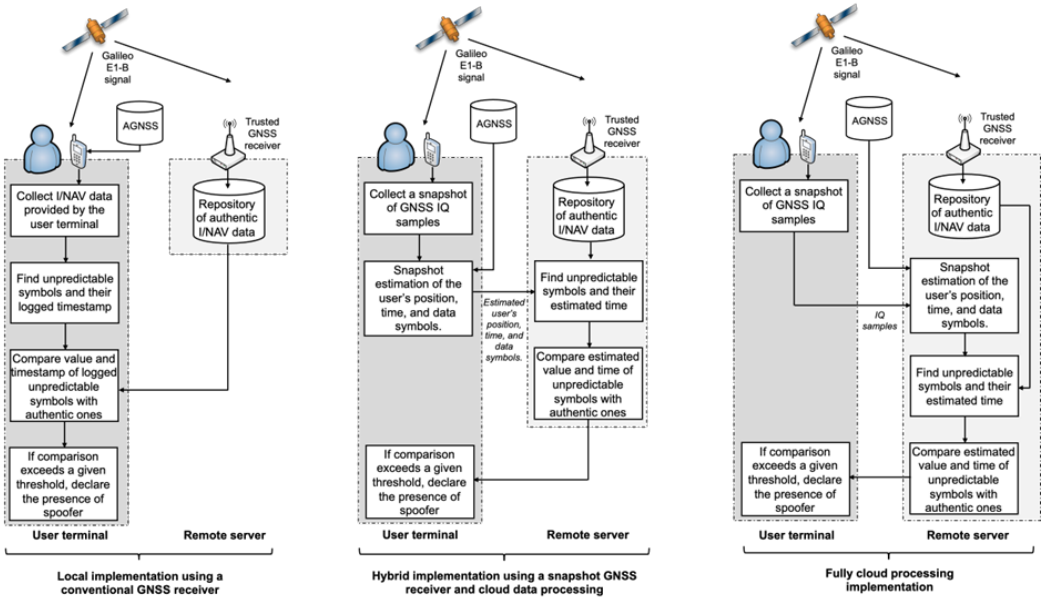


Figure 4.2: High-level architecture of the proposed snapshot OSNMA spoofing detector.

the authenticity detector, such as how many consecutive unpredictable symbols are needed and thus how many snapshots are needed to detect a SCER attack under different circumstances. The problem in this proposed scheme formulated using an equivalent binary symmetric channel (BSC) interpretation, where the performance is determined by the probabilities of error at the spoofer and the user sides.

4.1.2 Snapshot OSNMA System Architecture

The overall high-level architecture of the proposed snapshot OSNMA spoofing detector presented in this dissertation is shown in Figure 4.2. As can be seen, three different configurations are possible, all of them composed of two constituent elements, namely the user side and the remote side. In the first configuration, all the processing is carried out locally at the user terminal while the remote server is just in charge of providing the sequence of authentic symbols to be compared against, similarly to what is proposed in [24]. The second configuration involves a hybrid implementation whereby the user terminal sends the geo-tagged and timestamped received symbols to the remote side. The latter is then in charge of comparing with the authentic symbols and deciding on the presence of spoofing. Finally, the third approach

is a fully cloud-based implementation where the user terminal just gathers the IQ samples of the received Galileo signals and sends these samples to the cloud where all the processing is carried out. This approach would be in line with the general framework of the so-called cloud GNSS signal processing already proposed in [65], which is targeting low-power GNSS-enabled IoT devices.

In this work, the focus is on the second approach, whereby the user is gathering snapshots of just a few tens or hundreds of ms of GNSS received signal in an on-demand basis. These snapshots are processed locally to obtain the user's position and time using coarse-time navigation, in order to circumvent the limitation that the transmission time broadcast by the satellites cannot be retrieved from a ms-length short piece of received signal [66].

This is the common approach in many mobile devices that due to computational and power consumption constraints, must resort to an on-demand use of GNSS, and switch off for the rest of the time until the next position fix is requested. In the case under study, and apart from locally computing the user's position and time, the Galileo E1-B received symbols are demodulated as well. It is assumed for the sake of simplicity that the user's receiver is scheduled to gather the snapshots of Galileo E1-B signal at the time instants where unpredictable OSNMA are expected to broadcast. This is possible because the transmission of unpredictable symbols is deterministic, being conveyed in a specific field of the I/NAV message that is repeated every two seconds. However, in the case of any time uncertainties, a longer snapshot containing both predictable and unpredictable symbols would be required.

Once the user receiver has obtained its position, time, and the demodulated symbols, these three items are sent to the remote snapshot OSNMA service. When they are received at the remote end, the estimated user's position and time are used to access a repository where the set of all unpredictable OSNMA symbols transmitted by the Galileo satellites up to that moment is available. This repository is populated by a trusted Galileo receiver operating 24/7. When the authentic OSNMA symbols that were supposed to be received at the user's position and time are retrieved from the repository, the next step is to compare them with those received by the user, which actually contain both predictable and unpredictable symbols. If the user's received unpredictable symbols coincide with the authentic ones within a given time window, there is no guarantee that the underlying signal has not been spoofed, but at least at symbol level we can declare that the user's unpredictable symbols are authentic. Thus, the received snapshot can be trusted at symbol level. In contrast, if the user's received unpredictable symbols do contain too many errors with respect to the authentic unpredictable symbols, or the time at which these unpredictable symbols was received ex-

ceeds a given time window, then the received snapshot can be declared to be spoofed at symbol level, and consequently, at signal level as well. This satellite should then be discarded by the user.

4.2 Feasibility and Boundary Conditions of Snapshot OSNMA

Before starting with the problem of comparing the received symbols with the authentic ones, it is interesting to discuss the feasibility of working at symbol level, and whether the detection of non-coincidences is reliable enough to be used as a spoofing detection metric. By doing so, it would later be easy to design a decision detector taking into account the actual working conditions and to see how feasible it is for a spoofer to attack and counterfeit the unpredictable symbols. This section addresses some cases and considerations to support the above statements. To do so, the signal model at spoofer and user side is formulated first.

4.2.1 Signal model at the spoofer's side

The symbols transmitted by a given Galileo satellite will be denoted by $s(n)$ for a given time instant n, with $s(n) \in \{\pm 1\}$. A spoofer willing to implement a SCER attack will try to first track the authentic signal coming from GNSS satellites in order to estimate the unpredictable symbols contained within $s(n)$, and immediately transmit a replica of such GNSS signal using the estimates obtained in the first step. In the process of determining the unpredictable symbols, there is a non-negligible probability p_s that the spoofer may incur in error. With this in mind, we will denote the spoofer transmitted symbols by $\tilde{s}(n)$ so that

$$\tilde{s}(n) = \begin{cases} s(n) & \text{, with probability } 1 - p_s \\ \bar{s}(n) & \text{, with probability } p_s \end{cases} \tag{4.1}$$

where $\bar{s}(n) \doteq -s(n)$ is the sign-reversed version of symbol $s(n)$. As can be seen, the spoofer can be regarded as a BSC where input symbols are sign-reversed at its output with probability p_s. In the sequel, we will also refer to p_s as the symbol error rate (SER) at the spoofer side and $(C/N_0)_{|a,s}$ as the carrier to noise ratio of the authentic signal when received at the spoofer's terminal.

4.2.2 Signal model at the user's side

The binary symbols of the navigation message provided by most GNSS receivers are the result of taking a hard decision on the output of the prompt correlator, once the receiver is locked to the received signal. As such, these hard symbols can be expressed as,

$$\hat{s}(n) = \text{sign}\left(r(n)\right) \tag{4.2}$$

where $r(n)$ are the received symbols affected by the Independent and Identically Distributed (i.i.d.) Gaussian contribution of the thermal noise at the user's receiver. Despite being the optimal rule, taking the sign incurs in a non-negligible probability of error due to the presence of noise, which makes difficult to perfectly ascertain the mapping between the received symbols and the underlying true ones. In particular, the problem can be addressed through hypothesis testing with the following $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses:

$$\mathcal{H}_0 \;:\; \hat{s}(n) = \begin{cases} s(n) & \text{, with probability } 1 - p_{u,0} \\ \bar{s}(n) & \text{, with probability } p_{u,0} \end{cases} \tag{4.3}$$

$$\mathcal{H}_1 \;:\; \hat{s}(n) = \begin{cases} s(n) & \text{, with probability } 1 - p_{u,1} \\ \bar{s}(n) & \text{, with probability } p_{u,1} \end{cases} \tag{4.4}$$

where $p_{u,0}$ is the SER at the user's terminal when no spoofer is present. This is nothing but the probability of error when receiving the authentic symbols in AWGN at the user's terminal. That is,

$$p_{u,0} = \frac{1}{2}\text{erfc}\left(\sqrt{T_d\left(C/N_0\right)_{|a,u}}\right) \tag{4.5}$$

where erfc is the error complementary function and $(C/N_0)_{|a,u}$ is the C/N_0 of the authentic signal received at the user's receiver.

For the alternate hypothesis in (4.4), $p_{u,1}$ is the SER at the user's terminal when the spoofer is present, which is affected by the noise at the user's terminal but also by the error probability incurred by the spoofer. In this case we have the concatenation of two BSC, since errors can occur due to the spoofer or to the user's terminal. It is for this reason that the end-to-end SER at the user's side when the spoofer is present is given by,

$$p_{u,1} = p_s + p_{s,u} - 2p_s p_{s,u} \tag{4.6}$$

where p_s is the SER incurred by the spoofer already introduced in (4.1) and $p_{s,u}$ is the SER of the spoofed symbols when received at the user's terminal, which is given by,

$$p_{s,u} = \frac{1}{2}\text{erfc}\left(\sqrt{T_d\left(C/N_0\right)_{|s,u}}\right) \tag{4.7}$$

with $(C/N_0)_{|s,u}$ the C/N_0 of the spoofed signal received at the user's receiver.

Finally, and since there are a total of L symbols in each of the snapshots i being processed, we can stack the hard decided symbols into vector form leading to,

$$\hat{\mathbf{s}}_i = \text{sign}(\mathbf{r}_i) = [\text{sign}\left(r_i(0)\right), \ldots, \text{sign}\left(r_i(L-1)\right)]^T. \tag{4.8}$$

After formulating the signal models,the feasibility and boundary conditions of snapshot OSNMA are discussed in the following subsections.

4.2.3 Unpredictable symbol errors induced by a simple spoofer

For many spoofers, particularly those with limited resources, determining the unpredictable OSNMA symbols when implementing a SCER attack becomes a difficult task. A simple approach to circumvent this limitation is not to determine at all the symbols, and forge instead the sequence of unpredictable symbols. For instance, by randomly guessing their value and transmitting it toward the victim's receiver. This is the simplest case and the easiest to detect, so it is worth quantifying its effects because they provide a performance lower bound for other (i.e. more difficult) attacks.

To study this case, the probability of having an at least one error incurred by the spoofer is evaluated as a function of the number of unpredictable symbols being guessed. This will provide the information on how easy it is to have an error (one or more) in a given length of spoofed signal. Since it is being considered that a spoofer is randomly guessing the unpredictable symbols, the SER of such spoofer would be $p_s = 1/2$. The probability of incurring in at least one error is the complementary to the probability of incurring in no error at all. Assuming a sequence of Q unpredictable symbols, the probability of having no errors in such sequence would be prob(no errors in Q symbols) $= (1-p_s)^Q$ and therefore, prob(at least one error in Q symbols $= 1-(1-p_s)^Q$ which for a random spoofer with $p_s = 1/2$ becomes,

$$\text{prob(at least one error in } Q \text{ symbols)} = 1 - \frac{1}{2^Q} \tag{4.9}$$

The result of (4.9) is shown in Figure 4.3 on the curve corresponding to $p_s = 0.5$. It can be observed that for a signal snapshot with length comprising four or more unpredictable symbols, having at least one error due to the random guesses of the spoofer is almost certain. This suggests that detecting a random spoofer should be feasible with very short pieces of signal containing a minimum of four unpredictable symbols. This involves

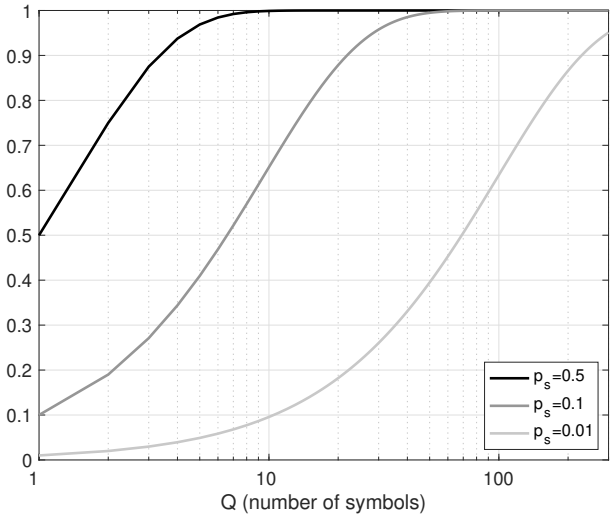


Figure 4.3: Probability of having at least one error in a set of Q unpredictable symbols estimated by the spoofer with probability of error p_s.

that the shortest Galileo E1-B signal length for making sure (i.e. $> 90\%$) that at least one error due to the spoofer is present, is 4×4 ms $= 16$ ms assuming the unpredictable symbols are consecutive. To this end, it is important to recall that up to nine consecutive unpredictable symbols can be received by the user, as shown in the upper row of Figure 4.1.

4.2.4 Unpredictable symbol errors due to a sophisticated spoofer

Sophisticated spoofers avoid random guesses of the unpredictable symbols when implementing a SCER attack. Instead, they try to accumulate the authentic signal for a very short period of time in order to collect enough energy to ascertain what the actual value of the current unpredictable symbol is. This feature was addressed in [17] and [18] where it was shown that integrating the authentic signal for just a few chips suffices to obtain a reliable estimate of the unpredictable symbol.

Following the same approach as in [18], two representative spoofing scenarios are considered. The optimistic case considers a SER at the spoofer side of $p_s = 0.1$, which corresponds to the integration of the authentic signal at $(C/N_0)_{|s} = 45$ dBHz for just 26 μs. The pessimistic case considers a SER at the spoofer side of $p_s = 0.01$, which corresponds to the integration of the authentic signal at $(C/N_0)_{|s} = 40$ dBHz for 271 μs. The number of unpredictable symbols that are required to have at least one error when the

spoofer is incurring in probability of error $p_s = \{0.1, 0.01\}$, are shown in Fig. 4.3

It is worth noticing that for $p_s = 0.1$, $Q > 22$ symbols are needed to make sure (i.e. $> 90\%$) that at least one of the symbols would be in error due to the spoofer. Following the availability of unpredictable symbols in the example of Figure 4.1 (b), at least three snapshots containing $L = 8$ unpredictable symbols would be needed to make sure that we gather at least one spoofer error. This statement is made upon the assumption that snapshots are taken to collect the unpredictable symbols only. An alternative approach would be to take one long snapshot of symbols, including both predictable and unpredictable symbols, spanning for several rows of Figure 4.1(b), so that enough symbols are gathered for detecting a spoofer with a given probability of error.

More sophisticated spoofers with an even lower SER, such as the case with $p_s = 0.01$ in Figure 4.3, are much more difficult to detect. This is because $Q > 230$ symbols are needed to make sure (i.e. $> 90\%$) that at least one error is present. In this case, several pages of the I/NAV message would need to be processed in order to collect the required number of unpredictable symbols, thus incurring in a latency for spoofing detection of several seconds. The total time for detection will be revisited later on.

4.2.5 Symbol errors due to user's receiver noise

So far we have discussed the errors that can appear in the unpredictable symbols that the spoofer transmits to the user's receiver. However, it is possible that even if the received unpredictable symbols are free from spoofer errors, the user may incur in some errors when trying to infer the actual value of these symbols. This would pose a serious trouble to the implementation of the snapshot OSNMA service because it would make difficult to distinguish when the received errors are either due to a spoofer or to the user's receiver itself.

Fortunately, this is not the case as far as the thermal noise is concerned. The SER at the user's side is determined by the energy of the received symbols, and this is the result of integrating the received signal during the whole symbol period. For Galileo E1-B this period is $T_d = 4$ ms, which is one to two orders of magnitude longer than the integration that a sophisticated spoofer would need to ascertain the unpredictable symbol. The SER purely due to the thermal noise at the user's receiver is actually given by $p_{u,0}$ in (4.5), and even for a relatively low C/N_0 such as 35 dBHz, it results in $p_{u,0} \approx 10^{-7}$ which is depicted in Figure 4.4. This is several orders of magnitude below the SER caused by spoofer errors and therefore the impact of thermal noise

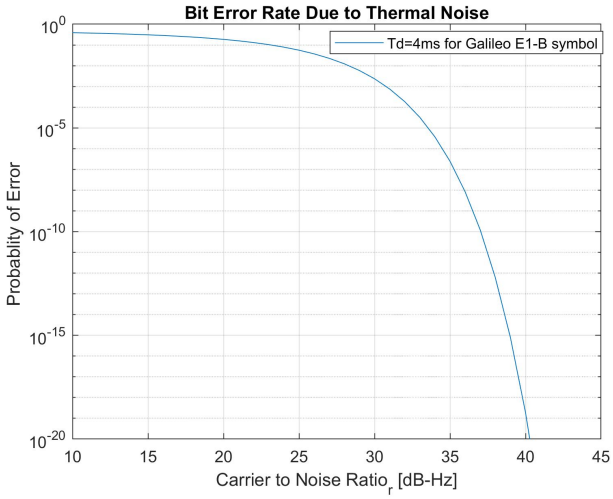


Figure 4.4: Impact of thermal noise in terms of Bit Error Rate (BER).

can be ignored. In other words, it is very unlikely that one of the received unpredictable symbols becomes accidentally inverted due to an erroneous decision caused by the user's receiver thermal noise.

4.2.6 Symbol errors due to the overlap of authentic and spoofed signals at the user's receiver

The discussion in the previous subsection relied on the fact that the user's receiver is processing a single signal corrupted by noise only. However, both the authentic and the spoofed signals are simultaneously received at the user's terminal, and thus, their overlapped aggregate signal is what the receiver actually processes. It is assumed henceforth that the spoofer managed to align its code replica in both time and frequency to that of the authentic signal. Nevertheless, it is very difficult or even impossible for a spoofer to align its carrier phase offset with that of the authentic signal. It is for this reason that the receiver will actually be processing the overlapped (authentic and spoofed) signals with some relative phase between them. Such relative phase offset has a direct impact onto the energy of the aggregated received signal since both individual signals might be added constructively (i.e. having a 0^{o} relative phase offset) or destructively (i.e. having a 180^{o} relative phase offset). This contributes to the user's receiver SER performance even when both the spoofed and authentic signals do convey exactly the same symbols.

Further insights about this impact can be obtained by formulating the following model for the overlapped received symbol,

$$r_i(n) = \alpha_0 s_i(n) + \alpha_1 \tilde{s}_i(n) + w_i(n) \tag{4.10}$$

for $n = 0, \ldots, L-1$ unpredictable symbols and $i = 0, \ldots, N-1$ snapshots, whereas $\alpha_0 = |\alpha_0| e^{j\phi_{i,0}}$ and $\alpha_1 = |\alpha_1| e^{j\phi_{i,1}}$ are the complex amplitudes of the received authentic and spoofed symbols, respectively.

Under the assumption that $\tilde{s}_i(n) = s_i(n)$ so that there are no spoofer errors, the overlapped received symbol becomes,

$$r_i(n) = \alpha_0 \left(1 + \frac{\alpha_1}{\alpha_0}\right) s_i(n) + w_i(n) \tag{4.11}$$

where $\hat{E}_s \doteq |\alpha_0 \left(1 + \alpha_1/\alpha_0\right)|^2$ now becomes the energy of the overlapped symbol. For the sake of clarity we will focus on the two limiting cases when both signals add constructively or destructively. After simplifying the overlapped symbol energy term and merging within (4.5), the SER in the presence of spoofer becomes,

$$p_{u,1} = \frac{1}{2}\text{erfc}\left(\sqrt{T_d \left(\frac{C}{N_0}\right)_{|a,u} \left[1 + \frac{1}{\text{SSR}} + 2\frac{\cos\Delta\phi}{\sqrt{\text{SSR}}}\right]}\right) \tag{4.12}$$

where the snapshot index i has been omitted for the sake of clarity and $\text{SSR} \doteq |\alpha_0/\alpha_1|^2$ is defined as the Signal to Spoofer Ratio (SSR) whereas $\Delta\phi \doteq \phi_1 - \phi_0$ is the relative phase difference between the authentic and the spoofed signals. Two limit cases can be distinguished depending on whether the two signals overlap constructively, i.e. $\Delta\phi = 0$, or destructively, i.e. $\Delta\phi = \pi$. The latter leads to the worst SER, which is therefore retained here and given by,

$$p_{u,1} = \frac{1}{2}\text{erfc}\left(\sqrt{T_d \left(\frac{C}{N_0}\right)_{|a,u} \left[1 + \frac{1}{\text{SSR}} - \frac{2}{\sqrt{\text{SSR}}}\right]}\right). \tag{4.13}$$

The resulting worst SER in (4.13) is shown in Figure 4.5 below. As can be seen, the largest degradation due to the phase misalignment between the authentic and the spoofed signal and therefore, the largest SER, is experienced when both signals have similar power levels and thus SSR = 0 dB. When they overlap destructively, the resulting signal vanishes and thus it is not possible to reliably retrieve the symbols anymore, thus leading to SER = 0.5, and clearly unveiling the presence of spoofer. This means that even if the spoofer is replaying exactly the authentic signal with no errors, just for the fact of having a relative phase offset with respect to the authentic signal, the resulting aggregate signal may significantly cancel out and the spoofer could easily

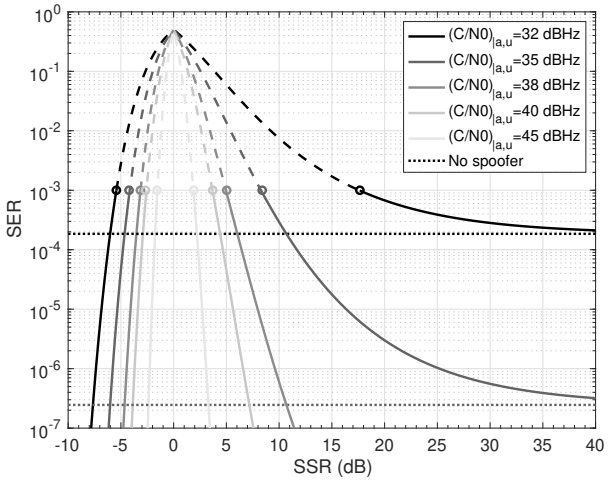


Figure 4.5: SER due to the destructive overlapping of the authentic and spoofed signals at the user's receiver as a function of the signal to spoofer ratio (SSR). Dashed lines represent the values of SSR that lead to an excessive SER (i.e. $> 10^{-3}$), and thus are likely to be avoided by a potential spoofer in order to remain unnoticed.

be detected. The more similar the power of the spoofer and the authentic signal, the more prominent this destructive effect is. It is for this reason that any spoofer willing to fool the victim's receiver without being noticed would try to avoid such working point where SSR = 0 dB. Instead, it would try to operate such that the SER caused by the phase misalignment between the authentic and the spoofed signal remains low. For instance, SER $< 10^{-3}$, such that the resulting SER is at least one order of magnitude smaller than the probability of error incurred by the sophisticated spoofer introduced in Section 4.2.4, when estimating the unpredictable symbols. As can be seen in Figure. 4.5, the region of SSR values to be avoided is that indicated by the dashed lines, since they incur in an easily detectable SER. For instance, $-5 <$ SSR < 5 dB at $(C/N_0)_{|a,u} = 40$ dBHz. Outside of this dashed line region, the overlap of the authentic and spoofed signals is well dominated by either the authentic or the spoofed signal, and therefore, it is reasonable to approximate the overlapped signal by its dominant signal only. Unless otherwise stated, this will be the assumption considered henceforth. Nevertheless, in another aspect, the spoofer could be compelled to be in worst SER region. Since the spoofer could be seen as a multi-path ray being aggregated with authentic signal with the provided relative phase offset and the power advantage herein. This working condition takes the spoofer outside

the region it is trying to avoid i.e. outside the dashed line region. However, a choke ring antenna could be used as an additional component due to its capabilities of attenuating the multi-path impinging from near the horizon and below the antenna [67]. Hence impelling the spoofed signal power to be equal to authentic signal. This enforced the spoofer into the worst SER region again.

4.2.7 Symbol errors due to multipath

The presence of multipath due to surrounding obstacles is another impairment that can hinder the detection of spoofed signals, since the energy per symbol is degraded and thus a higher SER is incurred, even when no spoofer is present. A higher SER than expected can mislead spoofing detection techniques working at symbol level, and therefore lead to a higher probability of false alarm. In order to assess the impact of multipath at symbol level, we will consider a simple one-ray multipath model following the same approach as in the performance requirements specification in [21], Appendix A3.3. Note that we are focusing on the symbol-level performance of the received signal and not on its positioning performance. It is for this reason that the SER becomes our target performance metric rather than the time-delay, pseudorange or position estimation accuracy. It is important to remark that while the latter strongly rely on the shape of the correlation peak, the former just depends on the energy of the maximum point of that peak, which is a more robust metric in front of multipath propagation effects.

The SER in the presence of multipath can be computed using the expression in (4.5) by replacing the nominal energy per symbol, $E_s = T_d C$ in AWGN, with its multipath-affected counterpart. The latter is computed herein following a similar procedure to the computation of the Multipath Error Envelope (MEE). That is, a delayed multipath replica is added to the Line Of Sight (LOS) signal and the ensemble is correlated with the local replica at the user's receiver. Two cases are considered, namely when the multipath replica adds constructively or destructively to the LOS. The maximum peak of the resulting correlation function is determined for both cases. Then instead of measuring the delay of those peaks, as it would be the case in the MEE, it is their energy what is computed here and the smaller value (i.e. worst energy per symbol) is retained, thus leading to the so-called worst SER.

The worst SER results are shown in Figure 4.6 as a function of the reflected path delay for different values of the C/N_0 of the authentic signal, namely $(C/N_0)_{|a,u}$. The results have been obtained for a Signal to Multipath Ratio (SMR) of 4.5 dB as specified in [21]. For Galileo E1, a relative

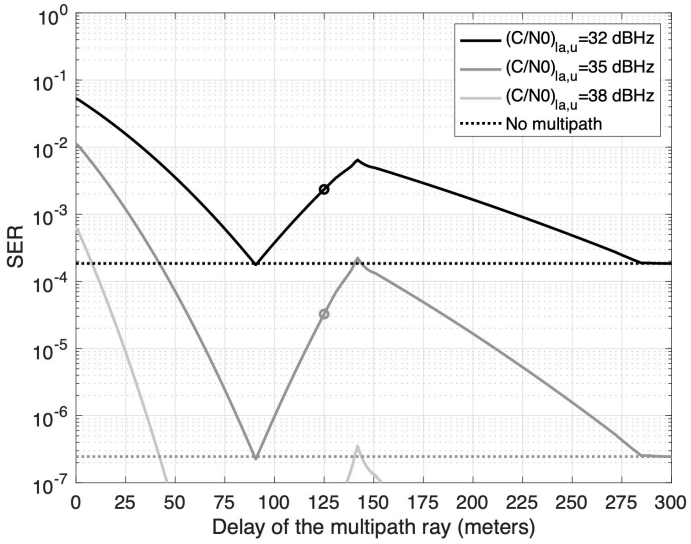


Figure 4.6: Worst SER for different C/N_0 values of the authentic signal at the user's receiver when a single-ray reflection is present, using SMR = 4.5 dB as specified in ([21], Appendix A3.3).

delay of 125 meters is considered as well in [21] for the reflected ray. This value corresponds to the '$\circ$' markers shown in Figure 4.6, which show a worst SER $\sim 10^{-3}$ at $(C/N_0)_{|a,u} = 32$ dBHz and SER $\sim 10^{-5}$ at $(C/N_0)_{|a,u} = 35$ dBHz. Note that despite the very low C/N_0 value, the resulting worst SER is one order of magnitude smaller than that incurred by the sophisticated spoofer considered in subsection 4.2.4 operating with 8 dB more C/N_0 and no multipath. This result suggests that multipath is not likely to cause a serious concern for symbol-level spoofing detection, as opposed to what often occurs for time-delay estimation in conventional GNSS receivers. To support this claim, note that barely 200 symbols were needed to detect a sophisticated spoofer in the pessimistic case considered in Section 4.2.4. In contrast, at least $1,000$ symbols are needed now when it comes to observe one symbol in error due to multipath only, and in actually worst C/N_0 working conditions than the sophisticated spoofer. In other words, it is far easier to observe a symbol error due to a spoofer trying to estimate the unpredictable symbols, than a symbol error due to multipath. A similar statement is also possible for close-in multipath, whose impact can be neglected provided that a slightly higher, $(C/N_0)_{|a,u} \geq 38$ dBHz, is considered. In summary, the impact of multipath as tested according to the guidelines in [21], does not see to be relevant provided that $(C/N_0)_{|a,u} > 32$ dBHz or $(C/N_0)_{|a,u} \geq 38$ dBHz for very close multipath.

Before concluding this section is worth mentioning that while multipath

does not seem to be a problem for symbol-level spoofing detection, at least for the reference scenario in [21], the situation is completely different when signal blockage is experienced. In that case the LOS is blocked and no signal arrives at the user's receiver. If this occurs for the whole snapshot, the satellite at hand will not be detected and thus no symbols will be provided. If this occurs during a piece of the snapshot only, but the satellite can successfully be acquired, then the symbols affected by the signal blockage will be randomly guessed, thus with SER = 0.5. In contrast, the rest of symbols will remain unaltered and thus providing their expected SER. In this situation, the average SER over the whole snapshot will be significantly degraded, and this may prevent the reliable implementation of a symbol-level spoofing detection technique. Signal blockage occurring in poor visibility working conditions is definitely the main source of degradation for the application at hand.

4.2.8 Symbol errors due to synchronization errors at the user's receiver

Another factor that may introduce errors when detecting the received unpredictable symbols is the presence of errors on the estimated code and carrier parameters of the received signal, which is often referred to as synchronization errors. This is particularly relevant in the case under study where a snapshot of signal is being processed. Unlike conventional receivers, snapshot receivers operate in acquisition mode only, thus there is no tracking stage. As a result, residual errors due to the inaccurate estimation of aforementioned parameters may contribute to the symbol error rate degradation. This effect is further aggravated when the user's receiver can only afford to gather a very short snapshot of just a few ms of signal. In that case, Q, the number of unpredictable symbols that are needed to guarantee at least one spoofer error, must be obtained by collecting N shorter snapshots of atleast L unpredictable symbols each such that $Q = NL$ symbols are finally obtained. Each snapshot is gathered and processed independently from each other, so the acquisition stage of the snapshot receiver must handle very short pieces of signal with only L symbols each. The snapshot length, L, is ultimately determining how accurately the code delay and carrier phase will be estimated, and thus, how large/small the residual code and carrier phase estimation errors will be.

In order to substantiate this fact and to further determine how much degradation is incurred in terms of SER, it is then to make use of the general result in [68] for the SER degradation of an M-PSK bandlimited Direct-Sequence Spread Spectrum (DS-SS) signal in the presence of estimation er-

rors on the synchronization parameters. The degradation is measured as the increase of C/N_0 that is required to preserve the same SER as when no estimation errors were present. Such degradation depends on the working conditions determined by the actual C/N_0 and it is given by (measured in dB),

$$D_\xi = -10\log_{10}\left(\frac{\mathrm{E}^2\left[d(\xi)\right]}{\sin^2(\pi/M)} - \frac{\mathrm{var}(d(\xi))}{\frac{2C}{N_0}T}\right) \tag{4.14}$$

where $d(\xi)$ is the distance between the M-PSK decision boundary and a received M-PSK symbol affected by generic estimation error ξ and, and T is the symbol period.

For carrier phase estimation errors, denoted henceforth as $\xi = \epsilon_\theta$ and for the BPSK symbols conveyed by the Galileo E1-B, the result in (4.14) simplifies to a degradation given by,

$$D_{\epsilon_\theta} \approx \frac{10}{\ln 10}\mathrm{var}(\epsilon_\theta) \geq \frac{10}{\ln 10}\frac{2L-1}{L(L+1)}\left(\frac{C}{N_0}T\right)^{-1} \tag{4.15}$$

where the variance of the phase estimation errors $\mathrm{var}(\epsilon_\theta)$ has been lower bounded in the right hand side of (4.15) by the corresponding Cramer Rao Lower Bound (CRLB) [69, Eq. (15.72)].

The resulting degradation is shown in Figure 4.7 as a function of the working C/N_0 when processing a snapshot of $L = \{2, 10, 25\}$ symbols, corresponding to a Galileo E1-B snapshot duration of $\{8, 40, 100\}$ ms, respectively. As can be seen, the worst losses are of about 0.2 dB, which are only experienced when working at the minimum detectable C/N_0 for each snapshot length. This minimum C/N_0 is indicated in Figure 4.7 by a '$\circ$' marker onto each curve and it was obtained so as to guarantee that each individual snapshot of Galileo E1-B symbols could successfully be detected at the acquisition stage of the user's receiver with a probability of detection $P_\mathrm{D} = 0.9$ and probability of global false alarm $P_\mathrm{FA} = 10^{-6}$. The user's receiver will typically operate well above this minimum detectable C/N_0, for instance under the standard values of 40 to 45 dBHz experienced outdoors, thus making the degradation due to carrier phase errors to be negligible at symbol level.

For time delay estimation errors, denoted henceforth as, $\xi = \epsilon_\tau$ the degradation in (4.14) particularizes to [68],

$$D_{\epsilon_\tau} \approx -\frac{10}{\ln 10}g''(t)_{|t=0}T_c^2\mathrm{var}(\epsilon_\tau) \tag{4.16}$$

where $g''(t)$ is the second derivative of the auto-correlation of the chip pulse used by the DS-SS signal and T_c the chip period. The results in [68] show

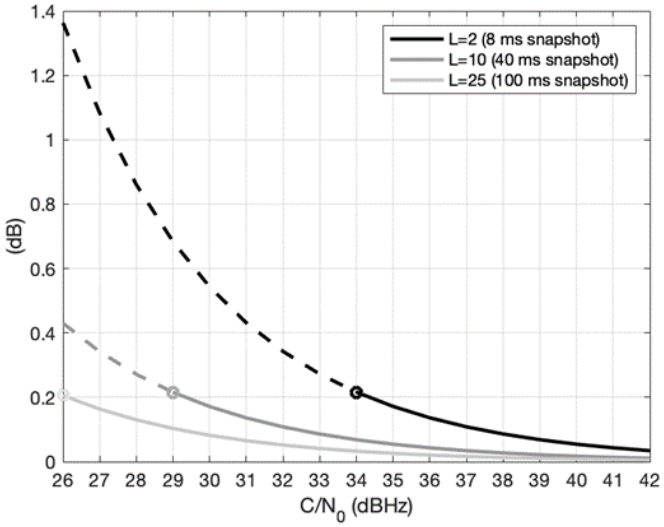


Figure 4.7: SER degradation, defined, as a loss in C/N_0 measured in dB, due to residual carrier phase estimation errors at the user's receiver. For the sake of completeness, the minimum C/N_0 for detecting a Galileo E1-B satellite with probability of detection 0.9 and probability of false alarm 10^{-6} is indicated in each curve by the '$\circ$' marker.

a similar effect to those already discussed for the carrier phase. That is, the degradation incurred by time delay estimation errors is in general very small, less than 0.1 dB provided that the time delay estimation jitter is smaller than 0.1 chips (1σ), or equivalently 30 meters. For the three cases considered when assessing the degradation due to carrier phase errors, namely snapshot lengths $L = \{2, 10, 25\}$ symbols, the degradation due to time delay estimation errors is shown below in Table 4.1. The worst case working conditions have been considered by taking the minimum detectable C/N_0 , which is again the minimum C/N_0 for which Galileo E1-B satellites can be detected using a snapshot of L symbols. The time delay estimation jitter has been obtained by numerically evaluating the CRLB for time delay estimation ([69], Eq. (3.40)), assuming a Galileo BOC(1,1) signal with a user's receiver bandwidth of 5 MHz. The corresponding SER degradation has been obtained by mapping such time delay estimation jitter onto Figure 4 in [68].

The results in Table 4.1 have been obtained for the minimum detectable C/N_0, which represents the worst possible working condition. Comparing the resulting SER degradation due to time delay estimation errors with that obtained for the same minimum detectable C/N_0 for carrier phase estimation errors in Figure 4.7, it can be seen that former is one order of magnitude

Table 4.1: Time delay estimation jitter in a snapshot receiver processing a snapshot of L Galileo E1-B symbols, operating at the minimum detectable C/N_0

.

Snapshot Length (symbols)	**Minimum detectable C/N_0** $P_d = 0.9$, $P_{fa} = 1 \cdot 10^{-3}$ (dB-Hz)	**Time delay estimation jitter at the minimum detectable C/N_0** (chips)	**SER degradation at the minimum detectable C/N_0** (dB)
2	34	0.04	0.02
10	29	0.04	0.02
25	26	0.04	0.02

smaller than the latter. This suggests that the impact of time delay estimation errors onto the SER can reasonably be ignored in practice, even when very short snapshots are processed. Finally, it is interesting to see that at the minimum detectable C/N_0, all snapshot lenghts exhibit the same SER degradation. This was already observed for the case of carrier phase errors (see 'o' markers in Figure 4.7), and it is due to the fact that at the minimum detectable C/N_0, all considered snapshots have the same energy, and it is energy what determines achieving a given probability of detection and probability of false alarm. This is the reason why shorter snapshots require a higher minimum detectable C/N_0, and longer snapshots a lower one. In this way, they all have the same energy. At the same time, energy is also what drives time delay and carrier phase estimation, so for the same energy, the same performance in terms of time delay and carrier phase estimation. This is the reason why the time delay jitter is the same in all rows of Table 4.1, and thus the corresponding SER degradation.

4.3 Symbol errors due to signal fading

The SER discussed so far at the user's side, taking into account that thermal noise, multipath and estimation errors were the only source of degradation on the received signal. While this may be the case in open-sky working conditions, the situation is dramatically different in urban scenarios. This is due to the presence of obstacles that sporadically block the line of sight

with the visible satellites, thus introducing severe fades in the received power levels. This situation poses serious concerns to the operation of the proposed spoofing detection method, because symbol errors are likely to appear at the user's side even if no spoofer is present at all. It is for this reason that a dedicated study is needed in order to assess the feasibility of the proposed spoofing detector in urban environments.

In this section, the focus is on the impact of shadowing effects onto the overall SER. To this end, it is resort to the well-known Land Mobile Satellite (LMS) narrowband propagation channel, a statistical model that becomes a self-standing approach for synthesizing large-scale environmental features leading to shadowing events [70]. The approach follows herein as in [71], where the signal transmission path is described in two separate states. On the one hand, a *good* state covering light shadowing conditions. On the other hand, a *bad* state covering heavy shadowing and blockage. Then, for each state, the fading properties are assumed to follow a stationary Loo distribution whose parameters depend on the environmental conditions such as user's motion, elevation angle of the satellite at hand, and environment itself, thus leading to multiple possible combinations of such conditions.

Let´s consider a synthetic Galileo E1-B signal with nominal LOS C/N_0 of 45 dB-Hz. By means of several Montecarlo realizations, it is to apply different LMS complex (*i.e.* in-phase and quadrature components) time series onto the above signal, and then repeat the process for the multiple environmental conditions mentioned above. For user's motion, the speeds of 50 and 3 km/h is considered, henceforth termed *vehicular* and *pedestrian* scenarios, respectively. For satellite elevation, the Galileo elevation statistics must be taken into account in order to select meaningful values. By taking Brussels as a reference location in Center Europe, elevation is below 30^{o} around 50% of the time, whereas 40% is found between 30^{o} and 60^{o} [72]. Therefore, we consider elevation angles of 20^{o}, 40^{o} and 60^{o}. Last, for the environment, we consider *urban* and *suburban* scenarios as representative of strong and mild shadowing conditions, respectively.

Figure 4.8 depicts the CDF of the SER experienced in the different combinations above, resulting in a total of 12 plots. In order to draw meaningful conclusions, the focus is on the SER values for which the cdf reaches the 0.9 barrier, thus providing some worst-case value that the SER can take. In that sense, for 20^{o} elevation, the SER degrades to $\sim 10^{-1}$ for vehicular motion in both urban and suburban environments, as well as the vehicular case for 40^{o} elevation in urban. From this point, the SER improves to $\sim 10^{-2}$ for more benevolent scenarios. These include the pedestrian case in urban and suburban, as well as the suburban vehicular, all three referring to 40^{o} elevation. Then, for 60^{o} elevation scenarios, the SER falls between 10^{-3} and 10^{-2}.

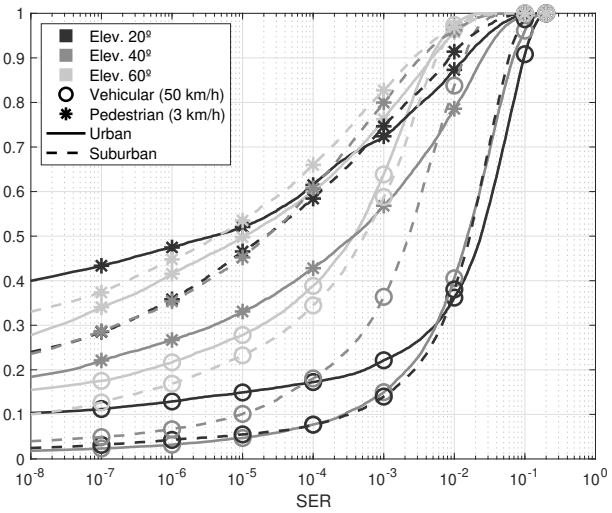


Figure 4.8: Cumulative distribution function (cdf) of SER in the presence of shadowing and blockage effects in urban and suburban environments, for different satellite elevation angles and a user at vehicular or pedestrian dynamics at a nominal $C/N_0 = 45$ dBHz.

The obtained results, particularly those for 20^{o} and 40^{o} satellite elevation angles, are comparable to the values of p_s considered herein, namely $p_s = \{0.1, 0.01\}$ in the optimistic and pessimistic cases, respectively. As a consequence, this is prone to increase the difficulties for a spoofing detector to dissociate whether a symbol error is due to a spoofing attack or it is caused by signal shadowing. Therefore, the importance of taking the shadowing effect into account for the design of the snapshot-based spoofing detector is concluded.

4.4 Detection of Spoofed Unpredictable Symbols

Once the problem statement and its boundary conditions have been introduced, it is now time to formulate and present the proposed symbol-level spoofing detector. This detector has two distinctive features. The first one is that it works on a short snapshot of received signal, typically of a few tens or hundreds of ms length, so it has only available a few symbols per snapshot to work with. The second feature is that it works at symbol level using the demodulated symbols provided by the user's receiver. By demodulated symbols mean the symbols obtained at the prompt correlator or maximum peak

of the correlation function between the received signal and the local replica, once the code delay, frequency and phase offsets have been estimated and compensated. Note that no decoding is needed but only to take the sign of the maximum peak of the correlation, as indicated in 4.2, which is actually the optimal decision rule for deciding equiprobably binary ± 1 symbols in AWGN [73].

4.4.1 Proposed Detector

Assuming the perfect synchronization, each snapshot of received signal is assumed to provide a set of L unpredictable symbols that are stacked into vector $\hat{\mathbf{s}}_i$ as in (4.8), where $i = 0, 1, \ldots, N-1$ and N is the total number of snapshots. Based on the set of received symbols, the problem is now how to compare them with the authentic ones in order to determine whether some of them may have been altered or not by the presence of a potential spoofer. This can be done by computing the Hamming distance between $\hat{\mathbf{s}}_i$ and $\mathbf{s}_i$, referred herein as $d_{\text{Hamming}}(\hat{\mathbf{s}}_i, \mathbf{s}_i)$, for each received snapshot. In this way the detector becomes,

$$H(\hat{\mathbf{s}}, \mathbf{s}) = \sum_{i=0}^{N-1} d_{\text{Hamming}}(\hat{\mathbf{s}}_i, \mathbf{s}_i)\,. \tag{4.17}$$

The Hamming distance returns the number of non-coincident elements between two vectors, in this case the received unpredictable symbols and the authentic ones. In other words, the Hamming distance applied to the problem at hand returns the number of errors in the received unpredictable symbols with respect to the authentic ones. By monitoring this metric one can make sure whether the number of errors that is obtained is reasonable for a receiver that should be processing an authentic signal at a given working conditions, and for which the probability of error should be constrained to $p_{u,0}$ in the absence of spoofing.

4.4.2 Statistical Characterization

For the two hypotheses under analysis, namely spoofer absent ($\mathcal{H}_0$) or spoofer present ($\mathcal{H}_1$), the statistical distribution of the detector in (4.17) is given by,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} B(Q, p_{u,0}) & : \mathcal{H}_0 \\ B(Q, p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{4.18}$$

where $B(m, p)$ stands for the Binomial distribution for a set of m symbols, $Q = NL$ is the total number of unpredictable symbols, $p_{u,0}$ is the probability

of symbol error at the user's side under $\mathcal{H}_0$, i.e. (4.5) when noise is the dominant degradation, and finally $p_{u,1}$ is the probability of symbol error at the user's side under $\mathcal{H}_1$, which is given by (4.6). Note that the latter depends on both the errors incurred by the spoofer and the errors incurred by the user's receiver itself.

Nevertheless, it must be taken into account that the demodulated symbols from a short snapshot of signal do not have an absolute phase reference and thus can be affected by a phase rotation of 180°. This means that the symbols obtained in (4.2) and stacked in $\hat{\mathbf{s}}_i$ can either be the correct symbols or the sign-reversed ones. This fact must be accounted for in the statistics of the proposed detector in (4.18), thus leading to a mixed Binominal distribution under each of the two hypotheses,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} \frac{1}{2}B(Q, p_{u,0}) + \frac{1}{2}B(Q, 1-p_{u,0}) & : \mathcal{H}_0 \\ \frac{1}{2}B(Q, p_{u,1}) + \frac{1}{2}B(Q, 1-p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{4.19}$$

Due to the mixed or bimodal distribution under each hypotheses, two different detection thresholds need to be implemented. The one on the lower side of the bimodal Binomial distribution will be referred to γ, while the one on the upper side of the bimodal Binomial distribution becomes its complementary, namely $Q - \gamma$.

Once the test statistic in (4.19) is computed using the symbols in $\hat{\mathbf{s}}$, the following decision rule can be implemented,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \leq \gamma \quad \Rightarrow \quad \text{decide } \mathcal{H}_0 \tag{4.20}$$

$$\gamma < H(\hat{\mathbf{s}}, \mathbf{s}) < Q - \gamma \quad \Rightarrow \quad \text{decide } \mathcal{H}_1 \tag{4.21}$$

$$H(\hat{\mathbf{s}}, \mathbf{s}) \geq Q - \gamma \quad \Rightarrow \quad \text{decide } \mathcal{H}_0 \tag{4.22}$$

4.4.3 Threshold Settings

The computation of detection threshold is one of the critical tasks due to the presence of many aspects that may affect the signal in the absence of spoofing, such as multipath and thermal noise effects. Therefore, the contribution of these nominal effects in terms of SER must be taken into account when designing γ, in such a way that γ encompasses all of these effects and allows determining when an abnormal number of symbol errors is present. Additionally, the decision of threshold implementation allows to provide insights about the number of errors that can be acceptable in detection process corresponding to the boundary conditions under $\mathcal{H}_0$.

Typically, the detection threshold can be determined by incorporating the desired probability of false alarm or vice versa. Statistically, the computation

of threshold requires the prior information of cumulative distribution function and given P_{FA} such that,

$$\gamma = \mathrm{cdf}^{-1}_{\mathrm{H}(\hat{\mathbf{s}},\mathbf{s})}(1 - P_{\mathrm{FA}}|\mathcal{H}_0) \tag{4.23}$$

It is also observed that the proposed detector follows the bimodal Binomial distribution, hence, the threshold will be calculated as a function of number of unpredictable symbols in a single snapshot, given probability of false alarm and the total accumulated probability of error due to each factor discussed above.

4.5 Performance Evaluation in Open Sky Environment

A preliminary assessment of the proposed detector has been carried out in open sky environment at first and then the urban and sub-urban scenarios are considered in later subsection to determine the behavior in front of different working conditions such as the snapshot length, Q, the probability of error incurred by the spoofer when estimating the unpredictable symbols, p_s, and the C/N_0 at the user's side, which determines the SER incurred by the user's receiver. Two types of experiments have been carried out.

`Experiment 1:` The detection performance has been assessed through the Receiver Operating Characteristic (ROC) curve, which represents the probability of detection as a function of the probability of false alarm. Further compressing ROC function into so-called Area under the curve (AUC) computes the integral of the ROC curve and summarizes into a single number the performance represented in the ROC curve. This is very useful because compressing the ROC curve into one single number leaves room for representing the results as a function of one more parameter than when the ROC curve is used, which needs already two dimensions for being represented (i.e. one for probability of detection and another one for probability of false alarm). A key feature of the AUC is that for a detector randomly declaring either $\mathcal{H}_0$ or $\mathcal{H}_1$, the ROC curve would be a straight line ranging from coordinate $(P_{\mathrm{D}}, P_{\mathrm{FA}}) = (0, 0)$ to coordinate $(P_{\mathrm{D}}, P_{\mathrm{FA}}) = (1, 1)$. This means that the AUC would be equal to 0.5 for a random detector. In contrast, for an ideal detector keeping $P_{\mathrm{D}} = 1$ when $P_{\mathrm{FA}} \to 0$ the AUC would be equal to 1. So the AUC values range from 0.5 (worst case) to 1 (best case). In some special cases the ROC may appear below the straight line of a random detector, thus leading to AUC < 0.5 or even AUC $\to 0$. This situation occurs when hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are reversed in the data being processed. For instance, when BPSK symbols are detected in the presence of a 180° phase

Table 4.2: The computation of threshold for snapshot length $L = 8$.

dB	**Noise** ($p_{u,0}$)	**Multipath** ($p_{u,0}$)	**Shadowing** ($p_{u,0}$)	**Total** ($p_{u,0}$)	**Threshold** ($P_{fa} = 10^{-4}$)
Open-sky					
$(C/N_0)_{\text{a,u}}$ (> 40 dB-Hz)	$< 10^{-18}$	0	0	$< 10^{-18}$	0
Open-sky					
$(C/N_0)_{\text{a,u}}$ (> 32 dB-Hz)	$2 \cdot 10^{-4}$	0	0	$2 \cdot 10^{-4}$	1
One-ray multipath,					
$(C/N_0)_{\text{a,u}}$					
(32 dB-Hz, $SMR = 4.5$ dB)	$2 \cdot 10^{-4}$	$3 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$	2
LMS shadowing					
$(C/N_0)_{\text{a,u}}$					
(45 dB-Hz, urban pedestrian, 95%)	~ 0	10^{-2}	10^{-2}	10^{-2}	4
LMS shadowing,					
$(C/N_0)_{\text{a,u}}$					
(45 dB-Hz, urban vehicular, 95%)	~ 0	10^{-1}	10^{-1}	10^{-1}	11

ambiguity, all symbols could incorrectly be decided sign-reversed. This leads to a mirrored ROC curve to that of the ideal case, resulting in AUC$\rightarrow$ 0, suggesting some underlying structure in the data, which is being interpreted in the opposite way it should be. If the detector was aware of it, then just reversing its decisions (i.e. declaring $\mathcal{H}_0$ instead of $\mathcal{H}_1$ and vice versa) would solve the problem.

The experiment conducted herein simulates the unpredictable symbols synchronously received at the user's terminal from an authentic GNSS satel-

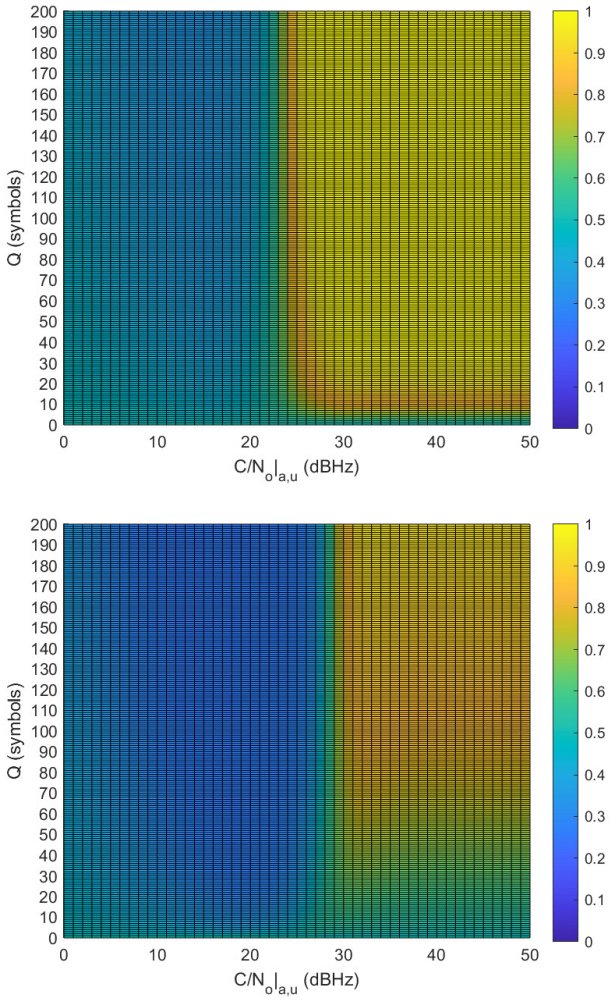


Figure 4.9: AUC for the proposed spoofing detector when the spoofer has 3dB power advantage in perfect LOS conditions than the authentic signal and the probability of error of the spoofer is $p_s = 0.1$ (upper) and $p_s = 0.01$ (lower).

lite at $(C/N_0)_{\mathrm{a,u}}$. When the spoofer is present, it appears simultaneously with the authentic signal and thus both signals overlap at the receiver. As in [74], it is assumed that the spoofer is perfectly aligned in time and frequency with the authentic signal, but with a random and uniformly distributed relative phase. It is also assumed that the spoofer has a 3 dB power advantage with respect to the authentic signal, which is a reasonable assumption taking into account that the goal of the spoofer is to prevail over the authentic signal, and have the user's receiver to lock onto it. The AUC of the proposed de-

tector is computed as a function of the snapshot length Q and $(C/N_0)_{\mathrm{a,u}}$ as shown in Fig. 4.9.

The plot at the upper side of Fig. 4.9 shows the AUC when the spoofer incurs in a probability of symbol error $p_s = 0.1$. In that case, at least 10 unpredictable symbols are needed for being able to observe at least one spoofer error. This is confirmed by the AUC rapidly raising in the Y-axis when more than 10 symbols are available and the C/N_0 is large enough for distinguishing spoofer errors from local errors incurred by the receiver due to its own thermal noise. For spoofer errors to be distinguishable from the receiver own errors, we need $p_{u,0} < p_s$, which starts to happen for $C/N_0 > 25$ dBHz, when the detector rapidly scores AUC $\rightarrow 1$. At the lower side plot of Fig. 4.9 the same experiment is shown but with a more sophisticated spoofer with $p_s = 0.01$. In that case, at least 150 unpredictable symbols are needed for AUC $\rightarrow 1$. Furthermore, the C/N_0 working point has now been shifted to the right to account for the fact that $p_{u,0} < p_s$, but that a more strict p_s is now involved. Now, at least $C/N_0 > 30$ dBHz is needed to reliably detect the presence of spoofer. In summary, the more sophisticated the spoofer (i.e. the smaller p_s) the more unpredictable symbols are needed to be processed and the larger the C/N_0 is needed to leave the receiver thermal noise symbol errors well below the spoofer incurred errors.

As can be observed in Figure. 4.9, we have region where AUC$\rightarrow$ 0 or AUC < 0.5, which is colored in dark blue. In this region, the symbol errors due to the boundary conditions effects are larger than those due to the spoofer, which remain at $p_s = 0.1$ and $p_s = 0.01$. This situation misleads the detector as it declares the opposite hypothesis to the correct one. This leads the AUC to be close to zero and in principle, this dark blue region should be avoided. It can be done by designing the two sided different thresholds which could be able to overcome the hypothesis inversion problem and enhance the detection region towards left. This opposite hypothesis problem and the relevant solution by modifying the statistical characteristics are presented in the following chapter.

`Experiment 2:` Keeping the boundary conditions into account, the second experiment intends to assess the time required by the proposed detector to reliably detect a spoofer. Three cases are defined, when spoofer is with 3dB C/N_0 advantage than user receiver, at the same level as user i.e. 0dB and when the user receiver has with 3dB C/N_0 advantage over spoofer. The results are shown in Fig. 4.10 again for $p_s = 0.1$ on the upper side plot, and $p_s = 0.01$ on the lower side one. The results have been obtained assuming that the receiver wakes up aligned with the time at which the unpredictable OSNMA symbols should be received, and therefore it is able to gather the maximum number of unpredictable symbols per snapshot. According to Fig.

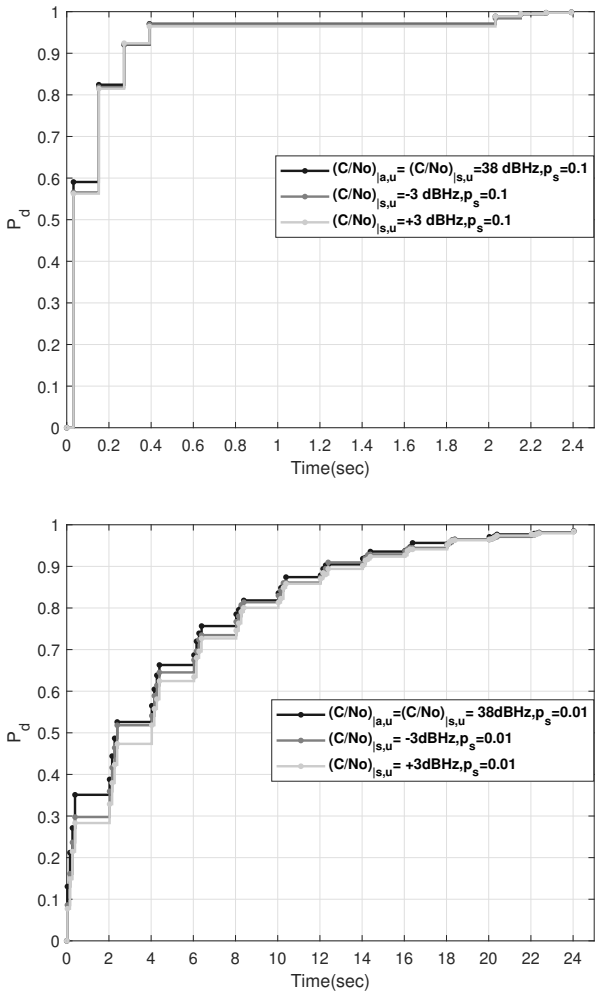


Figure 4.10: Probability of detecting the spoofer as a function of time when $p_s = 0.1$ (upper) and $p_s = 0.01$ (lower) for $C/N_0 = 38$ dBHz at the user's receiver and with the spoofer operating at -3, 0 and $+3$ dB more of C/N_0.

4.1, $L = 8$, and this number has been considered for all snapshots for the sake of simplicity. Note that the time depicted on x-axis set off upon the reception of unpredictable symbols following the 10 synchronization bit of odd page and the 7 symbols. The time vs detection plot starts exhibiting the value of detection as soon as the first batch of unpredictable symbols (i.e. 8) is processed. This explains why the detection step line initiate after $8 * 0.004 = 0.0032$ ms. The time for detecting 90% of the time a spoofer incurring in errors with $p_s = 0.1$ is less than 0.5 seconds at moderately low C/N_0 such as 38 dBHz. In contrast, for a spoofer with $p_s = 0.01$ and the

same C/N_0 at the user's terminal, more than 12 seconds are needed. Such a significant increase is mostly due to the fact that unpredictable symbols are transmitted every 2 seconds, so if the current symbols are not enough, the receiver must wait 2 seconds for the next group of unpredictable symbols to be received. The moderate C/N_0 is chosen here since it provides more insights about the difference in detection performance when either spoofer or user has a power advantage advantageous relative to this reference C/N_0. Opting for an even lower C/N_0 would not be representative of the nominal working scenario of a GNSS receiver, whereas opting for a higher C/N_0 would make the aggregated SER to become too sensitive to the presence of the spoofer when both the user and the spoofer have similar power levels. The latter can be observed in the sharpness of the SER curve in Figure 4.5. The more detailed intuition about detection time can be realized in the Table 4.3

Table 4.3: The time required to detect the spoofing attack under different conditions

L_s	P_d	**Time required** (high duty cycle), $p_s = 0.1$ (seconds)	**Time required** (low duty cycle), $p_s = 0.1$ (seconds)	**Time required** (high duty cycle), $p_s = 0.01$ (seconds)	**Time required** (low duty cycle), $p_s = 0.01$ (seconds)
8	0.90	0.278	4.03	12.39	54.03
8	0.95	0.39	6.03	18.03	72.03
8	0.99	2.15	8.03	24.15	98.03
6	0.90	0.38	6.02	18.02	72.02
6	0.95	2.02	8.02	22.3	96.02
6	0.99	2.26	12.02	34.14	142.02

Additionally, Table 4.3 provides a more detailed overview of the detection time for two practical use cases, namely when the receiver is operating in either low or high duty-cycle. Low duty-cycle refers to the case when the receiver only gathers one out of the four batches of unpredictable symbols that are available per odd page, which are shown in green color in Figure 4.1. In this case, the receiver will require a higher detection time in order to

compensate for the scarcity of gathered unpredictable symbols per odd page. This effect will be particularly critical for detecting spoofers that incur in a low probability of error, such as the considered $p_s = 0.01$ herein. In contrast, by high duty-cycle we refer to the case when all batches of unpredictable symbols per odd page are gathered by the receiver. An overview of the impact of such duty-cycle operation is summarized in Table 4.3, where it can be seen how the detection time significantly grows in low duty-cycle operations.

In spite of the performance degradation for low duty cycle operation, the resulting detection time can be upper bounded by approximately 10 seconds, which is smaller than the few tens of seconds that are needed by the partial correlation technique proposed in [18] in similar working conditions. It is worth mentioning, though, that both techniques are actually complementary and should be used jointly. The reason is that for a spoofer not to be detected by the partial correlation technique in [18], it should estimate the unpredictable symbols as soon as possible, thus incurring in the shortest possible delay in the transmitted spoofed signal with respect to the authentic one. However, as the observation time for estimating the unpredictable symbols decreases, the probability of error increases, making it more susceptible to detection by the symbol-level detection technique proposed in the present work.

4.6 Performance Evaluation in Urban and Sub-Urban Environment

Till now, the proposed detector is examined in an open sky environment only and taking into account all the boundary conditions while assuming that spoofer employs power advantage over the user´s receiver. It is evident that spoofer with such advantageous conditions can still reliably be detected for higher and moderate C/N_0 working scenarios. This section broadens the analysis of detection performance under the challenging environments, for instance, study the impact of signal fading in urban and sub-urban environment and at higher, moderate, and lower satellite elevation angles etc. It is possible that this fading impairments may have severe impact and hence incur more errors than the spoofer which could elevate the false alarms in detection performance. Moreover, a portion afterwards poses additional efforts to further optimize the detection performance by modifying the statistical properties of the proposed detector that significantly improves the spoofing detection.

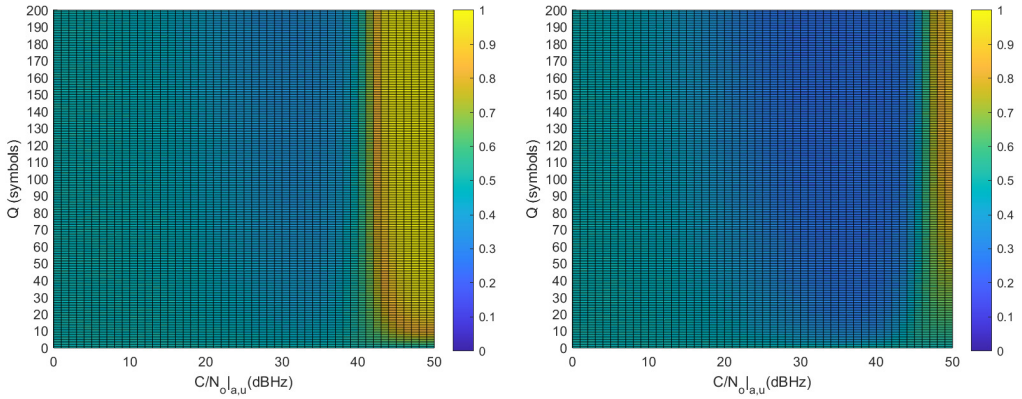


Figure 4.11: AUC for spoofer at 3dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

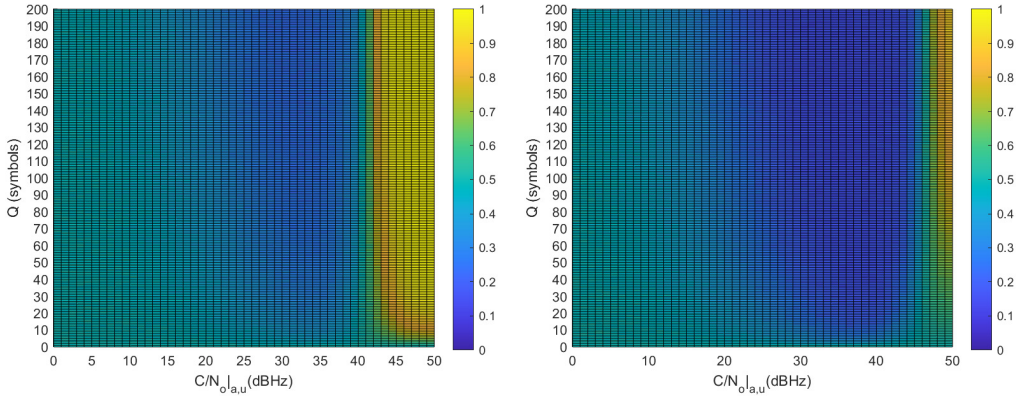


Figure 4.12: AUC for spoofer at 5dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

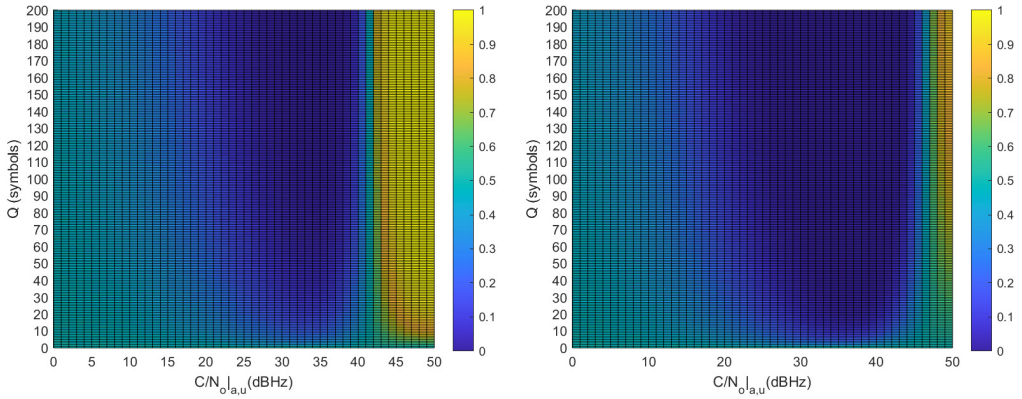


Figure 4.13: AUC for spoofer at 10dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

The detector performance in the presence of signal fading is analyzed through the same AUC curve as defined for open sky environment. However, AUC outcomes are extensively analyzed by considering different power advantage conditions over user´s receiver, for instance 3dB, 5dB, 10dB. It is realized from the Figure 4.8, the signal fading can have significant impact on detection performance since SER contribution from spoofer and signal fading is comparable. Therefore, it is imperative to comprehensively examine the detection performance for extensive scenarios. Thereby, it can provide meaningful and reliable information whenever a spoofer is present. This is a relevant question to be answered because, at first glance, symbol errors due to thermal noise, fading/shadowing, etc. are combined with symbols errors due to spoofing. Thus, it may not be fully clear whether detecting a symbol error is synonym of a spoofer being present or not.

As can be observed in Figure 4.11–4.13, the resulting AUCs can all be divided into three different regions as illustrated for AUC in previous chapter for the open sky environment . On the one hand, the region where AUC$\rightarrow$ 0.5, colored in green, which corresponds to Q and $(C/N_0)_{\text{a,u}}$ values making the detector to behave randomly, thus being unable to distinguish the presence or absence of spoofing. This region is clearly visible in Figure 4.11 and 4.12 ranging from $(C/N_0)_{\text{a,u}} = 0$ to $\sim 20 - 25$ dBHz and in Fig 4.13 from $(C/N_0)_{\text{a,u}} = 0$ to $\sim 10 - 14$ dBHz Within this region, the proposed detector is not feasible at all. This is due to the fact that in this region, the symbol errors by the spoofer and the symbol errors incurred by signal fading and all other factors introduced in the boundary conditions are nearly equal. As a result, the proposed detector is incapable of distinguishing whether the spoofer is present or absent, leading to abnormal behavior . However, $(C/N_0)_{\text{a,u}}$ at which the detector behaves randomly is comparatively very low and the typical operation of GNSS receivers under such low $(C/N_0)_{\text{a,u}}$ is not feasible.

On the other hand, the region where AUC$\rightarrow$ 1, colored in yellow is clearly distinguished in Figure. 4.11–4.13 when $(C/N_0)_{\text{a,u}} > 44 - 50$ dBHz and $(C/N_0)_{\text{a,u}} > 48 - 50$ for $p_s = 0.1$ and $p_s = 0.01$, respectively. Within this region, the detector can always detect the spoofer that incurs error with the given p_s values or greater . It is just a matter of time (i.e. having enough symbols) for the spoofer to be detected. It should be noted that as the propagation conditions harden, for instance, urban conditions in this case, a higher $(C/N_0)_{\text{a,u}}$ is needed for the yellow region to appear. This can be clearly observed when moving from the open-sky scenario in Figure. 4.9 to the LMS channel with 60° elevation angle in Figures. 4.11–4.13 . In general, the detector will continue to be feasible in these urban conditions just at the expense of requiring a higher nominal $(C/N_0)_{\text{a,u}}$.

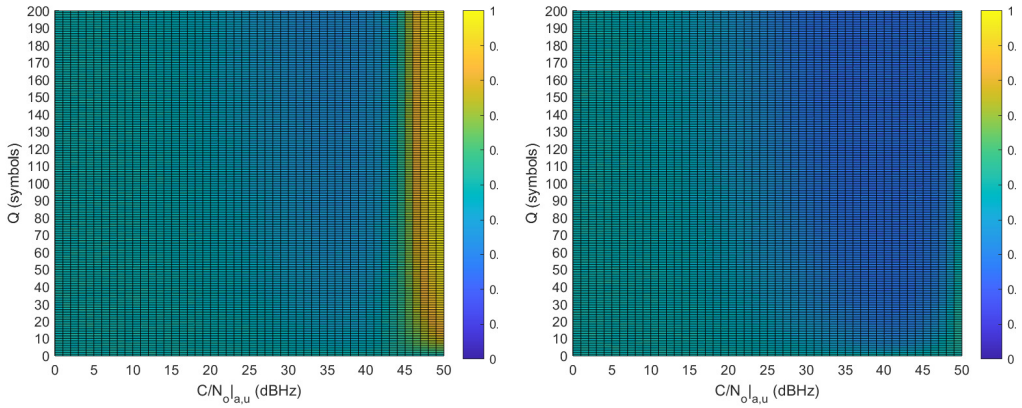


Figure 4.14: AUC for spoofer at 3dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

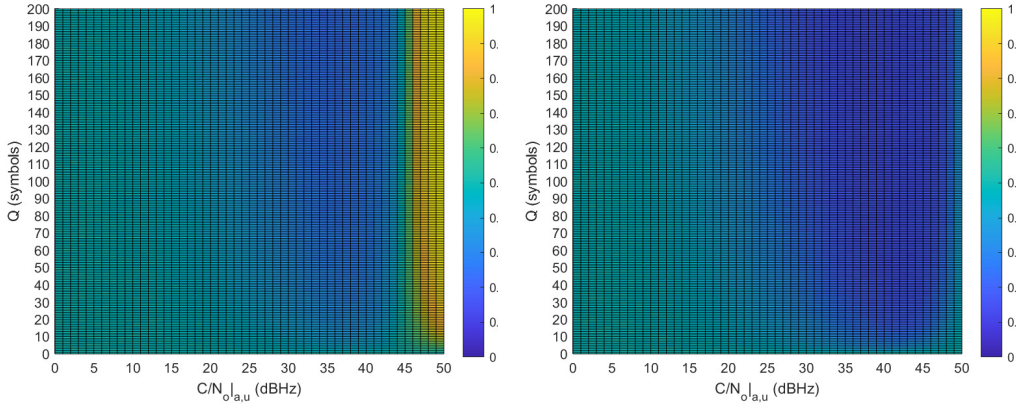


Figure 4.15: AUC for spoofer at 5dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

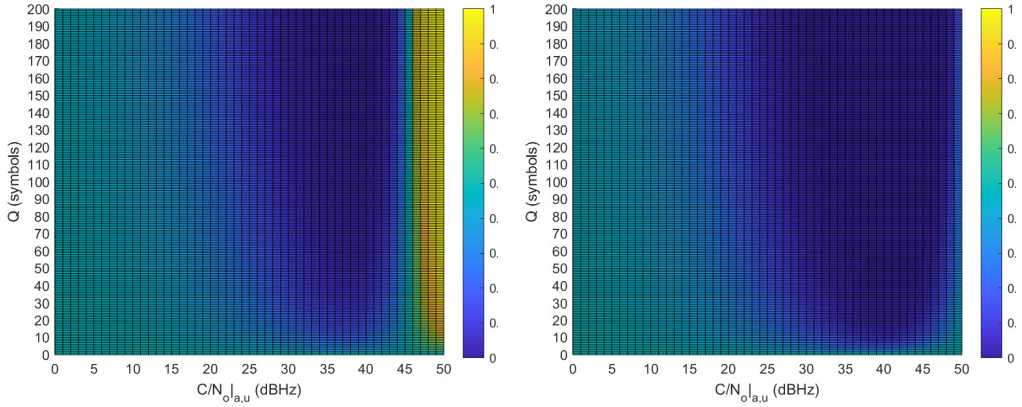


Figure 4.16: AUC for spoofer at 10dB power advantage in LMS, 40° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

Finally, there is a third region in the AUCs shown in the Figures 4.11–4.13 , corresponding to AUC$\rightarrow$ 0, colored in dark blue. This region is a depiction of hypothesis inversion problem when the symbol errors due to noise, fading and shadowing effects are larger than the errors incurred by spoofer. As a result, it leads to declare the opposite hypothesis and hence AUC < 0.5. This can be realized from the Figures. 4.11–4.13, as the power advantage of spoofer rises from 3dB to 10dB, the intensity of dark blue region is escalating. This is due to the fact that, SER contribution due to destructive overlapping of authentic and spoofed signal at user receiver becomes negligible as per given in Figure. 4.5, for higher values of power advantages. Hence, the contribution from noise, fading and shadowing effects becomes dominant than the spoofer itself and leading to hypothesis inversion. This situation misleads the detector because it tends to declare $\mathcal{H}_0$ when the spoofed signal is present, and $\mathcal{H}_1$ when the spoofed signal is absent, since far more errors are incurred when processing the noisy and degraded authentic signal than the spoofed one. This leads AUC $\rightarrow 0$ and in principle, this dark blue region should be avoided because the detector is not working properly. However, this problem is separately solved to a great extent in the following section.

Considering even more challenging working conditions in LMS channel, for instance, at 40^{o} elevation angle, the performance analysis in terms of AUCs is performed for the same power 3dB, 5dB, 10dB advantage scenario and illustrated in Figures 4.14-4.16. It is noticeable that the detection region highlighted in yellow color is significantly reduced when compared with the open sky and signal fading scenarios at 40^{o} elevation angle. However, detector will continue to be feasible for $p_s = 0.1$ just at the expense of requiring a higher nominal $(C/N_0)_{\text{a,u}}$. As can be seen from left hand side of Figures 4.14-4.16, the detection region remains nearly unchanged i.e. $p_s = 0.1$ regardless of power advantage scenario. This is due to the reason that at such higher $(C/N_0)_{\text{a,u}}$, the impact of destructive overlapping becomes negligible and the only contribution is from shadowing effect and the probability of error $p_s = 0.1$ incurred by spoofer.

The detector becomes unfeasible for the conditions, e.g. with 40° elevation and very sophisticated spoofers having a very low probability of error , such as in the right hand side plot of Figures 4.14 -4.16,regardless of any power advantage conditions. In such scenario, identifying the spoofing attack proves to be extremely formidable given that SER due to signal fading becomes dominant over SER by spoofer, where the latter stands at $p_s = 0.01$. Hence, as conclusive remarks at this stage, being a symbol-level detection, results show that the proposed detector is feasible and that spoofers can reliably be detected under most of the working conditions. However, the solution to the hypothesis inversion problem exists in all scenarios could further optimize

the detection performance. This can be done by modifying the statistical properties of the proposed detector as seen in next section.

4.7 Statistical Characterization of Snapshot OSNMA Spoofing Detector

The primary focus of this section is to provide the solution to incorporate the hypothesis inversion problem (i.e. chooses the wrong hypothesis under certain conditions) that appears due to the presence of signal impairments as seen in the preceding sections. This is important because the hypothesis inversion deteriorate the detection performance. Hence, this part of the chapter solves the problem through modifying the statistical properties of snapshot OSNMA detector i,e. by designing appropriate test statistics conditions and enhance the detection performance to a great extent.

Before delving into the solution, the hypothesis inversion must be depicted to clearly understand the problem. In this essence, let´s recall one of the figures that affected by the hypothesis inversion problem, for instance Figure 4.17 (upper) represents AUC when spoofer has 5dB advantage in perfect LOS conditions. Since AUC is a function of probability of detection P_d and false alarm probability P_{fa}, Figure 4.17 (lower) is a depiction of hypothesis inversion and further characterizes three different cases of AUC in terms of ROC curve. The central straight line refers to the random detector and can be specified as a lower bound for ROC curve. The right side or yellow region of Figure 4.17 (upper) but for $p_s = 0.1$, the grey curve in the upper side of Figure 4.17 (lower) is a representation of normal behavior, where the detector works efficiently. In contrast, the lower black curve of Figure 4.17 (lower) is similar to the situation for $p_s = 0.1$ when AUC < 0.5 or AUC $\rightarrow 0$ in dark blue color, where the detector is consistently declaring the opposite decision to the true one. The reason for displaying the AUC for $p_s = 0.01$ and ROC for $p_s = 0.1$ is to depict the abnormal situations for both error probabilities through concise and different perspectives. Fortunately, this problem could be circumvented by exploiting the detection threshold characteristics as explained by Figure 4.18.

Recalling two hypotheses under analysis, represents in the previous section, namely spoofer absent ($\mathcal{H}_0$) or spoofer present ($\mathcal{H}_1$). Figure 4.18 depicts three empirical and theoretical Probability Density Functions (PDFs) in terms of symbol errors under both hypotheses ($\mathcal{H}_0$ and $\mathcal{H}_1$). These three cases are picked from each of three regions of AUC described in Figure 4.9. The theoretical curves are acquired using Binomial distribution and the em-

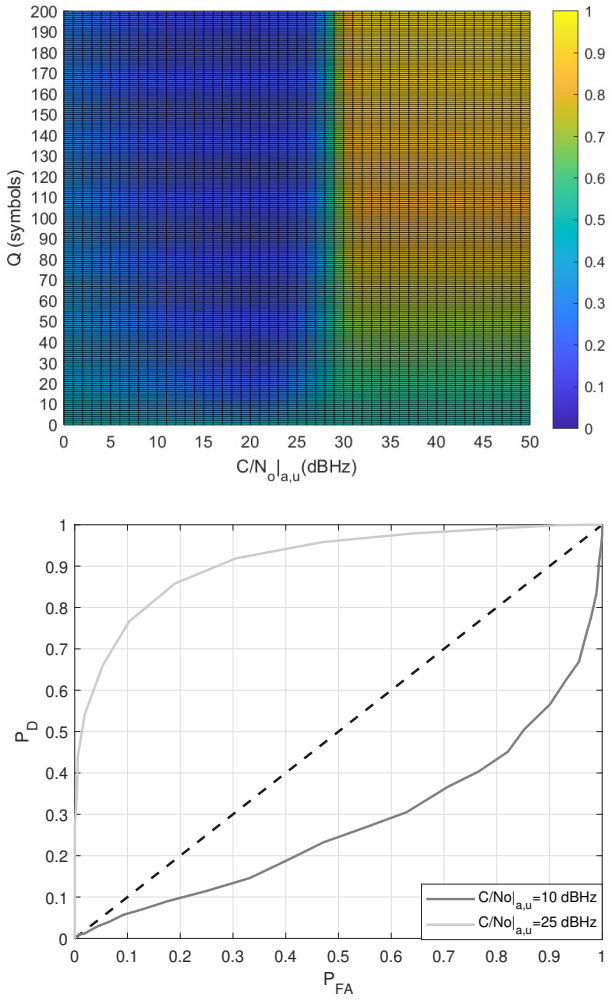


Figure 4.17: AUC when the spoofer has 5dB power advantage in perfect LOS conditions with $p_s = 0.01$ (upper) and Empirical ROC curve for a spoofer with 5dB power advantage in perfect LOS with $p_s = 0.1$ and $Q = 100$ (lower).

pirical curves are obtained using Monto Carlo simulations whereas the perfect match of theoretical and simulated curves confirm the authenticity.

As can be seen, Figure 4.18 (a) characterizes the situation when symbol errors due to signal impairments exceeds over the errors by spoofer. This happens when AUC < 0.5 at the selected working condition from Figure 4.9 i.e. $(C/N_0)_{\text{a,u}} = 15$ dBHz, $p_s = 0.01$ and $Q = 100$ and the proposed detector emerges with hypothesis inversion problem, while Figure 4.18 (b) depicts the normal behavior i.e. AUC > 0.5 at $(C/N_0)_{\text{a,u}} = 26$ dBHz, $p_s = 0.1$ and $Q = 100$ and detector works well at this situation as colored "yellow" in

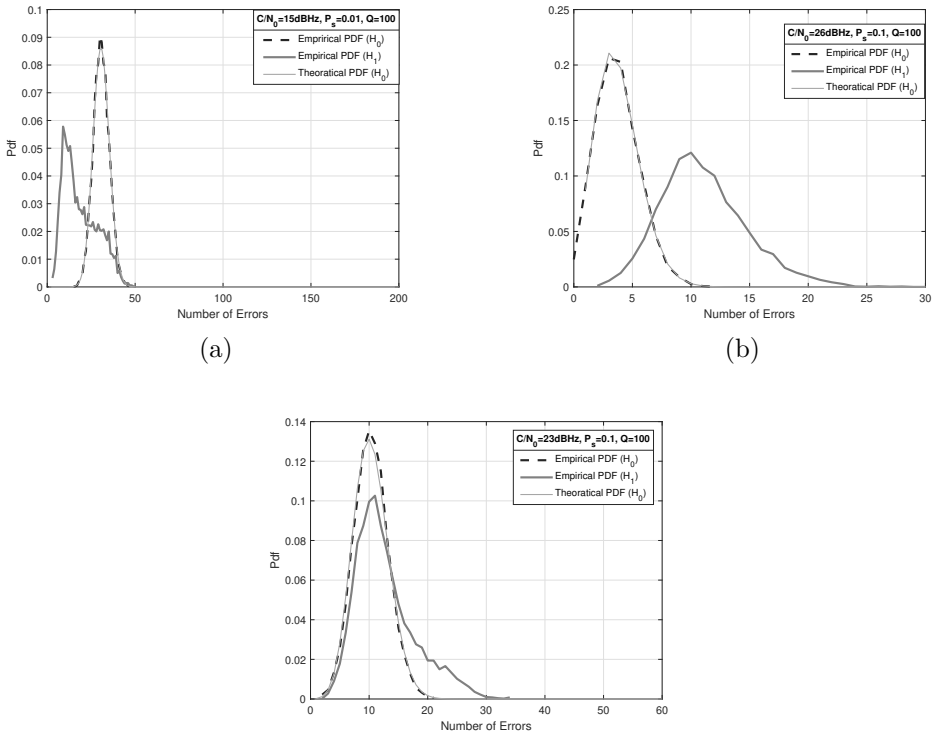


Figure 4.18: The empirical PDFs using Monto Carlo simulation and theoretical PDFs using Biomial distribution representing the AUC´s three regions (Blue, Green and Yellow) in terms of symbol errors under $\mathcal{H}_0$ and $\mathcal{H}_1$, when (a) AUC < 0.5, (b) AUC > 0.5 and (c) when AUC $= 0.5$.

Figure 4.9 (upper). The ultimate Figure 4.18 (c) is about the situation when symbol errors due to spoofer and impairments are comparable or almost equal, for instance at $(C/N_0)_{\text{a,u}} = 23$ dBHz, $p_s = 0.1$ and $Q = 100$ and detector is not able to detect the attack at all.

It can be observed from Figure 4.18 (a) and (b), the hypothesis $\mathcal{H}_1$ can exist on either side of the binomial distribution of $\mathcal{H}_0$, two different thresholds γ_1 and γ_2 must be placed for deciding among hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, and given by [75],

$$\gamma_1 = F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s})}(1 - P_{\text{FA}}|\mathcal{H}_0) \tag{4.24}$$

and

$$\gamma_2 = F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s})}(P_{\text{FA}}|\mathcal{H}_0) \tag{4.25}$$

where $F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s})}$ is the inverse cumulative distribution of the detector under $\mathcal{H}_0$ and P_{FA} is desired probability of false alarm. Moreover, it is already remarked that the demodulated symbols can be affected by a rotation of 180°. Therefore, the detection criteria will be based on the following decision rule,

$$\begin{array}{rcl} \gamma_2 \leq H(\hat{\mathbf{s}},\mathbf{s}) \leq \gamma_1 & \Rightarrow & \text{decide } \mathcal{H}_0 \\ Q-\gamma_1 \leq H(\hat{\mathbf{s}},\mathbf{s}) \leq Q-\gamma_2 & \Rightarrow & \text{decide } \mathcal{H}_0 \end{array} \tag{4.26}$$

and declares the alternative hypothesis $\mathcal{H}_1$ under any of the following test statistics conditions,

$$\begin{array}{rcl} H(\hat{\mathbf{s}},\mathbf{s}) < \gamma_2 & \Rightarrow & \text{decide } \mathcal{H}_1 \\ \gamma_1 < H(\hat{\mathbf{s}},\mathbf{s}) < Q-\gamma_1 & \Rightarrow & \text{decide } \mathcal{H}_1 \\ H(\hat{\mathbf{s}},\mathbf{s}) > Q-\gamma_2 & \Rightarrow & \text{decide } \mathcal{H}_1 \end{array} \tag{4.27}$$

The proposed detector with modified statistical characteristics would be capable to overcome the hypotheses inversion problem and further enhance the detection performance by converting the dark blue region of Fig. 4.17 (upper) and lower symmetrical region of Fig. 4.17 (lower) to the detection region, which is validated in the later subsection

4.8 Performance Evaluation

This section imparts the analysis of detection performance given the statistical characterization of snapshot OSNMA. In addition, it provides the insights of, to what extent the formulated detector is feasible to utilize for spoofing detection in an extensive working conditions. To this end, the performance is validated by analyzing the probability of detection P_{D} as a function of Q symbols and $(C/N_0)_{|\text{a,u}}$, while both thresholds γ_1 and γ_2 are calculated as a function of given $P_{\text{FA}} = 10^{-3}$ as in (4.24) and (4.25).

Using the proposed detector with modified statistical properties, it can be observed in Fig. 4.19 (upper), most of the part associated to dark blue region from Figure. 4.17 (upper) is translated into detection region. One could argue that this problem could be solved just by reversing the decision within a specific $(C/N_0)_{|\text{a,u}}$ window. However, it is only possible when BPSK symbols are detected in the presence of a 180° phase ambiguity. In this case it may happen that all symbols are decided incorrectly with a reversed sign and then reversing its decision could solve the problem. Since, one could not know about the exact contribution of error probability p_s by spoofer, which can be even higher and hence, the dark blue area would automatically be included into the detection region due to the significant contribution of

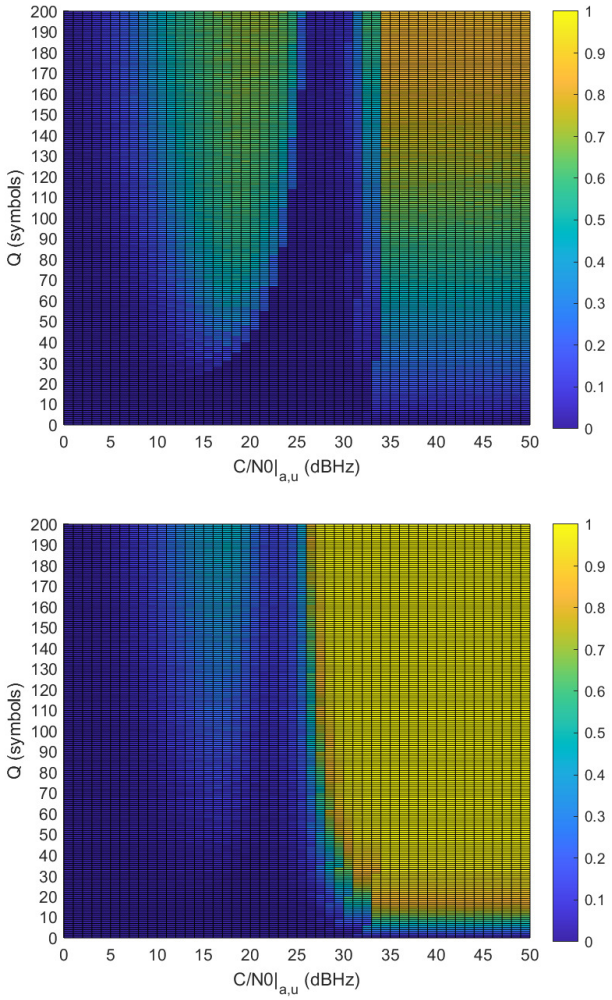


Figure 4.19: P_{D} for a spoofer with 5dB power advantage in perfect LOS conditions with $p_s = 0.01$ (Left) and $p_s = 0.1$ (Right).

symbol errors from the spoofer, which broadens the detection region towards left, but now, just inverting the hypothesis would make it again under $\mathcal{H}_0$. Therefore, it is need of the hour to exploit the statistical properties of the problem and place an appropriate threshold for efficient detection.

SImilar to previous discussions on AUC figures, the interpretation of Figure 4.19 can also be performed by dividing into three regions. On the one hand, the prominent region with $(C/N_0)_{\mathrm{a,u}} > 32 - 33$ dBHz can be categorized as normal region, in which the probability density function (PDF) under $\mathcal{H}_1$ lies just next to the PDF under $\mathcal{H}_0$ and the detector can always detect the spoofer provided that the latter has a probability of error dif-

ferent from zero. On the other hand, there is a region within the range of $24 < (C/N_0)_{\text{a,u}} < 32$ dBHz in Fig. 4.19 (Upper) and $20 < (C/N_0)_{\text{a,u}} < 26$ dBHz in Fig. 4.19 (Lower), where the detector is not feasible at all. It is due to the fact that the symbols error contribution due to impairments under $\mathcal{H}_0$ becomes identical to the total symbol errors under $\mathcal{H}_1$, consequently, two PDFs lie exactly on each other and leave no room to detect on either side of the distribution.

The third region is categorized as critical region for $(C/N_0)_{\text{a,u}} < 25$ dBHz in Figure 4.19 (Upper) and $(C/N_0)_{\text{a,u}} < 19$ dBHz in Figure 4.19 (Lower), which is a solution to the problem exists in left symmetry of Fig. 4.17 (Upper) when AUC < 0.5 or even AUC $\to 0$. It is worth to observe that the problematic region is converted into detection region in Figure 4.19 by identifying the appropriate threshold properties and solved the aforesaid hypotheses inversion problem. Note that, in this region, the detection probability for $p_s = 0.01$ is exceeding as compared to $p_s = 0.1$, which seems to be illogical because $p_s = 0.1$ should bring on with more symbol errors than $p_s = 0.1$ but it is in-fact logical. In this critical region, the distribution under $\mathcal{H}_1$ shall be next to the distribution under $\mathcal{H}_0$. Since the errors incurred by spoofer with $p_s = 0.01$ would be lesser and the corresponding distribution would lie on the extreme next as compared to the distribution associated to $p_s = 0.1$. In other words, AUC for $p_s = 0.01$ in the critical region would have more values closer to zero or less than 0.5 as compared to AUC for $p_s = 0.1$. Since it is implied that more closer the AUC to zero, farther will be the distribution under $\mathcal{H}_1$ from the distribution under $\mathcal{H}_0$. Therefore, it would be easy for a modified detector to detect the attack.

4.9 Practical Implementation Aspects

As already discussed, the performance of the proposed snapshot OSNMA spoofing detector strongly depends on the availability of unpredictable symbols, which are the key input data to ascertain whether the symbols being received might have been spoofed or not. The availability of OSNMA data or, in general, I/NAV data, is a general concern in spoofing detection techniques that make use of OSNMA data provided by existing mass-market receivers. This is due to the fact that, as reported in [24], the availability of I/NAV data in those receivers is currently below 10%, in the best case. It is for this reason that techniques operating in snapshot mode, as the one proposed herein, can make a difference because they directly demodulate the received data symbols from the gathered signal samples. Snapshot receivers are thus well-suited for the implementation of the proposed spoofing detec-

tion technique, since they circumvent many of the limitations and constraints of conventional receivers that try to fully decode the whole I/NAV message. Instead, snapshot receivers can focus on collecting just the short pieces of signal where unpredictable symbols are present. Nevertheless, snapshot receivers must also cope with certain impairments that seriously hinder the availability of unpredictable symbols, and thus, have an impact in terms of spoofing detection performance. The two most relevant impairments are, on the one hand, the fact that visible satellites have different ranges with respect to the user's position, and thus, their signals arrive at the user's receiver with slightly different reception times. This means that within the same snapshot of received signal, not all satellites have the same number of unpredictable symbols. It would be possible, though, to gather a long enough snapshot to encompass all the unpredictable symbols for all OSNMA active satellites. However, this would require an excessive snapshot length that could not be afforded, for instance, by devices with constraints on low-power consumption such as GNSS-enabled IoT devices. On the other hand, even if all satellites arrived perfectly time-aligned, the receiver is subject to clock offsets that prevent it from waking up at the exact time when the unpredictable symbols are expected to be received. Similarly to the previous effect, this would cause the received snapshot to contain less unpredictable symbols than the expected ones, and thus to incur in some performance degradation. Both impairments will be briefly discussed next.

4.9.1 Relative time delay between visible satellites

The impact of the relative time delays on received signals from different visible satellites is empirically analyzed by employing the open-source satellite observatory data acquired from the International GNSS Service (IGS) network stations of Sweden, France and French Guiana. The retrieved data is available in the form of Receiver Independent Exchange format (RINEX) files which is then processed for over a period of up to one day at a sampling rate of 30 seconds by using GFZRNX- RINEX GNSS Data Conversion and Manipulation Toolbox [76]. The high sampling rate and longer time duration allows to acquire a precise idea about the maximum time delay difference among all visible satellites, which can be taken into account when setting the snapshot length to be used by the receiver. The relative time delays are found by using the binomial coefficient terminology, which provides all the possible combination of relative delays corresponding to each satellite in view. After analyzing the real data, the relative time delays between visible satellites are found to exhibit a zero-mean gaussian-like distribution, as can be seen in the upper side of Figure 4.20. The corresponding Cumulative

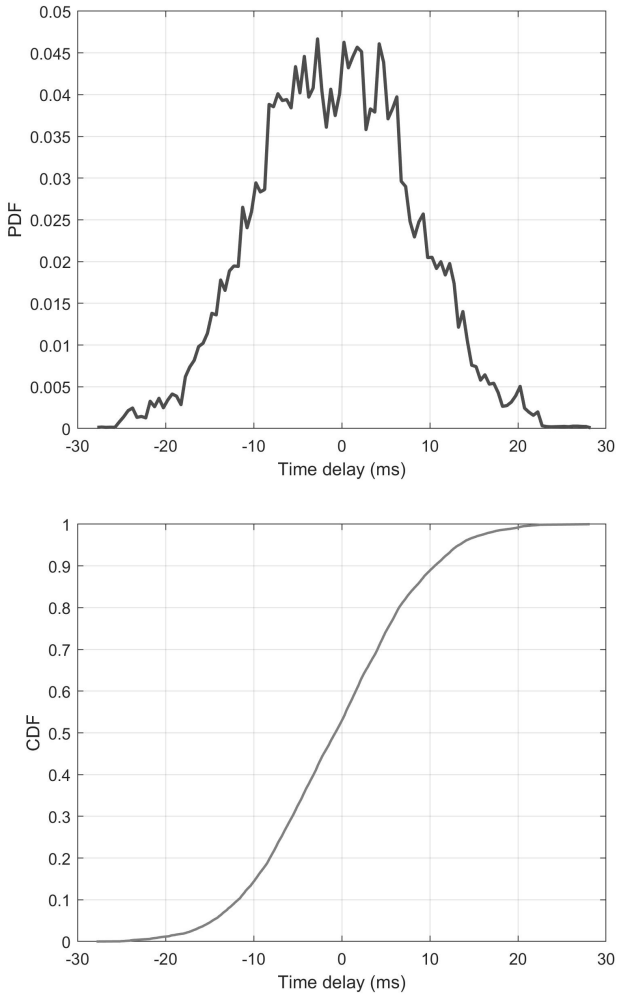


Figure 4.20: (Upper) Probability density function (pdf) of the time delay difference between satellites, with respect a reference one, using real satellite data. (Lower) Cumulative density function (cdf) corresponding to the upper one.

Density Function (CDF) is shown on the lower side of Figure 4.20, where can be seen that a maximum relative time delay of ±10 ms is observed for 90% of the time (i.e. ±2.5 I/NAV data symbols), or up to ±20 ms for 99% of the time (i.e. ±5 I/NAV data symbols). This observation must be taken into account when designing both the snapshot length and the wake up strategy to be used by the receiver, since the sequences of unpredictable symbols for different satellites may be offset by 5 symbols one from the other. This is a significant amount taking into account that up to 8 unpredictable symbols

are available in each of the four batches of unpredictable symbols that are conveyed per odd page, as shown in green color in Figure 4.1.

4.9.2 Clock offset affecting the wake up time

Another factor that may affect the detection performance is the presence of a receiver clock offset that translates into an offset on the time at which the receiver wakes up for gathering a snapshot of signal. As a result of such wake up time offset, some unpredictable symbols may be lost in the gathered snapshot, particularly when the length of the latter is short. It is worth mentioning that two sources of time are assumed to be available. The first one is provided by the local clock of the receiver, whose offset can be determined when solving the user's position and time using the received GNSS signal samples from previous snapshots. However, the error on the estimated clock offset is typically on the order of a few tens of ms when coarse-time navigation is adopted [77], as done in snapshot receivers to solve the user's position and time when no access to the transmission time of the received is available. Apart from the local clock, the snapshot receiver has access to the external time reference provided by the communication network over which the receiver is connected to the remote server. Such external time reference is often provided through Network Time Protocol (NTP) and can be used as well as an additional countermeasure to combat spoofing replay attacks. In particular, by making sure that the GNSS time estimated by the receiver lies within a certain admissible window. This feature is not fully addressed in the present work, since instead, the external time reference is used to determine the wake up time of the receiver that triggers the snapshot recording. As such, an offset of a few tens of ms is to be expected due to the inaccuracies of the NTP, which may translate into a loss of gathered unpredictable symbols, as discussed next. The results in Figure 4.21 show the mean number of unpredictable symbols that are available for each satellite in view as a function of snapshot length and the clock offset on the wake up time.

For the clock offset, three cases are considered, namely when there is no clock offset, when it is ±10ms or when it is ±20ms. Typically, the offset of ±20ms may discards a few of the unpredictable symbols, therefore, finding a sufficient snapshot length is important that can incorporate the maximum number of symbols despite of having offset. Referring to the provided outcomes in a given plot, the snapshot length of 16 symbols would be enough to capture maximum symbols from only visible satellites that distribute OSNMA at that time. As the snapshot length increases, the clock offset can also be compensated gradually without being affected the performance. Hence, a

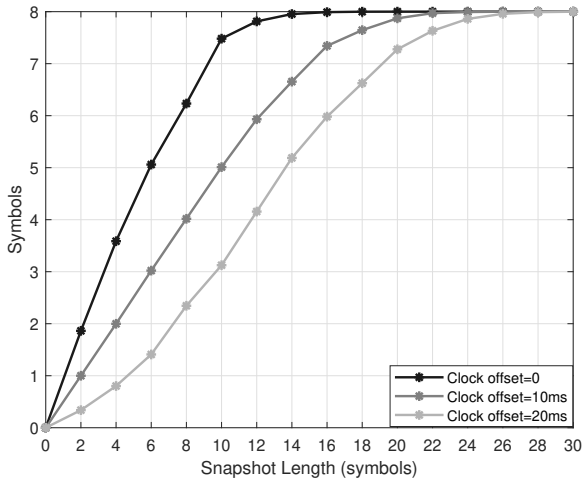


Figure 4.21: Mean number of unpredictable symbols for each satellite in view as a function of snapshot length .

receiver can be designed by taking these analytical outcomes of symbols and snapshot length plot into account to accomplish the performance according to the power consumption of device.

Conclusion

This chapter has provided an insightful analysis of the proposed snapshot OSNMA technique for spoofing detection, which relies on the use of the unpredictable symbols provided in the I/NAV message of Galileo E1-B signal. Being a symbol-level detection technique, concerns are raised on whether this approach is actually usable considering that additional symbol errors are often experienced due to many othersources of errors such as the presence of noise, the overlap between relative phased-shifted authentic and spoofed signals, the presence of multipath, estimation errors and signal fading conditions. The feasibility analysis reveals what are the operational regions at which this technique can work, and what its limitations are. Nevertheless, the answer to the hypothesis inversion problem exhibited by severe fading impact the efforts on modifying the statistical properties of detector are made. This is done by introducing multiple thresholds which significantly solved the hypothesis inversion problem and optimized the detection performance further. In addition, practical implementation aspects are also discussed considering whether a sufficient number of unpredictable symbols are provided by the satellites in view, as a function of the snapshot length and the re-

ceiver clock offset. Numerical results have shown that the proposed detector is feasible and that the spoofer can reliably be detected provided that a set of constraints are met and that a trusted external time reference is available.

Chapter 5

Detection Performance Under Time and Symbol Errors

Another aspect to examine the snapshot OSNMA detection performance is in the presence of timing errors that can arise from the factors such as varying propagation time of satellites in view, and the impact of coarse-time navigation, since snapshot OSNMA acquires position and timing information through A-GNSS. This encourages to highlight the challenges associated with determining the accurate synchronization between the symbol sequence received by the user and the sequence available on the server at the given time and position. Interestingly, the problem addressed herein has some similarities with frame synchronization in digital networks. Since the presence of propagation errors, time uncertainty and different propagation times among different satellites have an impact, therefore, it affect the accurate synchronization of two sequences and thereby the detection performance.

The contribution of the present chapter extends the results in the preceding chapters by considering the time uncertainty present on the estimated unpredictable symbols, and by analyzing the impact of symbol errors that naturally may arise at the receiver end due to adverse propagation effects. As for the time uncertainty, it is due to several factors. The first one is the unequal propagation time of the signals being received by the user from different satellites, which introduces a misalignment on the sequences of unpredictable symbols that are actually received, as observed in Figure 5.1. The second problem is that the user's receiver is often not perfectly synchronized with the GNSS time, and this introduces some uncertainty on the exact time at which the received signal is actually gathered by the receiver. On the one hand, this is due to the fact that clocks with modest performance (e.g. TCXO) are typically used in small devices implementing snapshot GNSS positioning. On the other hand, even though the clock offset could be esti-

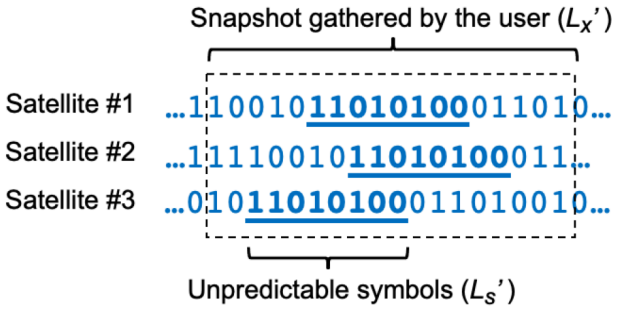


Figure 5.1: Illustration of the symbols received by the user due to the time uncertainty caused by the clock offset and the satellites different propagation times.

mated when solving the user's position, the use of a short snapshot of signal and thus coarse-timing navigation algorithms [66], results in time estimation errors on a few tens of ms [78].

As a result, the receiver must gather a sequence of symbols larger than the one strictly needed, in order to accommodate for such time uncertainty and to make sure that the sequence of unpredictable symbols is always contained within the gathered sequence. The problem to be solved at the server side is to decide whether the expected sequence of unpredictable symbols is contained within the estimated sequence of symbols received by the user. Such decision is based on analyzing the number of symbol errors that are incurred when comparing both sequences. This will ultimately determine whether the received signal is considered to be spoofed or not. As can be seen, this problem shares some similarities with that of unique word detection or frame synchronization in digital communications. Note however that while many contributions on frame synchronization do exist in the current literature, such as [79], [80] or [81], they are mostly based on the additive white Gaussian noise channel. The problem here is a different one because it is based instead on the estimated symbols, that is, the hard-decisions provided by the user's receiver. It is for this reason that the problem needs to be formulated instead as a Binary Symmetric Channel (BSC), for which the work in [82] provides some initial guidelines.

Recalling from the initial chapter, unpredictable symbols appear in the form of four batches of consecutive symbols, as discussed in [17, 20]. The first three batches contain 9, 8 and 8 unpredictable symbols respectively, and are separated apart by 21, 22 and 22 predictable symbols respectively, thus leading to 30 symbols per batch. Since the symbol period in Galileo E1-B is 4 ms, each of these batches has thus a duration of 120 ms, and

the three of them amount to a total duration of 360 ms. After these three batches, a fourth and last batch of just 7 unpredictable symbols is received, thus completing the total time period of 388 ms, containing a total of 32 unpredictable symbols per odd-page of the I/NAV message.

A snapshot receiver willing to gather these 32 unpredictable symbols per odd-page would need to precisely know the exact time at which the first unpredictable symbol is to be received. Unfortunately, this is difficult to be known in practice due to the presence of several sources of time uncertainty, such as: i) the satellite clock offset, which is typically smaller than 10 ms; ii) the user's receiver clock offset, assumed here to be on the order of 50 ms[1]; and iii) the different propagation times experienced by signals received from different satellites, as observed in Figure 5.1, which typically introduces an additional 20 ms time uncertainty.

All these time uncertainties amount to at least 80 ms (i.e. 20 symbols), which together with the 36 ms to gather the almost 9 unpredictable symbols per batch, leads to a snapshot length of roughly 120 ms, containing 30 symbols in total. This snapshot length is on the order of that typically used by small portable devices operating in snapshot mode and adopted in low-power IoT applications. While this snapshot length is enough for providing a position fix, it may not for detecting potential spoofers that incur in a low probability of error when trying to estimate the unpredictable symbols as seen in defining the boundary conditions. It is for this reason that several snapshots may need to be gathered by the user in order to collect a large enough number of unpredictable symbols to reliably detect the presence of spoofing.

5.1 Signal model

This section extends the signal model explicitly for the symbol synchronization problem being conisdered herein, in the presence of time and symols errors.

[1]For a short-term uncalibrated clock, even though less than 10 ms have been reported for small devices connected to current 4G/LTE networks [83].

5.1.1 Signal model for the sequence of received symbols

Let us stack the sequence of L'_x symbols contained in the n-th gathered snapshot into the $(1 \times L'_x)$ vector $\mathbf{x}_n$ as follows,

$$\mathbf{x}_n = \{[\hat{\mathbf{s}}_n \ \mathbf{d}_n]\}_m \tag{5.1}$$

where $\hat{\mathbf{s}}_n$ is the $(1 \times L'_s)$ sequence containing the unpredictable symbols estimated by the receiver,

$$\hat{\mathbf{s}}_n = [\hat{s}_{1,n}, \hat{s}_{2,n}, \ldots, \hat{s}_{L'_s,n}] \tag{5.2}$$

corresponding to the actual unpredictable symbols, $\mathbf{s}_n = [s_{1,n}, s_{2,n}, \ldots, s_{L'_s,n}]$, with $s_{i,n} = \{0, 1\}$, transmitted by the satellites. Since these symbols are assumed to be all unpredictable, and thus no a-priori information on their value is available [20], it is reasonable to assume that they are all equiprobable and *iid*. In turn, $\mathbf{d}_n$ is the $(1 \times L_u)$ sequence containing the remaining $L_u = L'_x - L'_s$ predictable symbols appearing as a result of the aforementioned time uncertainty,

$$\mathbf{d}_n = [d_{1,n}, d_{2,n}, \ldots, d_{L_u,n}]. \tag{5.3}$$

The notation $\{\cdot\}_m$ in (5.1) denotes the circular rotation of a sequence of symbols by m positions. Thus, since the sequence of unpredictable symbols $\mathbf{s}_n$ can appear anywhere within the long sequence $\mathbf{x}_n$, either at the beginning, at the middle or at the end, we have that $m = 0, 1, \ldots, L_u$.

The main objective here is to determine whether the true sequence $\mathbf{s}_n$ is contained within the long sequence $\mathbf{x}_n$. As a by product, this returns as well what the value for m is. It is also important to remark that since (5.2) is a sequence containing estimates (i.e. decisions) on the actual unpredictable symbols, each estimated symbol may incur in some probability of error or symbol error rate (SER),

$$\begin{aligned} P_e \ &= \ p(\hat{s}_{i,n} = 1 | s_{i,n} = 0) p(s_{i,n} = 0) \\ &\quad + p(\hat{s}_{i,n} = 0 | s_{i,n} = 1) p(s_{i,n} = 1) \end{aligned} \tag{5.4}$$

for any i and n. Since the unpredictable symbols are assumed to be iid with equiprobable values, the SER just simplifies to $P_e = \text{prob}(\hat{s}_{i,n} \neq s_{i,n})$. Finally, it worth mentioning that several snapshots may need to be gathered in order to collect a large enough number of unpredictable symbols to reliably

detect a spoofer. Assuming that a total of N snapshots are gathered, they can be stacked into a $(N \times L'_x)$ matrix $\mathbf{X}$ as follows,

$$\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_N \end{bmatrix} = \left\{ \begin{bmatrix} \hat{\mathbf{s}}_1 & \mathbf{d}_1 \\ \hat{\mathbf{s}}_2 & \mathbf{d}_2 \\ & \vdots \\ \hat{\mathbf{s}}_N & \mathbf{d}_N \end{bmatrix} \right\}_m \quad \Rightarrow \quad \mathbf{X} = \left\{ \begin{bmatrix} \hat{\mathbf{S}} & \mathbf{D} \end{bmatrix} \right\}_m \tag{5.5}$$

5.1.2 Symbol error rate for typical working scenarios

Recalling the SER for different working condition as considered in the previous chapters to analyze the performance. In a brief manner, the SER contribution is recalled as:

`In the absence of spoofer`: It is given by the nominal SER incurred by the user's receiver when estimating the symbols received from the authentic satellites. For perfect clear sky outdoor conditions, the channel can be modeled as an AWGN one with typical carrier-to-noise spectral density ratios, C/N_0, on the order of $40 - 45$ dBHz. In that case, the SER turns out to be negligible due to the relatively long symbol period, i.e. $T = 4$ ms, of Galileo E1-B. However, one may consider a pessimistic case with $C/N_0 \sim 30$ dBHz, which then results in $P_{e,0} = \frac{1}{2}\text{erfc}(T \cdot C/N_0) \sim 0.001$. In urban environments the situation significantly worsens due to the presence of multipath reflections. Assuming satellites at medium elevation angles such as $60°$, $P_{e,0} \sim 0.01$ as shown in previous chapter using the LMS channel. Assuming satellites at lower elevation angles such as $40°$, the SER then further worsens up to $P_{e,0} \sim 0.1$ instead as seen in previous chapter.

`In the presence of spoofer`: The spoofed and the authentic signals are received simultaneously at the user receiver and as illustrated in previous chapter that both signals were perfectly aligned in time and frequency, they could hardly ever be aligned in phase. This involves that the phase misaligned superposition of both the spoofed and authentic signals likely results in a SER as shown in Figure 4.5. While the other three different cases are considered same as before i.e. i) a spoofer randomly guessing the unpredictable symbols and thus leading to $P_{e,1} = 0.5$; ii) a pessimistic case with $P_{e,1} = 0.01$, thus being difficult to detect; and iii) an optimistic one with $P_{e,1} = 0.1$, being easier to detect as far as the difference with respect to $P_{e,0}$ is large enough to make both hypotheses distinguishable.

5.2 Proposed snapshot spoofing detection

5.2.1 Detector Formulation

The proposed spoofing detector is inspired by the problem of detecting a short sequence of binary symbols within a longer one, a task frequently encountered in frame synchronization for digital communications. One of the most widely adopted detectors is the BSC frame synchronization algorithm in [82]. This algorithm is based on computing the Hamming distance between the short sequence of interest and portions of the same length from the time-shifted longer sequence. The pseudo-code implementation of such detector adapted to the problem at hand would be as follows,

1 BSC frame detection and synchronization

1: $\mu \leftarrow 0$
2: **if** $\sum_{n=1}^{N} H(\mathbf{s}_n, \mathbf{x}_n; \mu) \leq \gamma$ **then**
3: $\quad$ $\mathbf{S}$ contained in the columns of $\mathbf{X}$,
4: $\quad$ $\hat{m} \leftarrow \mu$.
5: **else**
6: $\quad$ $\mu \leftarrow \mu + 1$
7: $\quad$ **if** $\mu < L_u$ **then**
8: $\quad\quad$ Jump to line 2.
9: $\quad$ **end if**
10: **end if**

where γ is a predefined detection threshold and $H(\mathbf{s}_n, \mathbf{x}_n; \mu)$ stands for the Hamming distance between $\mathbf{s}_n$ and $\mathbf{x}_n$ when the latter is time-shifted by μ positions. That is,

$$H(\mathbf{s}_n, \mathbf{x}_n; \mu) = \sum_{i=1}^{L'_s} s_{i,n} \oplus x_{i+\mu,n} \tag{5.6}$$

with $\oplus$ the XOR operator. Since the latter provides an output equal to 1 when the elements being compared are different, the result in (5.6) is actually providing the number of errors between both sequences, in line with the concept of Hamming distance. The threshold γ is therefore the maximum number of errors that are allowed to occur when comparing $\mathbf{s}_n$ and $\mathbf{x}_n$ for $n = 1, \ldots, N$.

Note that when the received sequence is affected by binary errors occurring with probability P_e, the average number of errors asymptotically tends to NP_e in virtue of the law of large numbers. This value can then be used

as a reference for detecting the presence of spoofers by comparing the actual number of errors with the expected one. In other words, by comparing the measured P_e with the expected one.

Based on these observations, and for the problem at hand, let us formulate the two hypotheses under analysis as follows,

$$\begin{array}{lcll} \mathcal{H}_0 & : & P_e = P_{e,0} & \Rightarrow \quad \mathbf{S} \subset \mathbf{X}, \\ \mathcal{H}_1 & : & P_e = P_{e,1} \neq P_{e,0} & \Rightarrow \quad \mathbf{S} \not\subset \mathbf{X}. \end{array} \tag{5.7}$$

Under $\mathcal{H}_0$ we would allow both sequences to have up to $NP_{e,0}$ different symbols to account for errors normally occurring in the symbols reception at the user's terminal (e.g. thermal noise, shadowing, etc.). If more errors than expected are incurred, then $\mathbf{S} \not\subset \mathbf{X}$ would be declared and this would be an indication that a spoofing attack is potentially taking place.

The detection problem under analysis is therefore formulated using the following detector,

$$T(\mathbf{S}, \mathbf{X}) = \min_{0 \leq \mu \leq L_u} \sum_{n=0}^{N} H(\mathbf{s}_n, \mathbf{x}_n; \mu) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \gamma. \tag{5.8}$$

The starting position of $\mathbf{s}_n$ within $\mathbf{x}_n$, which is assumed constant across n, can be understood as the short sequence alignment within the long sequence. It is obtained as a by product of the detector as follows,

$$\hat{m} = \arg \min_{0 \leq \mu \leq L_u} \sum_{n=1}^{N} H(\mathbf{s}_n, \mathbf{x}_n; \mu) \leq \gamma. \tag{5.9}$$

At this point it is important to emphasize that the threshold γ plays an important role in (5.8) for accommodating potential errors that could be incurred at the user side. For a negligible probability of error at the user receiver, one could safely set $\gamma = 0$ because no errors are expected to be incurred by the user. Any arising error should then be due to the spoofer, and thus be detected. In contrast, if some errors were expected to be incurred by the user due to shadowing or fading effects, one could set for instance, $\gamma = 1$, to allow one error to be incurred by the received symbols. For a total of $L_x = 50$ received symbols, for instance, this would mean allowing a SER of $1/50 = 0.02$, which may suffice to accommodate expected errors with $P_{e,0} < 0.02$ and thus allow detecting spoofers with $P_{e,1} > 0.02$. As can be seen, there is a trade off in setting γ because the larger it is, the more inherent errors at the user side can be accommodated (i.e. due to fading or shadowing), thus reducing the probability of false alarm, but at the same time, a larger $P_{e,1}$ is needed by the spoofer for being detected.

5.2.2 Probability of Detection

According to (5.8), the spoofer detection is successful when the spoofer is present and $T(\mathbf{S};\mathbf{X}) > \gamma$. The probability of detection can thus be mathematically formulated as follows,

$$\begin{aligned} P_{\mathrm{d}} &= p\left(T(\mathbf{S},\mathbf{X}) > \gamma | \mathcal{H}_1\right) && (5.10)\\ &= \prod_{0\le\mu\le L_u} p\left(\sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\mu) > \gamma | \mathcal{H}_1\right) && (5.11)\\ &= \prod_{0\le\mu\le L_u} \left(1 - p\left(\sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\mu) \le \gamma | \mathcal{H}_1\right)\right). && (5.12) \end{aligned}$$

Note that the step from (5.10) to (5.11) is done in virtue of the fact that $p(\min_\alpha U(\alpha) \le \gamma)$ for some positive semi-definite function $U(\cdot)$ and $\alpha = \{0,1,\ldots,M-1\}$, can be expressed as the joint probability $p(U(0) \le \gamma, U(1) \le \gamma, \ldots, U(M-1) \le \gamma)$. Furthermore, the set of values $U(\alpha) \doteq \sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\alpha)$ for $\alpha = \{0,1,\ldots,M-1\}$ can be assumed to be independent one from each other due to the unpredictability (i.e. uncorrelatedness) of the underlying symbols in $\mathbf{s}_n$ and $\mathbf{x}_n$.

At this point, two regions are considered for $p\left(\sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\mu) \le \gamma | \mathcal{H}_1\right)$ in (5.12) as a function of μ:

1. The first region corresponds to $\mu = m$, when the correct time-shift is applied in (5.6) so that the expected unpredictable symbols are aligned with those actually received by the user. The probability are being looked for is then given by,

$$\begin{aligned} P_1(L_s,\gamma,P_{e,1}) &\doteq p\left(\sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\mu=m) \le \gamma | \mathcal{H}_1\right)\\ &= \sum_{k=0}^{\gamma} \binom{L_s}{k} (1-P_{e,1})^{L_s-k} P_{e,1}^{k} && (5.13) \end{aligned}$$

2. The second region comprises the values $\mu \neq m$, when the expected and received unpredictable symbols are misaligned. Since we are dealing with sequences of unpredictable symbols, it is reasonable to assume that a sequence and its time-shifted version will be uncorrelated. As such, the errors γ that are sought in (5.12) are just the errors arising when comparing two independent sequences of random symbols. As

such, we can define

$$P_2(L_s,\gamma) \doteq p\left(\sum_{n=1}^{N} H(\mathbf{s}_n,\mathbf{x}_n;\mu\neq m)\leq\gamma|\mathcal{H}_1\right) = \frac{1}{2^{L_s}}\sum_{k=0}^{\gamma}\binom{L_s}{k} \tag{5.14}$$

Merging both results together, the probability of success in detecting the sequence of unpredictable symbols becomes,

$$P_{\mathrm{d}}(L_s,L_u,\gamma,P_{e,1}) = \big(1-P_1(L_s,\gamma,P_{e,1})\big)\big(1-P_2(L_s,\gamma)\big)^{L_u}. \tag{5.15}$$

5.2.3 Probability of False Alarm

Apart from the probability of success, it is of interest to determine the probability of false alarm that the proposed detector may incur. Such probability is defined as that of incurring in more than γ errors when comparing both the expected and the received unpredictable symbols, when actually no spoofer is present. That is

$$P_{\mathrm{fa}} = p\left(T(\mathbf{S},\mathbf{X})>\gamma|\mathcal{H}_0\right) \tag{5.16}$$

which is computed in the same manner as the probability of detection except for the fact that $P_{e,1}$ is now replaced by $P_{e,0}$. The result is given by

$$P_{\mathrm{fa}}(L_s,L_u,\gamma,P_{e,0}) = \big(1-P_1(L_s,\gamma,P_{e,0})\big)\big(1-P_2(L_s,\gamma)\big)^{L_u}. \tag{5.17}$$

5.3 Simulation Results

The goal of this section is two-fold. On the one hand, to assess the goodness of the theoretical expressions derived in subsections 5.2.2 and 5.2.3. On the other hand, once these expression are validated, to analyze the performance of the proposed detector in Section 5.2.1.

5.3.1 Goodness of the Theoretical Expressions for P_{d} and P_{fa}

The first step in the simulation results is to confirm the validity of the theoretical expressions for P_{d} and P_{fa} presented in (5.15) and (5.17), respectively. This is important in order to ensure that the underlying assumptions and

subsequent conclusions are consistent with the real behavior of the proposed technique. The way to proceed is by comparing the results provided by the theoretical expressions with those obtained empirically. The latter are obtained by generating random sequences of unpredictable symbols, introducing random errors on their reception, and adding random symbols before and after this sequence to emulate the effect of time uncertainty.

The results are depicted in Figure 5.2 for P_{d} and P_{fa}. Without loss of generality, and example is shown for the case of $P_{e,1} = 0.1$ and $P_{e,0} = 0.001$, respectively. A time uncertainty of 20 symbols is considered as defined in previous section and a threshold $\gamma = \{0, 1\}$. The results show that both theoretical and empirical curves closely match one with each other, thus validating the goodness of theoretical expressions. As can be seen, P_{d} increases with the length of the sequence of unpredictable symbols. This is because for a fixed $P_{e,1}$, the longer such sequence, the more errors will be encountered, and the easier will be to detect the spoofer. Increasing the threshold γ provides more tolerance to errors and dramatically reduces P_{fa}, as observed in the right hand side plot of Figure 5.2. This may be needed in cases when the user receiver is subject to shadowing or fading, and thus it is prone to non-spoofing errors that need to be accommodated in order not to be confused with spoofing ones. The price to be paid is a reduction as well on P_{d}. The tradeoff betwen P_{d} and P_{fa} will be assessed later on in subsection 5.3.3.

Another aspect to be highlighted is the influence of the time uncertainty onto the detection performance. Interestingly, the impact is only noticeable when the number of unpredictable symbols, L_s, is comparable to the number of symbols introduced by the time uncertainty, L_u. The reason is that the detector in (5.8) relies on taking the minimum of the Hamming distances among all tentative time shifts μ. This will tend to identify the time shift at which the unpredictable symbols are located, $\mu = m$, because it is at this position where the least number of errors will likely be observed. Falling outside of this region, namely selecting $\mu \neq m$, and therefore being misled by the presence of time uncertainty, becomes more unlikely as L_s grows. This is because the larger L_s, the more difficult it is to find a sequence of random symbols that might incur in less errors than the received sequence of unpredictable symbols. Actually, it can be seen in (5.14) that for a fixed and finite threshold (e.g. $\gamma = \{0, 1\}$ as in Figure 5.2), P_2 rapidly goes to 0 as L_s grows, and then P_{d} does not depend on L_u anymore. This effect can be observed in Figure 5.2 for $L_s > 10$ with $\gamma = 0$ and $L_s > 15$ with $\gamma = 1$, thus suggesting that time uncertainty does note have a relevant impact provided that $L_s > L_u$.

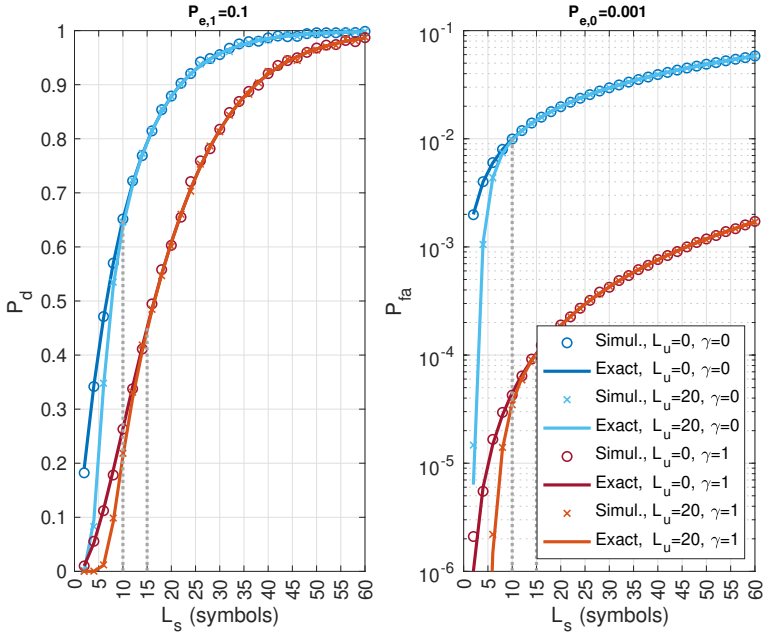


Figure 5.2: Comparison between the empirical and theoretical P_{d} for $P_{e,1} = 0.1$ (left), as well as P_{fa} for $P_{e,0} = 0.001$ (right), as a function of the unpredictable symbols L_s, using $\gamma = \{0, 1\}$.

5.3.2 Probability of Detection as a Function of P_{e}

Once the theoretical expressions have been validated, it is of interest to analyze the impact of the spoofer probability of error $P_{\mathrm{e},1}$ onto the spoofer detection. This is shown in Figure 5.3 for a wide range of lengths L_s of the unpredictable symbols sequence. For illustration purposes, the detection threshold is set to $\gamma = 0$ and $L_u = 20$ symbols introduced by the time uncertainty are considered.

As expected, P_{d} increases as $P_{e,1}$ does so, since the latter is ultimately unveiling the presence of the spoofer. Conversely, as $P_{e,1}$ decreases, it becomes more difficult to detect the spoofer and the only way to counteract this situation is by increasing the length of the unpredictable symbols sequence. Indeed, it can be observed that roughly $L_s \sim 2/P_{e,1}$ symbols are needed in order to ensure that the spoofer is detected with a high enough probability of detection. This makes challenging to detect spoofers with a low probability of error, since many unpredictable symbols will be needed, thus incurring in a high time to spoofing detection since only ~ 30 unpredictable symbols are available every 2 seconds of the I/NAV message.

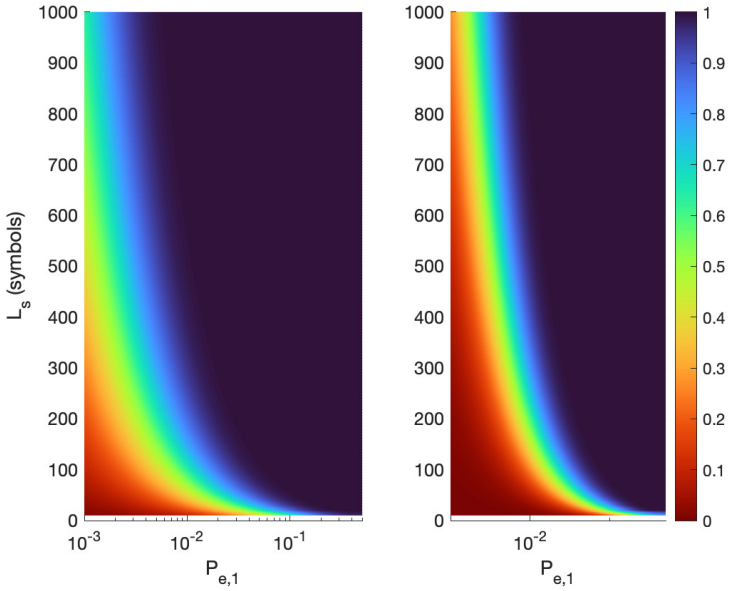


Figure 5.3: Probability of detection as a function of the probability of symbol error, $P_{e,1}$, for $L_u = 20$ symbols with $\gamma = 0$ (left) and $\gamma = 1$ (right).

5.3.3 Probability of Detection vs Probability of False Alarm

The results presented so far consider either the probability of detection or the probability of false alarm. In practice, though, both must be assessed simultaneously in order to determine what the price is (i.e. false alarms) for achieving the largest possible probability of detection. To this end, the ROC curve is a useful tool that represents the probability of detection as a function of probability of false alarm. Unfortunately, the proposed detector is strongly influenced by many parameters such as L_s, $P_{e,0}$ and $P_{e,1}$, thus making the ROC curve to be multi-dimensional and therefore, difficult to be analyzed.

In these circumstances it is often preferred to summarize the information content of the ROC curve into a lower dimensional metric. for instance AUC as presented in previous chapters. Another metric is the Youden index [84], which measures the vertical distance from a point of the ROC curve down to the diagonal line corresponding to the ROC of a random detector. As such, the Youden index is a threshold-dependent metric and consequently, it is well-suited for analyzing the detection performance of the proposed detector, whose detection threshold γ is playing a central role.

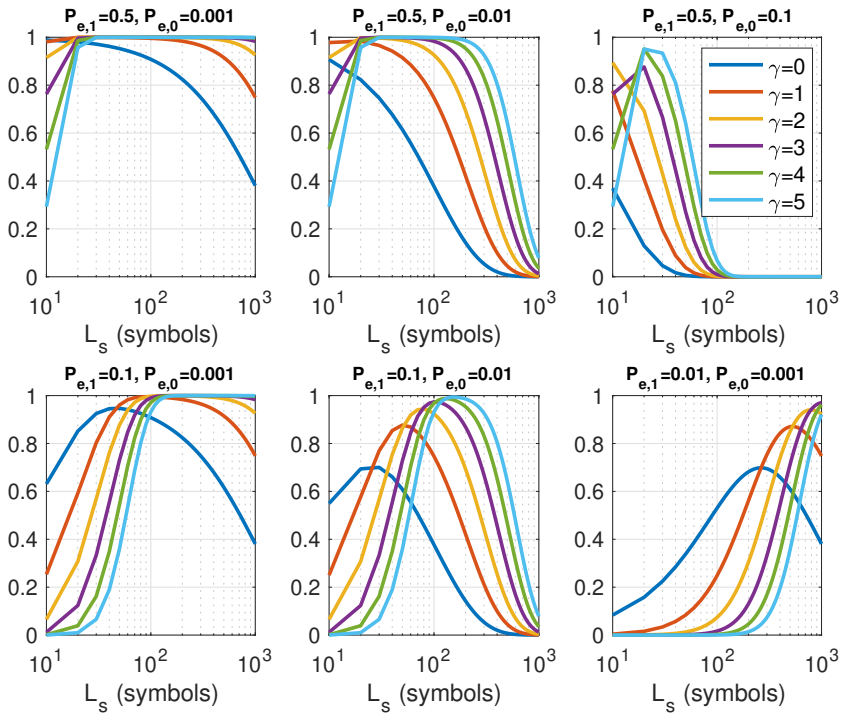


Figure 5.4: Youden index for the proposed detector in various working conditions for $P_{e,0} = \{0.001, 0.01, 0.1\}$, $P_{e,1} = \{0.5, 0.1, 0.01\}$, and time uncertainty of $L_u = 20$ symbols.

The Youden index for the detector in (5.8) is shown in Figure 5.4 for different pairs of $P_{e,1}$ and $P_{e,0}$, as well as for different detection thresholds γ. The Youden index ranges from 0, which means the worst possible performance (i.e. $P_{\mathrm{d}} = P_{\mathrm{fa}}$), up to 1, which means the best possible performance (i.e. $P_{\mathrm{d}} = 1$ and $P_{\mathrm{fa}} = 0$). It is interesting to observe that the more different $P_{e,1}$ and $P_{e,0}$ are, the easier it is to achieve the best detection performance. This can be seen in the upper left hand side subplot of Figure 5.4 for $P_{e,1} = 0.5$ and $P_{e,0} = 0.001$. In contrast, the more similar $P_{e,1}$ and $P_{e,0}$ are, the more difficult it is to succeed in detecting the spoofer. This can be seen in the upper right hand side subplot of Figure 5.4 for $P_{e,1} = 0.5$ and $P_{e,0} = 0.1$, where the Youden index struggles to reach its maximum value equal to one.

For the rest of intermediate combinations of $P_{e,1}$ and $P_{e,0}$, the detection threshold γ can be adjusted to provide the maximum Youden index. As a result, the optimal required number of unpredictable symbols can be obtained. For instance, in the bottom middle subplot of Figure 5.4 for $P_{e,1} = 0.1$ and $P_{e,0} = 0.01$, the smallest threshold achieving the maximum Youden index is $\gamma = 5$, thus confirming that optimal detection is possible for this working

scenario. To do so, the required number of unpredictable symbols amounts to 150, thus providing a valuable guideline to properly configure the detection technique for a given working scenario.

5.4 Conclusions

This chapter has extensively analyzed the spoofing detection performance of the snapshot OSNMA concept in the presence of time uncertainities. It is already envisaged by comparing both the received and expected sequences of unpredictable symbols, an abnormal number of symbol errors becomes an indication that the received sequence is likely to have been spoofed. This problem, though, is subject in practice to synchronization errors due to the misalignment between the time at which the user started to collect the received symbols, and the time at which unpredictable symbols actually arrive at the receiver after being transmitted by the Galileo satellites.

A detector to deal with such problem has been proposed in the chapter along with the mathematical characterization of its probability of detection and probability of false alarm. Special emphasis has been placed on characterizing the detection performance as a function of the unpredictable symbols length, L_s, time uncertainty L_u and probability of error in the presence, $P_{e,1}$, and in the absence of spoofer, $P_{e,0}$. The results provide insights that help in better understanding the advantages and limitations of OSNMA symbol-level spoofing detection.

Chapter 6

Experimental Analysis of Snapshot OSNMA

Till now , the performance has been analyzed in different aspects taking into account the derived theoretical relations. Henceforth, this chapter focuses on validating the developed snapshot OSNMA software and the theoretical relations at symbol level formulated in previous chapters. This is achieved through the utilization of real Galileo E1-B signal generated by the RF GNSS simulator available at the SPCOMNAV group.

6.1 Experimental Processing

The overall process involves, at first, the generation of authentic signal and the symbol-level spoofed signal at the same position and time through the experimental setup. Afterwards, the signals transfer to an open source software receiver to perform the signal acquisition and the decoding of predictable and unpredictable symbols explicitly from those satellites signals that receiver found during the acquisition stage. The forthcoming step comprises of authentication of the received symbols using snapshot OSNMA software working at the server side. It compares these received symbols with the unpredictable symbols that are present at the server side at the same position and time. As an ultimate step, the spoofing detector emerges with a binary output i.e. snapshot is "Spoofed" or " Not Spoofed". As can be seen that each step herein is performed with an individual source and the overall system is designed in such a way that the output from one source integrates as an input to the other source. In this essence, the overall system design is illustrated in Figure 6.1

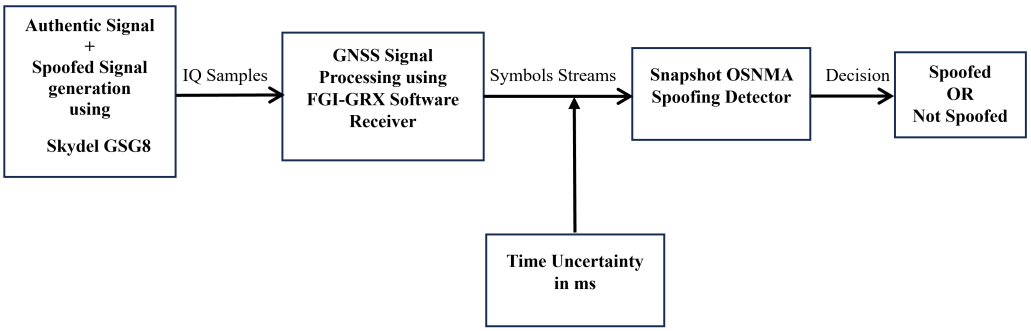


Figure 6.1: The experimental scheme for spoofing detection system incorporating Snapshot OSNMA capabilities.

6.1.1 Signal Generation:

The initial stage depicted in Figure 6.1 involves about the generation of authentic signal and its corresponding spoofed signal at symbol level. This can be done by utilizing the GNSS simulator i.e., Orolia Skydel GSG 8, as shown in Figure 6.2. This simulator ensures a realistic testing platform by employing GPU accelerated computing to generate GNSS signals in real time. Supporting its operational flexibility, it can be configured with various hardware setups and operating systems. In terms of simulation, Skydel simulation engine has capability to generate digital signals in the form of IQ (In phase, Quadrature) data in "Int 16" format. This IQ data is useful for various purposes, for instance, it can be recorded and subsequently playable for offline processing and also compatible to add with multiple other IQ files. Additionally, it provides the opportunity to be utilized as spoofed signal along with jamming transmitter. For further details about the working of Skydel, can be found in the user manual [22].



Figure 6.2: Skydel GSG-8 Advanced GNSS Simulator [22]

In the context of received signals at the user receiver, two Galileo E1B signals are generated together with the Skydel built-in settings, one signal corresponds to the "authentic signal" while the other one refers to "spoofed signal". Both are aggregated at the generation stage since it is what typically received at the receiver end when there is a spoofing attack.

6.1.1.1 Authentic Signal

The generation mechanism of authentic Galileo E1-B signals using Skydel is shown in Figure 6.3. The authentic Galileo E1 signal comprises of 8 satellites in view are simulated with carrier frequency of 1575.42 MHz and sampling rate of 25 Megasamples per seconds (MSps). Each satellite is being transmitted with different power thereby reach at user receiver with different C/N_0 ratios. The SV IDs closer to the midpoint of the constellation shown at the lower right corner of Figure 6.3 receive at comparatively high power than the ones away from central circle. However, the power and thereby C/N_0 is user controllable for each satellite in view at the given time.

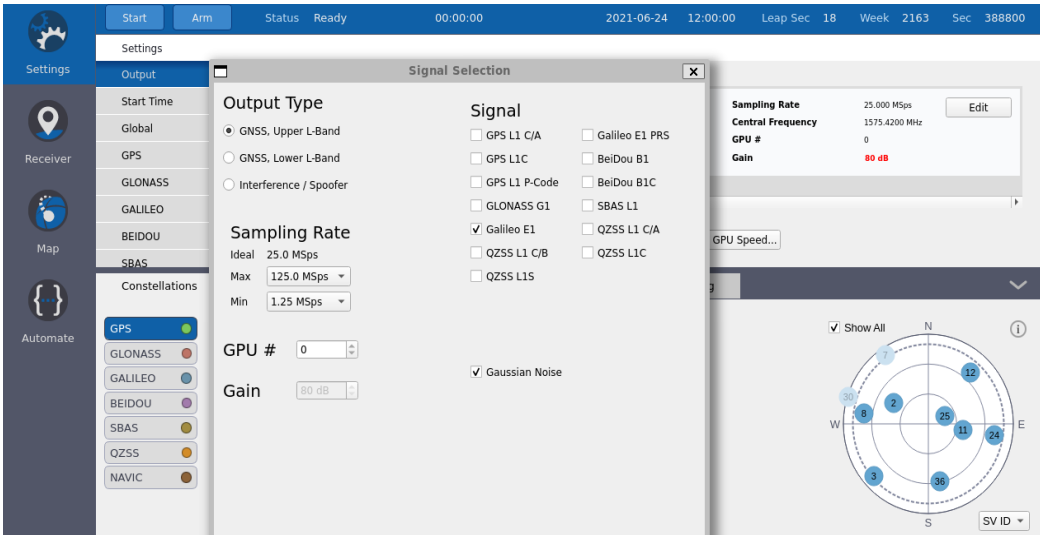


Figure 6.3: Illustration of Skydel generating Galileo E1 authentic signal

6.1.1.2 Spoofed Signal

The spoofed signal is generated using the "Multipath" function of Skydel since it allows adding two signals (line of sight (LOS) and the multipath ray/echo) together at the output. If LOS signal is regarded as an authentic signal and the multipath ray/echo as a spoofed signal, both can be added

constructively and destructively depending on carrier phase. This possibility is being provided in Skydel in multipath module and this is what the victim receiver will receive in the presence of spoofing i.e. the aggregation of the spoofed and the authentic signal. Note that a multipath echo is generated with the same properties as the LOS but with the inclusion of spoofing properties at symbol level. However, the power advantage for user and spoofer can be controllable for both LOS (authentic) and multipath ray (spoofed) signals, respectively. In the context of spoofer's error probability p_s that spoofer incurs during the estimation of unpredictable symbols, the spoofed signal is set to be simulated here with $p_s = 0.1$. That means the presence of 1 unpredictable symbol in error among 10 symbols and consequently around 3 unpredictable symbols will be inverted in 32 unpredictable symbols present in one odd page of I/NAV message to fulfill the condition of $p_s = 0.1$.

Skydel Limitations : Nevertheless, the Skydel simulator does not provide the possibility of directly inverting the symbols but only allows to modify the *bits* of both even and odd pages. Thereby, in our case, unpredictable *bits* will be inverted with the probability of $p_s = 0.1$. It's acknowledged in [20], the bits present in each page are convolutionally encoded and then interleaved and each bit provides 2 symbols at the output during performing the convolution encoding, where one symbol corresponds to the unpredictable and the other symbol refers to the predictable one.

Therefore, if 3 *unpredictable symbols* to be inverted due to spoofer, it's required to have 3 bits inverted since each bit gives 2 symbols, 1 *unpredictable* and 1 predictable. As our interest is in *unpredictable* ones, hence, 3 bits in error are required to invert 3 *unpredictable symbols*. This is done by using the "Navigation Message Modification (NMM)" function of I/NAV message, as the window shows in Figure 6.4

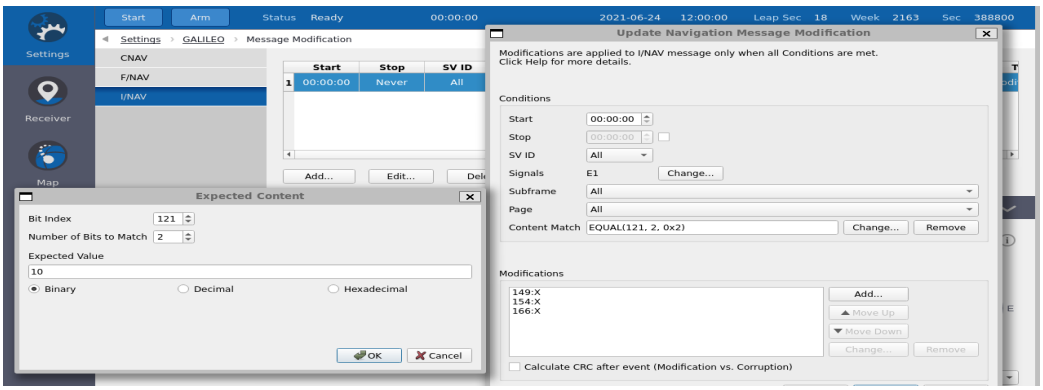


Figure 6.4: Illustration of Skydel modifying unpredictable bits in I/NAV message using NMM function

As can be seen, Figure 6.4 comprises of 2 sub-windows i.e. Update Navigation Message Modification (UNMM) and Expected Content (EC). UNMM is responsible of selecting the satellite ID, signal, sub-frames, and pages that could be modified by users and also depicts the modifications have been applied while EC shows the condition that should meet in order to successfully apply these modification. For instance, Bit Index (BI) in EC is set to 121 and the condition is set if the values of two bits i.e. 121 and 122 bits are 1 and 0 respectively, the modification will be applied. The reason of choosing BI equals to 121 is because Skydel starts the simulation with even page and both even and odd page contains 120 bits each as shown in Figure 4.1. Once the even page is passed, the odd page will start from 121st bit. The first bit of odd page is always "1" and the next bit value "0" represents the nominal page as the unpredictable bits are only available in nominal pages. It means, if the 121st and 122nd bits are 1 and 0 respectively, this would be a nominal odd page that contains the OSNMA unpredictable bits. Once the condition is met, the modifications are configured in UMMM sub-window will be applied i.e. 149th, 154th and 166th bit will be inverted as X in UNMM represents the inversion operation, i.e. invert the sign of symbol). In other words, 29th, 34th and 46th bit of the odd page will be in errors as compared to authentic symbols. These specific bits are choosen as these are a part of 40 bits "Reserved 1" field where OSNMA capabilities are configured and thereby belongs to unpredictable bits as depicted in Figure 4.1 (a). These 3 bits in error are noticeable in Figure 6.5, which is acquired by taking the amplitude difference of authentic and modified bits of odd page and the black window represents the "Reserved 1" field window.

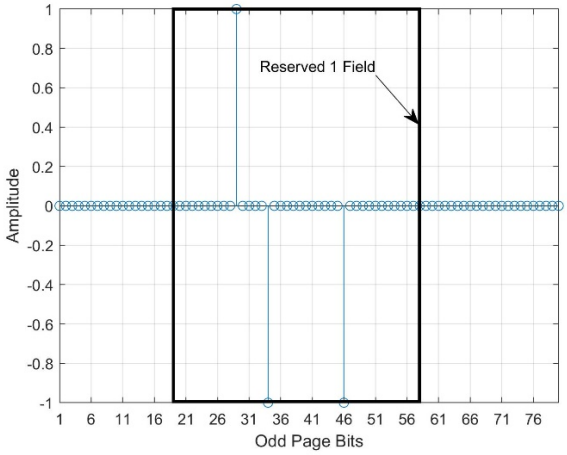


Figure 6.5: Erroneous Unpredictable bits using Skydel

Additional Errors: Based on the I/NAV message configuration, these 3 bits in error should produce 3 *unpredictable symbols* in errors as discussed above. However, during processing the signal, it is revealed about the presence of additional symbol errors due to convolutional encoding as it consists of memory registers and hence the bit in error would impact the bits coming in series during encoding operation. As Skydel provides the opportunity to modify only *bits* and the encoding and interleaving will be performed afterwards. Therefore, once bits are modified and then signal is generated and processed to decode the symbols at user receiver, the extracted sequence experiences some additional symbols errors other than the ones that are simulated by UMMM leading the $p_s \approx 0.3$ i.e. 10 to 11 errors in 32 unpredictable symbols. The unpredictable symbol errors corresponds to those 3 bits depicted above, and the additional errors caused by encoder are highlighted in Figure 6.6.



Figure 6.6: The symbol error analysis before and after interleaving to see the impact of additional symbol errors

After revealing about the system constraints regarding additional errors, the spoofed Galileo E1B signal scenario is regenerated but now imposing

only 1 bit in error since 1 bit provides around 3 unpredictable symbol errors encompassing the symbol errors incurred by encoder as well, as illustrated in Figure 6.6. This gives now 3 errors out of 32 unpredictable symbols leading to $p_s = 0.1$.

Following the system constraints discussion, at the signal generation side, the following signal scenarios are recorded to analyze the spoofing detection at symbol level in the scope of experimental analysis.

- A spoofing scenario with the aggregation of authentic and spoofed signals added destructively (the relative phase difference $\Delta\phi = \pi$ to validate results in Figure 4.5).
- The simulation of spoofed signal with probability of spoofer $p_s = 0.1$ as illustrated above.
- It is considered that spoofer has 5 dB advantage over user which is a reasonable assumption in order to take over the user receiver.

Once the scenarios with aforementioned properties are defined, the authentic and spoofed signals are then recorded for each scenario in the form of IQ files. These IQ files later serve as input to the open source FGI-GRX GNSS software receiver for processing and finally extracting the symbols from each odd page.

6.1.2 IQ Files Processing with FGI-GRX Software Receiver:

Given the IQ files by Skydel, the environment is set up to process these files in MATLAB based FGI-GRX GNSS receiver. FGI-GRX is an open-source software receiver comprises of different modules and has capabilities to process GNSS signals from multiple constellations, including GPS, Galileo, BeiDou, GLONASS, and NavIC. These software modules provide the opportunity to perform GNSS acquisition, code and carrier tracking, decoding the navigation message, pseudo-range estimation and finally PVT solution.

Given that the snapshot OSNMA works on symbol level, the "navigation message decoding" module of FGI-GRX software can process and assist in the extraction of decoded symbols from Galileo E1B signal generated by Skydel [85]. The overall parameters setup and data properties to record through Skydel and process those E1 B signal IQ files with FGI-GRX software in this work is summarized in the Table 6.1.

Once the parameters are configured in FGI-GRX software, the recorded signals by Skydel are now ready to process through the software receiver.

Table 6.1: The overall parameters configuration to process IQ files through FGI-GRX software receiver.

Parameters	**Values**	**Parameters**	**Values**
Sampling Frequency (MHz)	25	Complex Data	Yes
Center Frequency (MHz)	1575.42	Data Type	16
Coherent Integration	1	SNR (dB)	30
Non-Coherent Integration	1	Elevation Mask (degrees)	10

Figure 6.7 gives a snapshot of E1B in-phase and quadrature component in time domain, frequency domain signal and histogram plots recorded by Skydel and processed by the software.

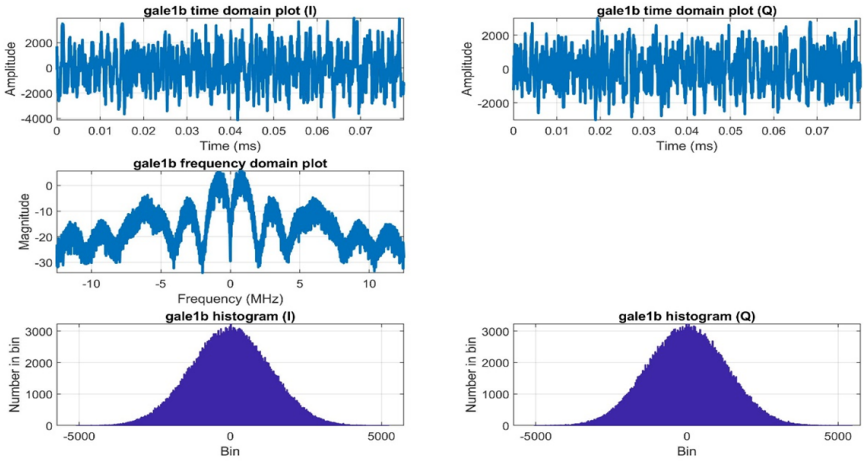
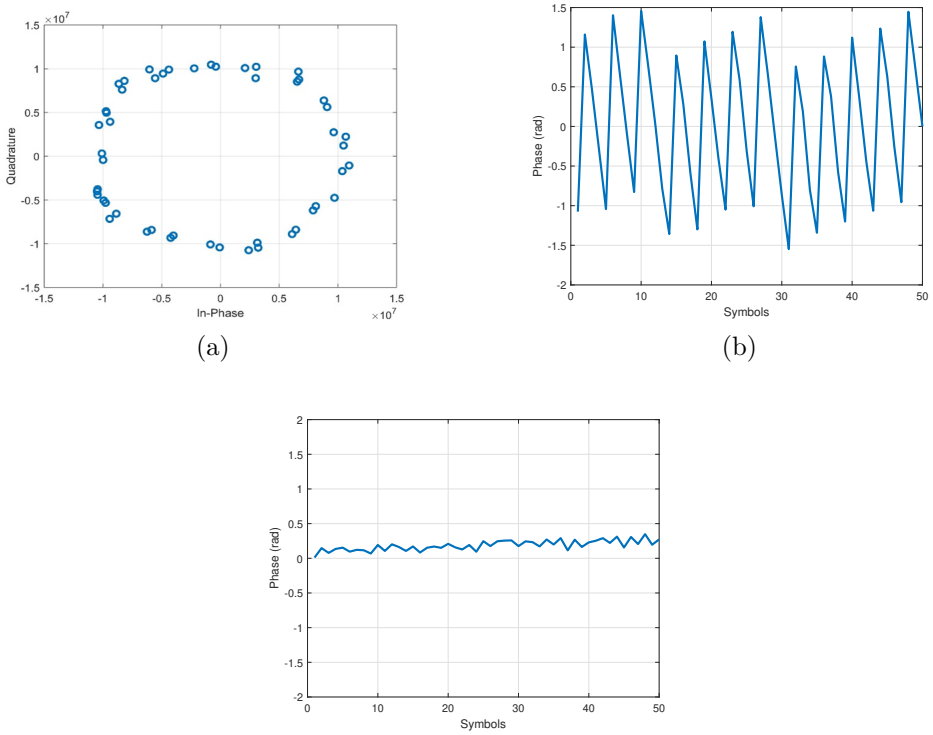


Figure 6.7: A snapshot of Galileo E1B time, frequency domain plots

Hereinafter, the efforts of processing the recorded scenarios and testing the snapshot based spoofing detector are made. In this prespective, the primarily step is the correct extraction of symbols present in odd pages of I/NAV message. But prior to that, this is important to validate the scenario when spoofed and authentic signal aggregated but spoofer could not able to align its carrier phase with the authentic signal. It is one of the prominent

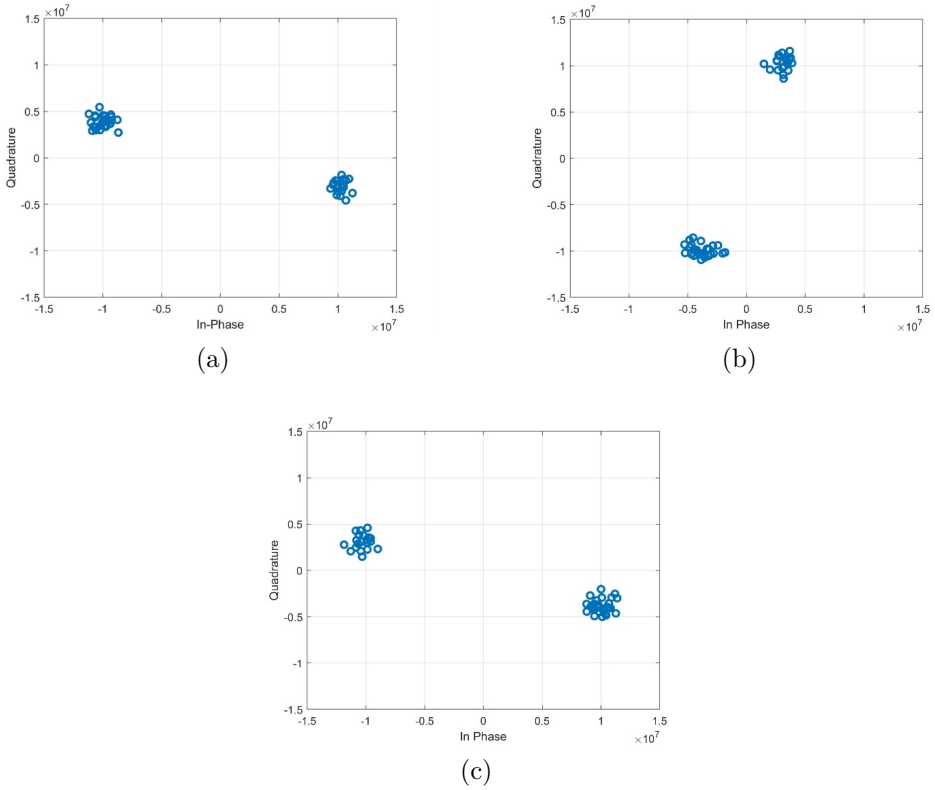


(a) (b) (c)

Figure 6.8: (a) BPSK constellation after acquisition stage affected Doppler and phase discontinuity. (b) The phase discontinuity between the consecutive symbols visible by phase jumps. (c) The phase continuity between the consecutive symbols visible by negligible phase jumps.

impacts caused by the spoofer which leaves a room to detect and is found to be significant in (4.13).

Verification of Relative Phase offset: In the context of relative phase offset, to ensure if the Skydel is correctly applying the phase offset between authentic and spoofed signal, the IQ samples are further processed using software and extract the symbols at the acquisition stage. To do so, the initial step is to acquire the satellite in view by searching the maximum peak in 2D time-Doppler search and then extract the symbols from prompt correlator output. Once the maximum peak is detected during the acquisition stage, the symbols constellation is extracted as in Figure 6.8 (a)for both in-phase and quadrature components. It is to see if the symbols are phase shifted by the same degree as applied in Skydel during recording the signals. However, it is observable that symbols are rotating in a circular region. This is found



(a) (b) (c)

Figure 6.9: The BPSK constellation with Phase continuity, Doppler removed, and Phase offset of (a) 0 degree, (b) 90 degrees and (c) 180 degrees.

that FGI-GRX software does not incorporate the phase continuity between consecutive prompts during the acquisition stage as the jumps seen in Figure 6.8 (b).

Correction to BPSK cosntellation: The additional modifications to the FGI-GRX software are implemented to: i) maintain the phase continuity among symbols; ii) refine the Doppler removal by using an additional Fast Fourier Transform (FFT) to estimate the remaining coarse Doppler error. The problem of phase discontinuity is solved by taking into account the previous phase each time when processing the next piece of signal and the outcomes are depicted in Figure 6.8 (c).

As of now, the phase discontinuity is removed and the further step is to remove the Doppler impcat. This is done by estimating the Doppler and then removed by the following commands in Figure 6.10, where “14 ” and “ 12025” are frequency bin number and code phase respectively, of the appeared maximum peak and “ 0.75” is estimated Doppler. Once these correction are made,

the signals are then tested with different values of relative phase offsets for instance, 0, 90 and 180 degrees and can be verified by examining the in-phase and quadrature BPSK constellation in Figure 6.9.

```
%Doppler Estimation by FFT
fftshift(abs(fft(exp( 1i*angle ( exp ( 1i * pi * (angle(squeeze(tmp(14,1:end,12025)))) / (pi/2) )) / pi ) * (pi/2),128)))
%Doppler Removal
 exp ( 1i * pi * (angle(squeeze(tmp(14,1:end,12025).*exp(1i*0.75*(1:length(tmp(14,:,12025)))))) / (pi/2) ) / pi ) * (pi/2);
```

Figure 6.10: MATLAB commands to estimate and remove the Doppler from prompts.

Overlap of Spoofed and Authentic Signal: Since Figure 6.9 (a), (b) and (c) is an evidence that Skydel is modifying the phase offsets in a correct way. Hence, it is time to simulate a spoofing scenario with both authentic and spoofed signal at use receiver with the exactly same properties except phase offset to validate the relation in (4.13). To do so, an authentic signal with a duration of 9 seconds is started recording at $(C/N_0)_{\mathrm{a,u}} = 45$ dbHz. After passing 3 seconds, a spoofer is introduced with 3dB power advantage over authentic signal but with a relative phase offset of 180 degrees. The spoofer arrives at receiver for 3 seconds and aggregated with authentic signal during this entire time. After passing 6 seconds, the spoofer is removed and only authentic signal is being received for next 3 seconds by software receiver. The impact on C/N_0 metric is shown in Figure 6.11.

It is interesting to analyze also the Figure 4.5 and the corresponding relation (4.13) with C/N_0 *point of view*. As soon as spoofer started to align itself with authentic signal with destructive relative phase offset, the C/N_0 dramatically drops to mean value of 34dB, depicted in Figure 6.11. This actually satisfies the (4.13) when relative phase offset is 180°, $(C/N_0)_{\mathrm{a,u}} = 45$ dBHz and spoofer is having 3dB power advantage. According to the relation (4.13) and the same simulated signal properties, the received power should drop to around 11dB and become 34dB when the signal received at the receiver, as happened in Figure 6.11.

In another POI, recalling the Figure 4.4 of SER due to C/N_0, the SER corresponds to dropped $C/N_0 = 34$dB in this case is coinciding with the SER spoofer scenario defined at $(C/N_0)_{\mathrm{a,u}} = 45$ dBHz in Figure 4.5. Hence, the other prospective to detect the spoofing attack at symbol level is tracking of C/N_0. Note that, to do so, the prior information is required at the server if signal is being received impacted by urban or sub-urban environment.

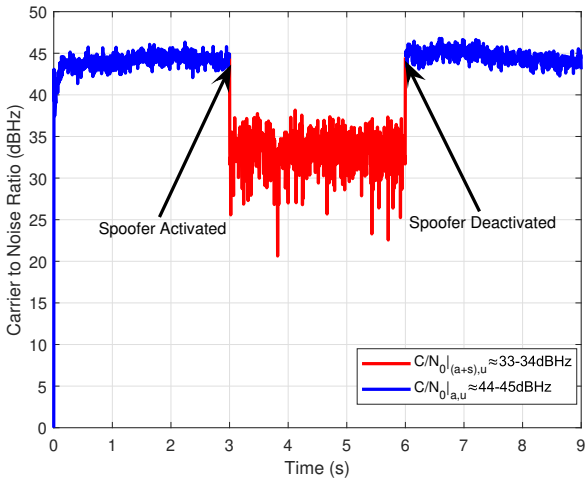


Figure 6.11: The aggregation of authentic and spoofed signal with 3dB power advantage and relative phase offset 180°, where spoofing starts at time = 3 seconds and ends at 6 seconds represented in red.

6.1.3 Snapshot OSNMA Spoofing Detection

This subsection offers insights about the implementation of snapshot OSNMA on the recorded IQ files with scenario when $(C/N_0)_{\text{a,u}} = 45$ dBHz, spoofer error probability $p_s = 0.1$, spoofer with 5dB power advantage and the relative phase offset sets to 0°. Th efforts make here to detect the spoofing attack taking into account the p_s factor since all other impacts will be almost negligible. Two cases are presented herein,

- The scenario corresponds to the time uncertainty of 0ms and the position of unpredictable symbols can be exactly known in this case. Hence, the snapshot receiver could wake up at exactly the time when unpredictable symbols appear.

- The second scenario is about the existence of time uncertainty due to clock offsets primarily as discussed in Chapter 5 and the longer snapshots are needed comprises of predictable and unpredictable symbols so that the snapshots contain all the available unpredictable symbols available to be authenticated.

Without Time Uncertainty: As an initial step after founding the satellites, it is required to detect the position of unpredictable symbols. In reality, the unpredictable symbols are time tagged at the server, so the time at which the unpredictable symbols should appear is already known. And

also, the detector would perform the spoofing detection test as soon as unpredictable symbols are received. However, in the Skydel settings, the entire signal is to be recorded first to process with software receiver. Therefore, the entire symbols extraction is performed at once and later distributed snapshot by snapshot basis. This is done by identifying the odd page first i.e., by using the preamble or synchronization pattern since it is known in advance. In essence, the receiver finds the preamble by correlation the received symbols and local replica of preamble with the correlation output of the maximum $+10$ or minimum -10. The later case is due the presence of phase ambiguity of π. It is illustrated in Figure 6.12, the receiver able to capture 8 satellites in view and the preamble found for each satellite at the delay of a symbol time. The index where the preamble is found is referred as "First Sub-frame" . Once it is known, the next symbol sign reveals about the even or odd page since even and odd page starts with -1 and 1 respectively. The identification of odd page later depicts about the position of unpredictable symbols as per OSNMA settings illustrated in Figure 4.1 (b).

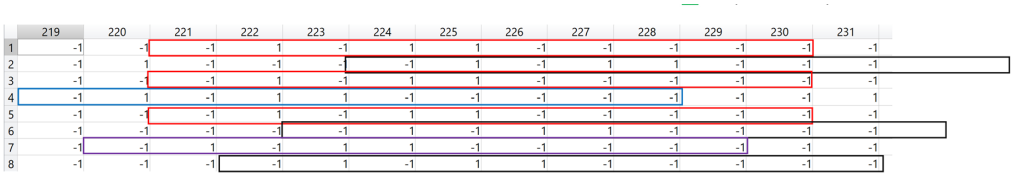


Figure 6.12: The preamble identification to detect the even and odd pages, where the index for instance, 219, 221, 244 are the first subframes for respective satellites in view.

Once the unpredictable symbols are detected, the snapshot OSNMA detector can be utilized to take those unpredictable symbols in each snapshot and compare with the ones, available at the server side. Taking into account the configured parameters of recorded signals, the threshold is theoretically calculated which sets to 0 since there is no prominent contribution in SER from any other impairments. Moreover, the time uncertainty is 0 in this simulation because the position of unpredictable symbols is known. Hence, the snapshot lengths are taken to coincide with the length of unpredictable symbols per batch, as highlighted with green color in Figure 4.1 (b) i.e. $L = \{9, 8, 8, 7\}$. It reveals the unpredictable symbols that have been spoofed in each snapshot number (SN) against the derived threshold as shown in Figure 6.13 and 6.14.

With Time Uncertainty: In the presence of time uncertainty, then the position of unpredictable symbols will be advanced or delayed with respect

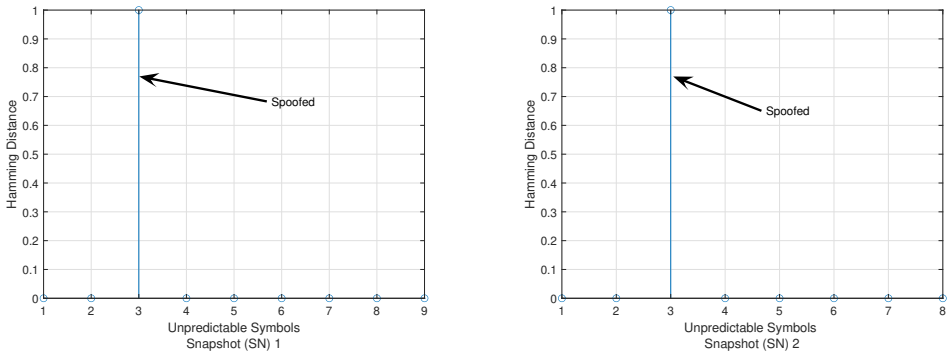


Figure 6.13: The 3rd unpredictable symbol of 1st snapshot is inverted by spoofer (left).The 3rd unpredictable symbol of 2nd snapshot is inverted by spoofer (right).

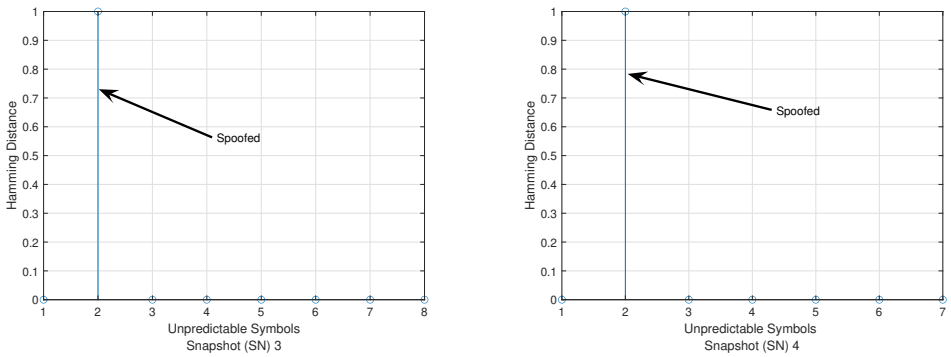


Figure 6.14: The 2nd unpredictable symbol of 3rd snapshot is inverted by spoofer (left).The 3rd unpredictable symbol of 4th snapshot is inverted by spoofer (right)

to their original position. In this scenario, already discussed in Chapter 5, a longer snapshot is required to combat the impact of time uncertainty. It was also discussed in that chapter, in general terms, it is reasonable to assume uncertainties amounting up to 80ms. This value, together with the 36ms of 9 unpredictable symbols per batch, requires to capture a snapshot of around 120ms in total, which equals 30 symbols, in order to avoid loosing unpredictable symbol.

Without loss of generality, a moderate scenario is considered now for assessing the impact of time uncertainty. A time offset of 20ms, which delays the unpredictable symbols positions by 5 symbols, is considered. Since the snapshot length is of 30 symbols, it comprises of both predictable and

unpredictable symbols. Therefore, the problem is extended to find the unpredictable symbols sequence position in the longer sequence and later compare with calculated threshold to detect the attack. This is executed by following the relation in (5.9). It slides the sequence of unpredictable symbols over each position of received symbols and stores the hamming distances. Afterwards, it finds the minimum of all hamming distance to get acquainted with the position of unpredictable symbols sequence and then compares it with pre-defined threshold.

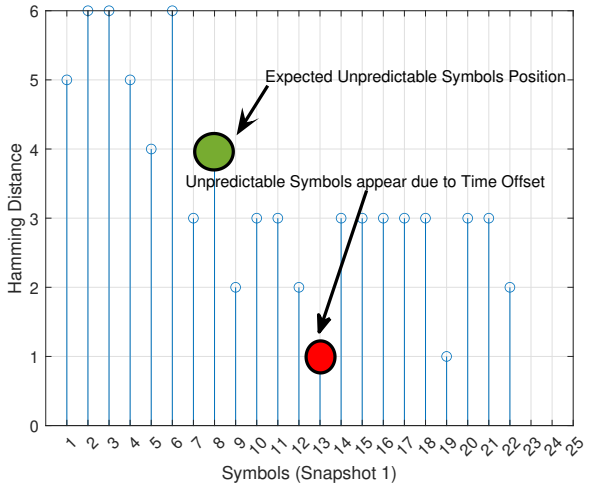


Figure 6.15: The impact of time uncertainty on the position of unpredictable symbol sequence.

The results in Figure 6.15 show the value of the detection metric, namely the Hamming distance. The unpredictable symbols are expected to be received at the position marked in Figure 6.15 using a green circle. However, due to the presence of a time offset, the sequence of unpredictable symbols is delayed and received at the delayed position marked with a red circle in Figure 6.15. It is important to note that the longer snapshot helped to detect the unpredictable symbols, otherwise 5 unpredictable symbols would have been missed. Taking a look at Figure 6.15, it can be seen that the Hamming distance actually takes its minimum value at the position where the unpredictable symbols are located, thus confirming that both spoofing detection and sequence alignment can simultaneously be achieved. Since the minimum hamming distance obtained in Figure 6.15 is shown to be 1, while the detection threshold is set 0 because no other impairments are expected, the snapshot OSNMA detector would flag this snapshot as “Spoofed”. This simple experiment shows, using real (i.e. RF) Galileo signals and a software

receiver, that spoofing can successfully be detected.

6.1.4 Conclusion

This chapter focused on validating the snapshot OSNMA and other theoretical relations from an experimental point of view. In this regard, it illustrated about the overall experimental scheme to implement the snapshot OSNMA on real like Galileo E1B signal. The overall scheme comprised of 3 modules. The first module is about the authentic and spoofed signal generation in the form of IQ samples employing the GNSS simulator i.e. Skydel. The other module is to process the recorded IQ files by using open source FGI-GRX GNSS software receiver which assisted to extract the symbols for authentication. The ultimate module is snapshot OSNMA software itself which provided insights about authenticating the received symbols extracted from experimental setup, by comparing with the authentic symbols. This final module is with the capabilities of providing the binary output about spoofer detection. Moreover, the experimental system level constraints are identified, thoroughly discussed and then solved to enable the normal working of the entire experimental system.

Publications and Other Supports

Publications

[1] **Shahid, H.**, Locubiche, S., Canzian, L., Sarto, C., Pozzobon, O., Fernandez-Hernandez, I., Reyes-González, J., Seco-Granados, G. and López-Salcedo, J.A., 2023. Feasibility of snapshot OSNMA for spoofing detection in urban scenarios. In Proc. European Navigation Conference (ENC).

[2] **Shahid, H.**, Canzian, L., Sarto, C., Pozzobon, O., Reyes-Gonzalez, J., Seco-Granados, G. and López-Salcedo, J.A., 2023, June. Statistical Characterization of Snapshot OSNMA Spoofing Detection. In 2023 International Conference on Localization and GNSS (ICL-GNSS) (pp. 1-6). IEEE.

[3] **Shahid, H.**, Canzian, L., Sarto, C., Pozzobon, O., Reyes-González, J., Seco-Granados, G. and López-Salcedo, J.A., 2023, October. Spoofing Detection Performance of Snapshot OSNMA Under Time and Symbol Errors. In 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall) (pp. 1-7). IEEE..

[4] **Shahid, H.**, Egea-Roca, D., Canzian, L., Sarto, C., Pozzobon, O., Fernandez-Hernandez, I., Reyes-González, J., Seco-Granados, G. and López-Salcedo, J.A., 2023. Boundary Conditions for Snapshot-Based Spoofing Detection using OSNMA Unpredictable Symbols. In GPS Solutions, 2024 (Submitted).

Support to Patent

The contribution other than publications is providing the comprehensive study of literature review in identifying the signal level and data level state-of-the-art techniques in snapshot based processing. The motivation behind is differentiating the work with the proposed snapshot OSNMA concept. Later,

snapshot OSNMA becomes as Italian patent application n. 102022000025806 filed on 16/12/2022.

Support to Develop Snapshot OSNMA Prototype

The support is provided to develop the software prototype which is an emulation of this defined "Snapshot OSNMA" technique and comprises of three main functional blocks, 1) Main emulator script file. 2) Receiver side emulating the user terminal. 3) Server side emulating the remote server where the snapshot OSNMA technique would be running. The functional flow of these blocks is illustrated in the Figure 6.16 , where it is highlighted that the main_emulator.m script is the main script in charge of initializing the simulation, setting all configuration parameters, and finally calling each of the required modules.

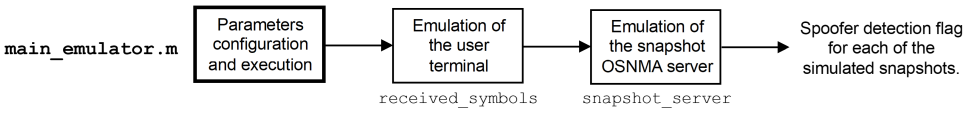


Figure 6.16: Functional flow of the software developed for the emulation of the snapshot OSNMA concept.

Bibliography

[1] G. Seco-Granados, J. Lopez-Salcedo, D. Jimenez-Banos, and G. Lopez-Risueno, "Challenges in indoor global navigation satellite systems: Unveiling its core features in signal processing," *IEEE Signal Processing Magazine*, vol. 29, no. 2, pp. 108–131, 2012.

[2] F. Dovis, *GNSS interference threats and countermeasures*. Artech House, 2015.

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

[4] W. De Wilde, J.-M. Sleewaegen, B. Bougard, G. Cuypers, A. Popugaev, M. Landmann, C. Schirmer, D. E. Roca, J. A. López-Salcedo, and G. S. Granados, "Authentication by polarization: A powerful anti-spoofing method," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 3643–3658.

[5] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, 2012.

[6] D. Miralles, A. Bornot, P. Rouquette, N. Levigne, D. M. Akos, Y.-H. Chen, S. Lo, and T. Walter, "An assessment of GPS spoofing detection via radio power and signal quality monitoring for aviation safety operations," *IEEE Intelligent Transportation Systems Magazine*, vol. 12, no. 3, pp. 136–146, 2020.

[7] F. Gallardo and A. P. Yuste, "SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection," *IEEE Access*, vol. 8, pp. 85 515–85 532, 2020.

[8] J. Wang, H. Li, X. Cui, and M. Lu, "A new method in acquisition to detect GNSS spoofing signal," in *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*. IEEE, 2013, pp. 2913–2917.

[9] J. Huang, L. L. Presti, B. Motella, and M. Pini, "GNSS spoofing detection: Theoretical analysis and performance of the ratio test metric in open sky," *Ict Express*, vol. 2, no. 1, pp. 37–40, 2016.

[10] M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets," *GPS solutions*, vol. 21, pp. 577–589, 2017.

[11] Y. Yang, H. Li, and M. Lu, "Performance assessment of signal quality monitoring based GNSS spoofing detection techniques," in *China Satellite Navigation Conference (CSNC) 2015 Proceedings: Volume I.* Springer, 2015, pp. 783–793.

[12] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," *IEEE Access*, vol. 6, pp. 66 428–66 441, 2018.

[13] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via Automatic Gain Control (AGC)," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[14] S. V. Achanta, "Multi-constellation GNSS integrity check for detection of time signal manipulation," Jul. 18 2017, uS Patent 9,709,682.

[15] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-dimensional signal quality monitoring for spoofing detection," in *Proceedings of the ESA/ESTEC NAVITEC 2016 Conference, Noordwijk, The Netherlands*, 2016, pp. 14–16.

[16] H. Maghdid, "Hybridisation of GNSS with other wireless/sensors technologies onboard smartphones to offer seamless outdoors-indoors positioning for lbs applications," Ph.D. dissertation, University of Buckingham, 2015.

[17] I. Fernández-Hernández and G. Seco-Granados, "Galileo NMA signal unpredictability and anti-replay protection," in *2016 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2016, pp. 1–5.

[18] G. Seco-Granados, D. Gómez-Casco, J. A. López-Salcedo, and I. Fernández-Hernández, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *GPS Solutions*, vol. 25, no. 2, p. 33, 2021.

[19] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improving secure code estimate-replay attacks and their detection on GNSS signals," *Proceedings of NAVITEC*, vol. 2014, 2014.

[20] C. O'Driscoll and I. Fernández-Hernández, "Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to Galileo OSNMA," in *Proc. ION GNSS+*, 2020, pp. 3751–3765.

[21] ETSI, "TS 103 246-3 - Satellite Earth stations and systems (SES); GNSS based location systems; Part 3: Performance requirements," October 2020.

[22] Skydel, "Orolia Skydel Software-Defined GNSS Simulator User Manual," November 2023.

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

[24] C. O'Driscoll, J. Winkel, and I. F. Hernandez, "Assisted NMA proof of concept on Android smartphones," in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2023, pp. 559–569.

[25] K. Borre, "The E1 Galileo signal," *Aalborg University, Denmark*, 2009.

[26] L. Wang, P. D. Groves, and M. K. Ziebart, "Multi-constellation GNSS performance evaluation for urban canyons using large virtual reality city models," *The Journal of Navigation*, vol. 65, no. 3, pp. 459–476, 2012.

[27] M. Falcone, J. Hahn, and T. Burger, "Galileo," *Springer handbook of Global Navigation Satellite Systems*, pp. 247–272, 2017.

[28] Y. Yang, Y. Mao, and B. Sun, "Basic performance and future developments of BeiDou Global Navigation Satellite System," *Satellite Navigation*, vol. 1, no. 1, pp. 1–8, 2020.

[29] H. Magsi, A. Hussain, A. Ahmed, F. A. Chachar *et al.*, "Investigation of ionospheric scintillation using Beidou during geomagnetic and non-geomagnetic storm conditions over Pakistan," in *2021 Seventh International Conference on Aerospace Science and Engineering (ICASE)*. IEEE, 2021, pp. 1–6.

[30] I. G. Petrovski, *GPS, GLONASS, Galileo, and BeiDou for mobile devices: from instant to precise positioning*. Cambridge University Press, 2014.

[31] W. Lechner and S. Baumann, "Global Navigation Satellite Systems," *Computers and Electronics in Agriculture*, vol. 25, no. 1-2, pp. 67–85, 2000.

[32] J. J. Spilker Jr, P. Axelrad, B. W. Parkinson, and P. Enge, *Global positioning system: theory and applications, volume I*. American Institute of Aeronautics and Astronautics, 1996.

[33] D. Gebre-Egziabher and S. Gleason, *GNSS applications and methods*. Artech House, 2009.

[34] E. Ochin, "Fundamentals of structural and functional organization of GNSS," in *GPS and GNSS technology in geosciences*. Elsevier, 2021, pp. 21–49.

[35] A. Alaqeeli, J. Starzyk, and F. Van Graas, "Real-time acquisition and tracking for GPS receivers," in *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03.*, vol. 4. IEEE, 2003, pp. IV–IV.

[36] P. D. Groves, Z. Jiang, B. Skelton, P. A. Cross, L. Lau, Y. Adane, and I. Kale, "Novel multipath mitigation methods using a dual-polarization antenna," in *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, 2010, pp. 140–151.

[37] S. Taylor, Y. Morton, Y. Jiao, J. Triplett, and W. Pelgrum, "An improved ionosphere scintillation event detection and automatic trigger for GNSS data collection systems," in *Proceedings of the 2012 International Technical Meeting of The Institute of Navigation*, 2012, pp. 1563–1569.

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

[39] K. Borre, J. A. López-Salcedo, and M. Z. H. Bhuiyan, *GNSS Software Receivers*. Cambridge University Press, 2022.

[40] T. E. Humphreys, M. L. Psiaki, B. M. Ledvina *et al.*, "GPS carrier tracking loop performance in the presence of ionospheric scintillations," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, 2005, pp. 156–167.

[41] L. Deambrogio and C. Macabiau, "Vector tracking aiding for carrier phase estimation in the presence of ionospheric scintillation," in *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, 2013, pp. 333–342.

[42] L. Dong, S. Chai, B. Zhang, S. K. Nguang, and X. Li, "Cooperative relay tracking strategy for multi-agent systems with assistance of voronoi diagrams," *Journal of the Franklin Institute*, vol. 353, no. 17, pp. 4422–4441, 2016.

[43] K. Huang, K. He, and X. Du, "A hybrid method to improve the BLE-based indoor positioning in a dense bluetooth environment," *Sensors*, vol. 19, no. 2, p. 424, 2019.

[44] M. Adjrad and P. D. Groves, "Enhancing least squares GNSS positioning with 3D mapping without accurate prior knowledge," *Navigation: Journal of The Institute of Navigation*, vol. 64, no. 1, pp. 75–91, 2017.

[45] P. Misra, B. P. Burke, and M. M. Pratt, "GPS performance in navigation," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 65–85, 1999.

[46] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *NAVIGATION, Journal of the Institute of Navigation*, vol. 63, no. 1, pp. 85–102, 2016.

[47] K. Zhang and P. Papadimitratos, "Safeguarding NMA enhanced Galileo os signals from distance-decreasing attacks," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, 2019, pp. 4041–4052.

[48] C. O'Driscoll, "What is Navigation Message Authentication?" *GNSS Solutions*, 2018.

[49] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service," in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2014)*, 2014, pp. 2810–2827.

[50] L. Heng, D. B. Work, and G. Gao, "Cooperative GNSS authentication," *Reliability from unreliable peers. Inside GNSS*, vol. 8, pp. 70–75, 2013.

[51] K. T. Seferoglu and A. S. Turk, "Review of spoofing and jamming attack on the global navigation systems band and countermeasure," in *2019 9th international conference on recent advances in space technologies (RAST)*. IEEE, 2019, pp. 513–520.

[52] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," *NAVIGATION: Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 73–82, 2015.

[53] U. Hunkeler, J. Colli-Vignarelli, and C. Dehollain, "Effectiveness of GPS-jamming and counter-measures," in *2012 International Conference on Localization and GNSS*. IEEE, 2012, pp. 1–4.

[54] D. Shuli, Z. Taotao, and L. Min, "A GNSS anti-spoofing technology based on power detection," in *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*. IEEE, 2019, pp. 1134–1137.

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

[56] T. Zhang, X. Chen, D. He, and Y. Jin, "Performance analysis and tests for GNSS spoofing detection based on the monitoring of cross ambiguity function and automatic gain control," in *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation*, 2021, pp. 98–110.

[57] C. Hegarty, B. O'Hanlon, A. Odeh, K. Shallberg, and J. Flake, "Spoofing detection in GNSS receivers through cross-ambiguity function monitoring," in *Proceedings of the 32nd International Technical Meeting of the*

Satellite Division of the Institute of Navigation (ION GNSS+ 2019), 2019, pp. 920–942.

[58] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Demicheli, and W. Feng, "A new signal quality monitoring method for anti-spoofing," in *China Satellite Navigation Conference (CSNC) 2018 Proceedings: Volume II*. Springer, 2018, pp. 221–231.

[59] D. Yuan, H. Li, F. Wang, and M. Lu, "A GNSS acquisition method with the capability of spoofing detection and mitigation," *Chinese Journal of Electronics*, vol. 27, no. 1, pp. 213–222, 2018.

[60] F. Chu, H. Li, and M. Lu, "A GNSS spoofing detection method based on the consistency of measured and calculated carrier dopplers," in *Proceedings of the ION 2017 Pacific PNT Meeting*, 2017, pp. 832–841.

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

[62] L. Xiao, P.-C. Ma, X.-M. Tang, and G.-F. Sun, "GNSS receiver anti-spoofing techniques: a review and future prospects," in *Electronics, Communications and Networks V: Proceedings of the 5th International Conference on Electronics, Communications and Networks (CECNet 2015)*. Springer, 2016, pp. 59–68.

[63] T. E. Humphreys, J. A. Bhatti, and B. M. Ledvina, "The GPS assimilator: a method for upgrading existing GPS user equipment to improve accuracy, robustness, and resistance to spoofing," in *Proceedings of the 23rd international technical meeting of the satellite division of the Institute of Navigation (ION GNSS 2010)*, 2010, pp. 1942–1952.

[64] D. Egea-Roca, G. Seco-Granados, and J. A. López-Salcedo, "Comprehensive overview of quickest detection theory and its application to GNSS threat detection," *Gyroscopy and Navigation*, vol. 8, pp. 1–14, 2017.

[65] V. L. Sabola, G. S. Granados, J. A. L. Salcedo, and J. A. García-Molina, "GNSS IoT positioning: from conventional sensors to a cloud-based solution," *Inside GNSS*, 2018.

[66] F. S. T. Van Diggelen, *GPS: Assisted GPS, GNSS, and SBAS*. Artech House, 2009.

[67] A. Kerkhoff, R. B. Harris, C. P. Petersen, and A. Pickard, "Modifications to GPS reference station antennas to reduce multipath," in *Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010)*, 2010, pp. 866–878.

[68] K. Bucket and M. Moeneclaey, "Effect of random carrier phase and timing errors on the detection of narrowband M-PSK and bandlimited DS/SS M-PSK signals," *IEEE Trans. on Commun.*, vol. 43, no. 2/3/4, pp. 1260–1263, 1995.

[69] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall, 1993, vol. I.

[70] D. Arndt, T. Heyn, J. König, A. Ihlow, A. Heuberger, R. Prieto-Cerdeira, and E. Eberlein, "Extended two-state narrowband LMS propagation model for S-Band," in *IEEE international Symposium on Broadband Multimedia Systems and Broadcasting*, 2012, pp. 1–6.

[71] R. Prieto-Cerdeira, F. Perez-Fontán, P. Burzigotti, A. Bolea-Alamañac, and I. Sánchez-Lago, "Versatile two-state land mobile satellite channel model with first application to DVB-SH analysis," *International Journal of Satellite Communications and Networking*, vol. 28, no. 5-6, pp. 291–315, 2010.

[72] K. Liang, Q. Chen, K. Han, Z. Yang, A. Zhang, and C. Ding, "Time transfer via BDS and Galileo compared to time transfer via GPS," in *Proc. Annual Precise Time and Time Interval Systems and Applications Meeting*, 2019, pp. 131–136.

[73] J. G. Proakis and M. Salehi, *Communication systems engineering*, 2nd ed. Prentice-Hall, 2002.

[74] G. Seco-Granados, D. Gomez-Casco, J. A. López-Salcedo, and I. Fernandez-Hernandez, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *GPS Solutions*, vol. 25, no. 2, pp. 1–15, 2021.

[75] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Prentice-Hall, 1998, vol. II.

[76] T. Nischan, "GFZRNX-RINEX GNSS data conversion and manipulation toolbox (version 1.05). GFZ data services," *Potsdam, Germany: German Research Centre for Geosciences (GFZ) https://doi.org/10.5880/GFZ*, vol. 1, no. 2016.002, 2016.

[77] B. Peterson, R. Hartnett, and G. Ottman, "GPS receiver structures for the urban canyon," in *Proceedings of the 8th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 1995)*, 1995, pp. 1323–1332.

[78] K. Muthuraman, J. Brown, and M. Chansarkar, "Coarse time navigation: Equivalence of algorithms and reliability of time estimates," in *Proc. ITM of the Institute of Navigation (ION GNSS)*, 2012, pp. 1115–1138.

[79] J. Massey, "Optimum frame synchronization," *IEEE Trans. on Commun.*, vol. 20, no. 2, pp. 115–119, 1972.

[80] R. Mehlan and H. Meyr, "Optimum frame synchronization for asynchronous packet transmission," in *Proc. IEEE Intl. Conf. on Commun. (ICC)*, vol. 2, 1993, pp. 826–830.

[81] M. Chiani and M. G. Martini, "Analysis of optimum frame synchronization based on periodically embedded sync words," *IEEE Trans. on Commun.*, vol. 55, no. 11, pp. 2056–2060, 2007.

[82] R. Scholtz, "Frame synchronization techniques," *IEEE Trans. on Commun.*, vol. 28, no. 8, pp. 1204–1213, 1980.

[83] R. Miškinis, D. Jokubauskis, D. Smirnov, E. Urba, B. Malyško, B. Dzindzelėta, and K. Svirskas, "Timing over a 4G mobile network," in *Proc. European Freq. and Time Forum (EFTF)*, 2014, pp. 491–493.

[84] W. J. Youden, "Index for rating diagnostic tests," *Cancer*, vol. 3, no. 1, pp. 32–35, 1950.

[85] S. Söderholm, M. Z. H. Bhuiyan, G. Ferrara, S. Thombre, and H. Kuusniemi, "A Multi-GNSS software receiver," *GNSS Software Receivers*, p. 174, 2022.