Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

Ingegneria Elettronica, Informatica e
delle Telecomunicazioni

Ciclo XXVII

Settore Concorsuale di afferenza: 09/F2

Settore Scientifico disciplinare: ING-INF/03

GNSS Interference Management Techniques Against Malicious Attacks

Presentata da: **Roberta Casile**

Coordinatore Dottorato	**Relatore**
Prof. Alessandro Vanelli Coralli	**Prof. Giovanni Emanuele Corazza**

Esame finale anno 2015

ROBERTA CASILE

GNSS INTERFERENCE MANAGEMENT TECHNIQUES AGAINST MALICIOUS ATTACKS

Ph.D. Programme in Electronics Engineering, Telecommunications
and Information Technology - XXVII Cycle
Department of Electrical, Electronic and Information Engineering -
DEI
Alma Mater Studiorum - Università di Bologna

GNSS INTERFERENCE MANAGEMENT TECHNIQUES AGAINST MALICIOUS ATTACKS

ROBERTA CASILE

Ph.D. Programme in Electronics Engineering, Telecommunications and Information Technology - XXVII Cycle

Coordinator: Prof. Alessandro Vanelli-Coralli
Supervisor: Prof. Giovanni E. Corazza

SC: 09/F2
SSD: ING-INF/03

Department of Electrical, Electronic and Information Engineering - DEI
Alma Mater Studiorum - Università di Bologna

March 2015

Roberta Casile: , Department of Electrical, Electronic and Information Engineering - DEI, Alma Mater Studiorum - Università di Bologna, © March 2015

To strive, to seek, to find, and not to yield.
— Alfred Tennyson, *Ulysses*

ABSTRACT

This thesis collects the outcomes of a Ph.D. course in Telecommunications Engineering and it is focused on the study and design of possible techniques able to counteract interference signal in Global Navigation Satellite System (GNSS) systems. The subject is the jamming threat in navigation systems, that has become a very increasingly important topic in recent years, due to the wide diffusion of GNSS-based civil applications. Detection and mitigation techniques are developed in order to fight out jamming signals, tested in different scenarios and including sophisticated signals. The thesis is organized in two main parts, which deal with management of GNSS intentional counterfeit signals.

The first part deals with the interference management, focusing on the intentional interfering signal. In particular, a technique for the detection and localization of the interfering signal level in the GNSS bands in frequency domain has been proposed. In addition, an effective mitigation technique which exploits the periodic characteristics of the common jamming signals reducing interfering effects at the receiver side has been introduced. Moreover, this technique has been also tested in a different and more complicated scenario resulting still effective in mitigation and cancellation the interfering signal, without high complexity.

The second part still deals with the problem of interference management, but regarding with more sophisticated signal. The attention is focused on the detection of spoofing signal, which is the most complex among the jamming signal types. Due to this highly difficulty in detect and mitigate this kind of signal, spoofing threat is considered the most dangerous. In this work, a possible techniques able to detect this sophisticated signal has been proposed, observing and exploiting jointly the outputs of several operational block measurements of the GNSS receiver operating chain.

INTRODUCTION

Nowadays, the major part of the people worldwide relies on satellite navigation systems to provide Position-Velocity-Time (PVT) solutions to a number of critical and commercial applications, with a strong impact on most aspects of the daily human life and for the society too. All common devices used everyday, as smartphones and vehicles, have a GNSS receiver, thus several applications rely on the accuracy of the delivered PVT solutions. In addition, the civilian applications that range from emergency to route instructions, including also all the types of transportation systems, from air through marine to land, and police and rescue services and many more, are based on the efficient functionalities of the GNSS infrastructure and thus they depend on the correct and reliable geosecurity location information. As a consequence of this growing demand, as a resource becomes spread and useful among civil infrastructure, malicious agents attempt to disrupt the GNSS services exploiting possible weakness inside the target system.

INTERFERENCE IN GNSS

The widespread use of civil location-based applications is due to the Global Positioning System (GPS), and more in general GNSS, signal structure which is defined in a freely-available and open-access specification [24][72]. Due to the low received power at earth's surface, GNSS signals are highly vulnerable to the most common attack as denial-of-service by jamming and intentional interference, which can be effective also within a range of several kilometers. The GNSS service deterioration is the result of natural disruptions, as ionospheric and tropospheric effects, unintentional artificial effects, as multipath, deliberate,intentional and malicious artificial effects, as jamming, meaconing and spoofing signals. In order to limit these deteriorating effects, it is necessary to design techniques against interfering signal due to the increasing diffusion of the GNSS based applications. Several types of interfering signals can affect GNSS operation in a different manner and a main characterization in different groups can be made. Thus, navigation system interfering signal can be divided in intentional and unintentional, and thus in jamming and out of band signals, respectively.

Unintentional

GNSS services can be deteriorated by Radio Frequency Interference (RFI) generated by instruments that are not working properly. This electronics elements can deny the service of navigation systems generating out-of-band frequencies that fall into the GNSS bands [83]. In

[15] the attention has been focused on the effects of the Digital Video Broadcast - Terrestrial (DVB-T) standard in the GNSS system. Authors have studied and show that due to the large diffusion of the receiver equipments for DVB-T system, this type of unintentional interferer represents an important issue to be solved also because the corresponding transmitters emit signals with a very close frequency to GNSS band, causing a high interference level. However, harmonic suppression capabilities of the antennas can reduce the effect of this kind of interference. Moving from electronic devices, the more dangerous non-intentional interfering signal occurs when the correct signal is affected by multipath propagation. When a GNSS receiver is located in a worse scenario as a urban canyon and it is not in Line of Sight (LOS), its functionalities are highly corrupted due to the several delayed replicas that are received, generated by the reflection of the useful signal on obstacles surfaces surrounding the receiver. These delayed replicas reduce the capabilities of the receiver in decoding and evaluating the PVT solutions (the shape of the correlation peak is distorted) and thus deteriorating the reception of the signal.

Intentional

The other main category is represented by the intentional interferer. These signal are generated to deny intentionally services provided by GNSS system. The scope of the jammer is to completely destroy the communication between transmitter and receiver and to deny the possibility of a correct exchange of information, and thus to receive PVT solutions (especially in military domain). Several possible strategies can be implemented by a jammer in order to be effective, and it depends on the type of target to be jammed. Usually, jamming waveforms are modulated signals as continuous wave, pulsed continuous wave, chirp signal. Electronic devices able to generate this jamming waveform can be purchased on-line at a very low cost, thus being available to be easily used. This Personal Privacy Device (PPD)s even if generating a low power signal, can deny the correct reception to the target and also to the closer receiver in a radius of less meters [31].
Among intentional interferer, also meaconing and spoofing signals have to be considered. These signals belong to the category of structured interferer with the main scope to mislead the GNSS sending to it a wrong PVT information, without any awareness by the receiver. Meaconing signal refer to the reception and the rebroadcast of the GNSS signal aiming to confuse with a wrong time-alignment the target receiver. Usually, meaconing is generated using a low noise amplifier and two passive antennas, without any navigation processor. On the other hand, spoofer represents the counterfeit copy of the GNSS signal. Among spoofer it is possible to discern simplistic spoofer, intermediate spoofer and sophisticated one. The first type is generated by a GPS generator and a transmitting antenna. It is very easy to detect simplistic spoofer signals because they are not able to duplicate or reproduce the correct time-synchronization of the GNSS signal-in-space.

The other types of spoofer signal are more complex. The intermediate and sophisticated spoofer is able to generate a malicious signal that it is totally equal to the useful one. This jammer source can correctly estimate the right time-synchronization of the constellation in view and consequently the receiver acquires and tracks this counterfeit copy without knowing that a malicious attack is occurring. In other words, under a spoofing or meaconing attack, a GNSS receiver is providing PVT solutions with good signal quality measures even if the position solutions do not represent the actual location of the receiver.

MOTIVATION

Taking into account this ever-growing dependance on GNSS, due to the several civil and safety existing applications, strong motivation to attack civil GNSS infrastructure has increased, for either an illegitimate advantage or terrorism purposes. Due to the known structure of the GNSS signal and for a non in-built security feature in the GNSS open service, the design of a jamming source able to deteriorate the correct operational function is becoming more feasible thanks to the very low cost of the necessary equipment [36]. Consequently, all jamming events and in particular the spoofer are becoming a serious issue for the next-generation of the GNSS infrastructure, and techniques capable to counteract these malicious attacks are required. The principal problem is strictly correlated to the huge diversification of the GNSS receivers; in other words, it is necessary to design detection and mitigation methods that do not require big hardware modifications. So far, several methods have been proposed to harden civil GNSS receiver against jamming attacks and in particular against spoofing effects. But in any case, civilian GNSS infrastructure is still subjected and without any defense solution against this sophisticated attack.

CONCLUSION

In summary, GNSS interference management research topic still presents open challenge due to the wide application arena and to the growing technological developments. In this dissertation the results of the research carried out during my Ph.D. activity are presented, in the context of structured interference management for satellite navigation systems. This activity has been mainly characterized by the continuous interaction with industrial partners within the framework of international research project [Pr1]. All the results of my activity provided in this dissertation represent possible solutions to the problems encountered within the aforementioned project. The collaboration and interaction with industrial partners have lead to a deeper comprehension of the requirement and of the trade-offs due to practical implementation. This opportunity has allowed to test the provided techniques with real data collected in a controlled scenario, satisfying the practical requirements.

ORIGINAL CONTRIBUTIONS

In this dissertation, the effects of interfering signal in satellite navigation systems have been studied and analyzed. Possible and innovative techniques are provided with the aim of reduction of the jamming effects and thus to enhance the reliability and the functionality of the GNSS receiver. It is worthwhile to underline that the scope of the thesis is then trying to detect interferers and collect malicious signals from the very statistical point of view taking into account that the GNSS receiver aims to mitigate interfering effects rather than to detect it. This consideration allows to deal with detection and characterization of even very low-power jammers. The principal contribution of the thesis regards with the jamming management technique in complex scenarios. In the framework of the DETECTOR project [Pr1] a deep description and overview of the interfering issue in satellite navigation systems has been carried out. Considering the main purpose of the project, the PhD candidate has described and provided new approaches in detection and mitigation of jamming signals. In particular, moving from scientistic previous references, interfering signal with particular characteristics have been considered, evaluated from exhaustive measurement campaigns. From these results, an innovative approach for the detection and above all for the mitigation of interfering signals has been designed [P4]. Moreover, a development of the study-case is provided. The aforementioned detection and mitigation techniques has been tested in a different scenarios, worse than the previous one. The innovative aspect consists in the possibility of apply the already described methods to more complex scenario, as can be the dispersive channel, and verify that they still properly work. In other words, in this dissertation a general study of the interfering signal in a multipath scenario (urban canyon) is provided and numerical results show that provided technique is still effective in detecting and canceling the jamming waveform, with a slightly decreased performance but without any increasing of the computational complexity of the solution in [P4]. Furthermore, the attention has been focused on a more sophisticated class of jamming signal, i. e.the spoofer. It is well known that spoofing signals represent the most difficult kind of signal to be detected and consequently to be mitigated. In the dissertation, a possible and innovative approach is presented. This technique is based on the jointly observation and evaluation of measurement outputs from several blocks locating inside GNSS receiver. Through these measurements, it is possible to define threshold in order to detect the spoofer when it occurs. The results have been carried out by observing real data collected in controlled scenario with different implementation and by evaluation from real-space GNSS signal collected in airport station.

PERSONAL PUBLICATIONS

[P1] Bartolucci, M; Casile, R.; Pojani, G.; Corazza, G.E.;, "Joint Jammer Detection and Localization for Dependable GNSS," *Positioning, Navigation and Timing (ION-PNT), 2015 International Conference on,* April 2015 (*SUBMITTED TO*).

[P2] Bartolucci, M; Casile, R.; Gabelli, G.; Guidotti, A.; Corazza, G.E.; "Distributed-Sensing Waveform Estimation for Interference Cancellation," *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014),* September 2014.

[P3] Bartolucci, M; Casile, R.; Corazza, G.E.; Durante, A.; Gabelli, G.;Guidotti, A.;, "Cooperativedistributed localization and characterization of GNSS jamming interference," *Localization and GNSS (ICL-GNSS), 2013 International Conference on,* June 2013.

[P4] Gabelli, G.; Casile, R.; Guidotti, A.; Corazza, G.E.; "GNSS Jamming Interference: Characterization and Cancellation," *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation,* January 2013.

[P5] Gabelli, G.; Corazza, G.E.; Deambrogio, L.; Casile, R.; , "Code acquisition under strong dynamics: The case of TT&C for LEOP," *Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC)*, 2012.

PROJECTS

[Pr1] "Detection, Evaluation and Characterization of Threats to Road Applications (DETECTOR)," FP7 Grant Agreement: 277619-2 - in collaboration with Nottingham Scientific Limited (NSL), SANEF, ARIC, Black Holes B.V. and IPSC.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

AWGN	Additive White Gaussian Noise
AC	Autocorrelation
AGC	Automatic Gain Control
AOA	Angle Of Arrival

BOC	Binary Offset Carrier
CIE	Central Instant Error
CN0	Carrier-to-Noise Ratio
CRB	Cramer Rao Bound
DC	Duty Cycle
DFT	Discrete Fourier Transform
DLL	Delay Lock Loop
DOA	Direction of Arrival
DVB-T	Digital Video Broadcast - Terrestrial
ESD	Energy Spectral Density
FFT	Fast Fourier Transform
FM	Frequency Modulated
FT	Fourier Transform
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICC	Interference Characterization and Cancellation
IFFT	Inverse FFT
IIR	Infinite Impulse Response
JNR	Jammer-to-Noise Ratio
LNA	Low Noise Amplifier
LOS	Line of Sight
ML	Maximum Likelihood
MSE	Mean Square Error
O_D	Obsevation Duration
PLL	Phase-Locked Loop
PM	Phase Modulated
PPD	Personal Privacy Device
PRN	Pseudorandom Noise
PSD	Power Spectral Density
PVT	Position-Velocity-Time
RAIM	Receive Autonomous Integrity Monitoring

RFI	Radio Frequency Interference
RMS	Root Mean Square
RMSE	Root Mean Square Error
SQM	Signal Quality Monitoring
TDOA	Time Difference Of Arrival
WT	Wavelet Transform

Part I

INTERFERENCE MANAGEMENT TECHNIQUES

Due to their low power levels, GNSS signals are highly susceptible to both intentional and unintentional RFI sources disruptions. The increasing diversification of everyday life applications based on satellite navigation systems requires a high reliability of the communication link, in each step from the transmission to the reception one, above all for the safety-critical applications [45]. Jamming signals, which can deteriorate or even deny the provided GNSS services, and unintentional RFI sources, as malfunctioning elements, represent a paramount problem in GNSS operating chain. Thus, the problem of how to face RFI, and in particular the intentional one, has become a hot topic in recent years [12], [P4],[9]. For this reason, it is necessary to define solutions able to guarantee and to maintain the GNSS service and reliability in presence of such threats.

The aim of this thesis is to analyze the problem and to propose new solutions able to counteract interfering signals. In particular, the main aim is to design techniques in order to detect the presence of interfering signals, to localize the malicious sources, and to mitigate and reduce their effects.

1

INTERFERENCE DETECTION

1.1 INTRODUCTION

The diversity of the GNSS [58] based applications in the majority of the human life habits increases its importance and consequently its vulnerability against malicious attacks. As well known, the GNSS signals hare broadcast and received at a very low power level at the receiver side and for this reason are very vulnerable to the RFI effects, both unintentionally and intentionally generated [45]. The malicious attacks aim to degrade the performance of all that systems and applications based on correct information of timing and positioning provided by the GNSS, leading to the complete disruption of the service [8][7][61][13][33]. The higher the jamming power, the more dangerous the consequence on the GNSS quality of service. Due to these powerful issues, it is necessary to design techniques able to contrast interfering effects and to minimize their disruptive aims. The first step is to identify if an interferer is present or not. In literature, several detection techniques have been proposed based on the analysis of signal outputs of blocks in the reception chain as Automatic Gain Control (AGC) [32], Carrier-to-Noise Ratio (CN0) evaluation [39] and cooperative techniques which exploit correlator metric information from distributed nodes [70]. The major part of detection techniques is essentially based on the Time Difference Of Arrival (TDOA) and Angle Of Arrival (AOA) estimation methods and some research works analyzed also the Direction of Arrival (DOA) estimates [71]; some researchers also studied a possible combination of the cited techniques [18].

Instead, in this work a different interference detection approach is presented. The method is performed in the frequencies domain, thus exploiting spectral signatures of the jamming signals, moving from the above cited and widely used localization techniques. Our technique exploits the Wavelet Transform (WT) of the Power Spectral Density (PSD) of the interfering signal. By means of the time-scale transform, it is possible to detect discontinuities in the received signal spectrum, corresponding to the higher values of the wavelet coefficients. Once transients are detected it is possible to estimate the bandwidth of the jamming signal and to evaluate the mean spectral energy. Furthermore, this method is also applied in the time-domain in order to define the time envelope of the received signal. The goal is to determine the duty cycle of the signal, and so the periodical repetition of the interfering event. The algorithms have been thoroughly described, and validated by means of numerical simulations and results with both synthetized signal by MATLAB tool and collected data in controlled scenarios [Pr1].

The rest of the chapter is structured as follows: in Section 1.2 the system model is present; in Section 1.3 and Section 1.4 the approaches in the frequency domain and time domain are described, and validated by performance evaluation and numerical results, respectively; in Section 1.5 an update version of the frequency domain approach is described with several numerical results obtained by testing our algorithm with data, collected in controlled scenario. Concluding remarks are given in Section 1.6

1.2 SYSTEM MODEL

Previously an introduction to the most common approaches for interference detection in GNSS has been provided. As already explained, the interfering signals aim to deteriorate the communication between transmitter and receiver. The malicious signal is received with the useful signal trying to corrupt the receiver's capabilities in decoding correct information and PVT solutions. The received signal at the target device can be expressed as [28][65]:

$$\begin{aligned} r(t) &= \sum_{k=1}^{N_s} \sqrt{P_k} s_k\left(t-\tau_k\right) e^{j\left(\theta_k+2\pi f_k t\right)} \\ &+ \sqrt{P_I} s_I\left(t-\tau_I\right) e^{j\left(\theta_I+2\pi f_I t\right)} + w(t) \end{aligned} \tag{1}$$

where N_s is the number of satellite signals, P_k and P_I are the useful signal power of the k-th satellite and the interference power, respectively; τ_k, f_k, θ_k and τ_I, f_I, θ_I are the time delay, frequency and phase offset of the useful signal and the interfering signal respectively, $w(t)$ is the Additive White Gaussian Noise (AWGN) with power spectral density equal to σ_w^2. Considering $\lfloor i \rfloor_A = \lfloor \frac{i}{A} \rfloor$ and $|i|_A = i \bmod A$, the k-th satellite signal can be expressed as [28]:

$$s_k(t) = \sum_{l=-\infty}^{+\infty} D_k\left(\lfloor l \rfloor_{L_s}\right) a_k\left(\lfloor l \rfloor_{L_s}\right) g\left(t - lT_c\right) \tag{2}$$

where $D_k(l)$ is the data sequence, $a_k(l)$ is the pseudo-random spreading sequence transmitted by the k-th satellite, L_s is the spreading sequence length and $g(t)$ is the filter response with a limited support of $[0, T_c]$, where T_c is the chip period. The whole frequency band of the GNSS was firstly divided in two bands:

- Upper L band: $f \in [1559 - 1610]$MHz to which Glonass G1, GPS L1 and Galileo E1 belong;
- Lower L band: $f \in [1151 - 1214]$MHz to which Glonass G3, GPS L5, Galileo E5 belong.

Successively, GPS L2, Glonass G3 and Galileo E6 have been located in the remaining frequencies $f \in [1215.6 - 1350]$MHz for radio-location services. This is the reason why this partial band is more susceptible to the interfering than the previous ones. However, in the following the upper L band will be considered and the effects of the interfering signal will be analyzed. Now, a description of the considered interfering signals is carried out. The most common GNSS interfering signals are defined by periodic envelope, with particular Autocorrelation (AC) function characteristics [12],[48]. Current interfering waveforms are defined by angle modulated signals which have a periodic core $z(t)$. They can be written as:

$$s_{FM}(t) = A\exp\left\{j2\pi\left(f_0 t + \int_{-\infty}^{t} z(\xi)d\xi\right)\right\} \tag{3}$$

$$s_{PM}(t) = A\exp\{j2\pi(f_0 t + z(t))\} \tag{4}$$

which correspond to Frequency Modulated (FM) and Phase Modulated (PM), respectively. For a generic and periodic modulation function

$$z(t) = \sum_k z_0(t - kT) \tag{5}$$

and consequently the equations (3) and (4) can be rewritten, respectively, as:

$$s_{FM}(t) = \sum_k A_k \bar{s}_{FM}(t - kT)e^{\Theta_{FM}(k)} \tag{6}$$

$$s_{PM}(t) = \sum_k A_k \bar{s}_{PM}(t - kT)e^{\Theta_{PM}(k)} \tag{7}$$

These signals are defined as structured signals due to their periodic core waveform. Due to these properties, they can be classified as parametric waveforms because by exploiting AC characteristics it is possible to represents them by means of specific parameters, estimated by tracking the periodic waveform. However, it is worthwhile to notice that among interfering signals also non parametric waveforms are presents. These kind of signals do not present periodic envelope and consequently particular AC characteristics and thus they cannot be identified by a parametric representation. Non-parametric waveforms represent a more difficult family of interfering signals that are more difficult to characterize and classify simply because *a priori* information is not available. Accordingly, solutions to detect and estimate this kind of signals are the spectrum estimation techniques and time-scale and time-frequency mathematical tool, able to extract primary information from the received signal [53].

1.3 INTERFERENCE BAND DETECTION

As mentioned previously, several interference detection techniques have been proposed and deeply discussed in literature. By exploiting the well known WT [21], it is possible to estimate the interference bandwidth, for both structured and non-structured interference. In the last case, bandwidth estimation is one of the few information regarding the received interfering signal. In [25] and [54] interference mitigation algorithms that exploit WT are presented. This mathematical tool allows for identification and reconstruction of the interfering signal due to the split in the time-scale domain from the useful signal, with interesting results in terms of mitigation purposes. The basic idea is to use the wavelet coefficients, the output of the WT on the PSD of the signal, as the identifiers of the transient processes in the PSD envelope. In particular, the discontinuities of the signal correspond to high values of the wavelet coefficients. Once the discontinuities have been detected, the PSD samples to which a high coefficient value correspond are identified, and it is thus possible to localize the signal in the frequency domain, and to evaluate the mean interference energy. The characterization algorithm identifies the bands inside which most of the interfering signal energy is concentrated. More in particular, this algorithm provide means to determine how the interfering signal is distributed in the frequency domain, and consequently it is possible to determine the number and the dimension of the interfered bandwidths. The *Band Detection* algorithm exploits the WT of the received signal PSD in order to detect interfered bands. By means of the WT, it is possible to identify where any discontinuities is localized. The proposed algorithm is described by the pseudo code in the algorithm1 and shown in the block diagram in Figure (1).

```
Frequency Characterization & Band Detection;

1) $\bar{\mathbf{r}} = \{r(nT_s) : kO_D < nT_s < (k+1)O_D\}$;

2) $\bar{\mathbf{S}} = |fft(\bar{\mathbf{r}})|^2$;

3) $\bar{\mathbf{a}} = [a_1, \dots, a_{N_s}] = [2^1, \dots, 2^{N_s}]$;

4) $\mathbf{W}(n, a) = \left[\mathbf{W}_{\mathbf{a_1}} \star \bar{\mathbf{S}}, \dots, \mathbf{W}_{\mathbf{a_{N_s}}} \star \S\right]$;

5) $\mathbf{P}(n) = \prod_{a=1}^{N_s} |\mathbf{W}(n, a)|$;

6) $\mathbf{F} = \{n : \mathbf{P}(n) > \xi_{WT}\}$;

7) $\mathbf{B} = \{[\mathbf{F}(i), \mathbf{F}(i+1)] :; \frac{1}{\mathbf{F}(i+1) - \mathbf{F}(i)}; \sum_{j=\mathbf{F}(i)}^{\mathbf{F}(i+1)} \bar{\mathbf{S}}(j); > A\sigma^2\}$;
```

Algorithmus 1 : Frequency Characterization & Band Detection

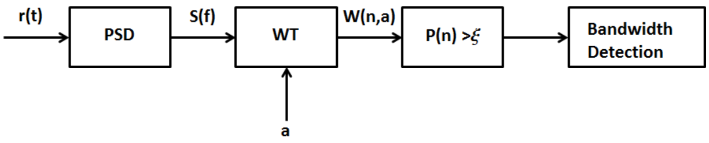


Figure 1: Band Detection - Block Diagram

The procedure consists in sampling the received signal in a time window of Obsevation Duration (O_D)(line 1) and then the PSD is calculated (line 2). In order to perform WT it is necessary to select the scale factors, according to the resolution to be achieved. The scale factors have been chosen to be the set of powers of 2, ranging from 2 to 2^{N_s} (line 3). The time-scale transform is then evaluated for each scale factor, which identifies different frequency bands with different resolutions. The chosen mother wavelet is the *Haar* wavelet function $\phi(t)$ defined as:

$$\phi(t) = \begin{cases} 1 & 0 < t < 1/2 \\ -1 & -1/2 < t < 0 \\ 0 & \text{otherwise} \end{cases}$$

For each scale factor the WT can be implemented as the convolution between the wavelet function and the signal $\bar{S}$ (line 4). The output of the convolution is a matrix with each row corresponding to a scale factor and each column corresponding to a time instant. If a discontinuity is present in the PSD envelope, the wavelet coefficient, obtained from the convolution, is very high. Through this analysis it is possible to identify the discontinuities of the signal, in particular when and also where, at which sample, the signal shows transients. Subsequently, for each time instant, the product of the absolute values of the wavelet transform corresponding to the different scale factors is calculated, as indicated in line (5). The rationale is that if a PSD discontinuity exists for a certain frequency value, this results in a high wavelet transform, for all the scale factors; taking the product of the absolute values helps eliminating undesired peaks due to noise. Frequencies corresponding to peaks of the sequence obtained as result of the previous product are selected. In order to eliminate undesired measurements due to noise a comparison with a threshold is performed, as indicated at line (6). The power of each detected interferer band, comprised between two successive detected frequencies, is compared to a threshold, and only those bands in which the mean power spectral density crosses the threshold are identified (line 7).

1.3.1 *Performance Analysis*

The performance evaluation for the above algorithm is presented below.

1.3.1.1 *Performance Evaluation Criteria*

The chosen performance evaluation criteria are the *Probability of Missed Detection* (P_{md}) and the *Probability of Outlier* (P_{out}). We define P_{md} as the probability of not-detecting the presence of the interfering signal within the interfered band. On the other hand, we identify P_{out} as the probability of detecting at least an interfered band event outside the ideal interferer interval. These kinds of detected events are classified

J_0/N_0	$[0, 5, 10, 15]$ [dB]
Minimum frequency	0.5 [MHz]
Maximum Frequency	$[8, 4, 2, 1]$

Table 1: Simulation parameters for frequency characterization

as outliers because they are detected outside the real interferer signal and so they are the results of a wrong detection analysis. Under the hypothesis of correct detection, we also evaluate the accuracy of the bandwidth measurements. In particular, we evaluate the mean error of estimation of the central frequency f_c defined as

$$e_c = \sqrt{E\left[|\hat{f_c} - f_c|^2\right]} \tag{8}$$

defined as the difference between the estimated central frequency of the interfered band and the estimated central frequency, and the error of the estimated bandwidth

$$e_c = \sqrt{E\left[|\hat{B} - B|^2\right]} \tag{9}$$

defined as the difference between the estimated bandwidth and the interfered bandwidth. Previous errors have been estimated by means of *Root Mean Square Error* (RMSE) for both the central frequency error (RMSE CFE) and the bandwidth error (RMSE BE).

1.3.1.2 *Scenario*

Simulation tests are carried out considering an interfering signal embedded in *Additive White Gaussian Noise* (AWGN) with a power spectral density ratio J_0/N_0 ranging from 0 to 15 dB. We consider wide band interfering signal with power lower than the saturation level. The minimum frequency is set equal to 500kHz and the maximum frequency is determined from the f_s/f_{max} factor, which interval is set equal to $[2.5, 5, 10, 15]$.

1.3.1.3 *Algorithm Optimization*

In the following the parameters characterizing the algorithm are presented. The parameters are resumed in table 2. An observation duration O_D equal to $10, 20[\mu s]$ has been considered in order to follow also rapid variations of the signal frequency characteristics. The number of scales factors considered has been calculated according to the dimension of the observable length. In particular maximum wavelet duration equal to one fourth of the observable duration has been considered. A wavelet threshold equal to twice the variance of noise after the wavelet transform has been considered. This is due to the fact that, according to the Central Limit Theorem, the distribution of the Haar wavelet transform of the square of a noise sequence with i.i.d. samples distributed as Gaussian random variables with zero mean and variance σ^2 ($\sim N(0, \sigma^2)$), converges to a Gaussian random variable with zero mean variance equal to $2\sigma^2$ ($\sim N(0, 2\sigma^2)$). Different values for the last verification threshold are selected as shown in table 2

Sampling Frequency	f_s	20 [MHz]
Observation Duration	O_D	$10, 20[\mu s]$
Number of scales factors	N_s	round((log$_2$(O_D))-2)
Wavelet threshold	ξ_{WT}	$2(2\sigma^2)^{N_s}$
Mean PSD threshold	$A\sigma^2$	A=[1, 3, 5, 7, 9, 11, 15]

Table 2: Algorithm parameters for frequency characterization

1.3.1.4 *Numerical Results*

In this section the numerical results of the performance of the Band Detector algorithm are presented. In Figures [2,3,4,5] the probability of missed detection and probability of outlier with observation duration equal to $10[\mu s]$ are presented. It is possible to observe that both the probabilities increase as the ratio f_s/f_{max} becomes higher, that is, with decreasing maximum frequency. This is in line with the expectations since for constant J_0/N_0 the signal power decreases with its bandwidth, thus becoming less visible.

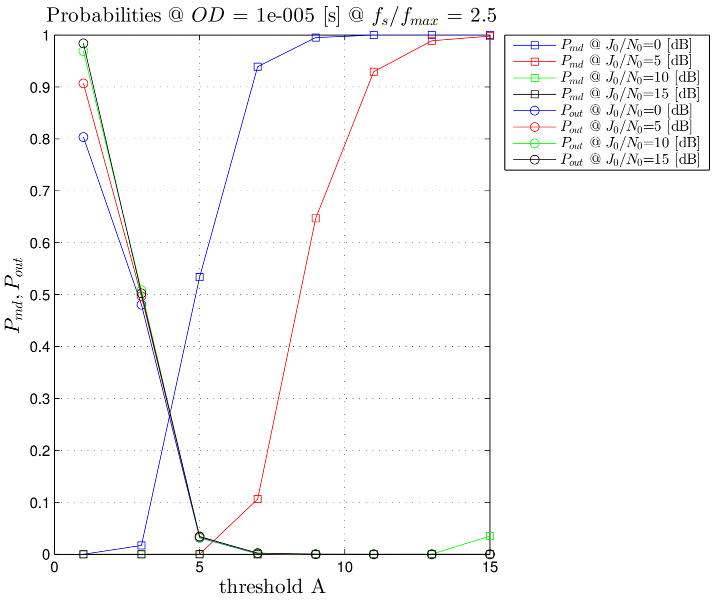


Figure 2: P_{md}, P_{out}@ Observation duration equal to $10[\mu s]$ and $f_{max} = 8[MHz]$

On the other hand, in Figures [6,7,8,9], the probability of missed detection and probability of outlier behaviors are respectively shown considering the observation duration equal to $20[\mu s]$. In this case the performance result to be better than in the previous case, but still the probabilities increase with decreasing maximum frequency.

The Root Mean Square Error (RMSE) for the bandwidth estimation error has been evaluated considering $f_s/f_{max} = 2.5(f_{max} = 8MHz)$ and the observation window at $10, 20[\mu s]$. As shown in Figures [[10,11]], the RMSE values saturate for $J_0/N_0 = 0$, but decreases rapidly when the interferer becomes more visible, resulting in errors of magnitude of 10^{-3} for the best case.

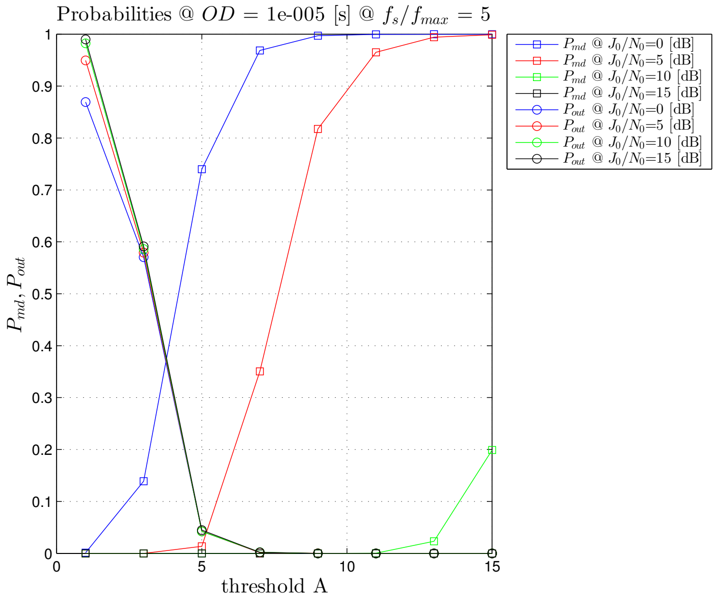


Figure 3: P_{md}, P_{out}@ Observation duration equal to $10[\mu s]$ and $f_{max} = 4[MHz]$

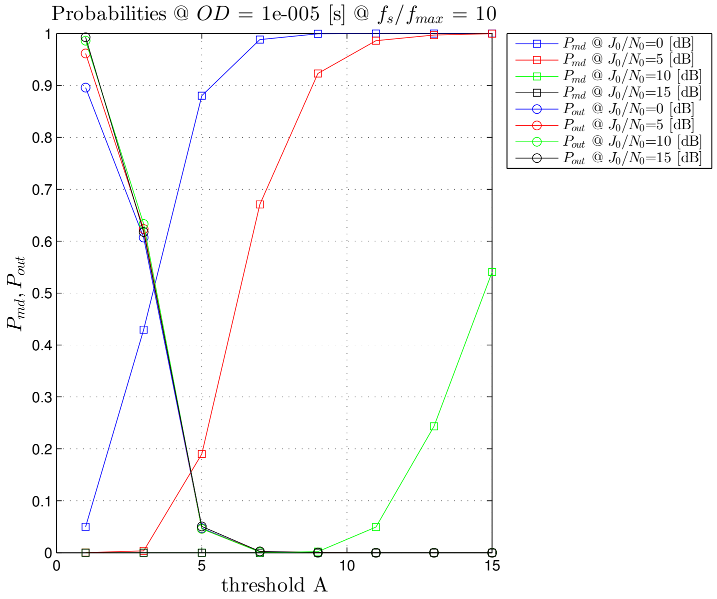


Figure 4: P_{md}, P_{out}@ Observation duration equal to $10[\mu s]$ and $f_{max} = 2[MHz]$

A similar behavior is shown for the Root Mean Square (RMS) of the central frequency estimation error. As shown in Figures [12,13], no significant information is provided by the algorithm in case $J_0/N_0 = 0$, but it becomes rapidly precise with increasing interference to noise ratio. Moreover, it is possible to observe that a little gain can be obtained by considering longer observables.

1.3.1.5 *Numerical Complexity*

The numerical complexity of the Band detection block is principally defined by the complexity of the Wavelet Transform WT. The com-

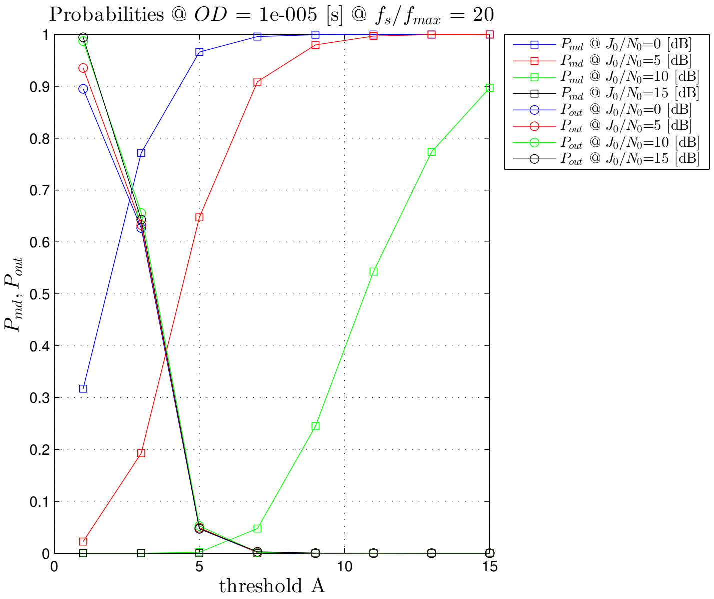


Figure 5: P_{md}, P_{out}@ Observation duration equal to $10[\mu s]$ and $f_{max} = 1[MHz]$

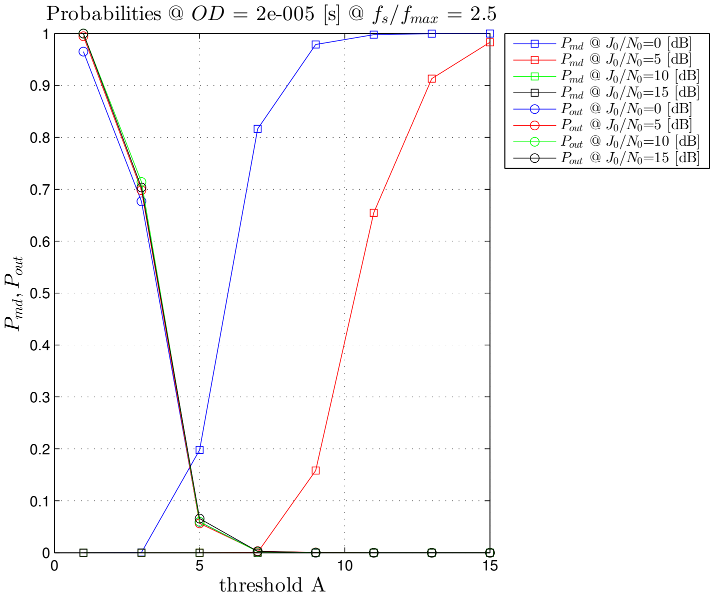


Figure 6: P_{md}, P_{out}@ Observation duration equal to $20[\mu s]$ and $f_{max} = 8[MHz]$

plexity of the algorithm, expressed in terms of number of needed operations, is given by the following:

- $\mathcal{O}\left(\frac{O_D}{2}\log_2(O_D)\right)$ products and sums for the or the calculation of the signal Fast Fourier Transform (FFT);
- O_D products needed for the calculation of the power spectral density;
- $O_D\left(2^{N_s+1}-2\right)$ products and sums, for the calculation of the incoming signal Wavelet Transform WT;

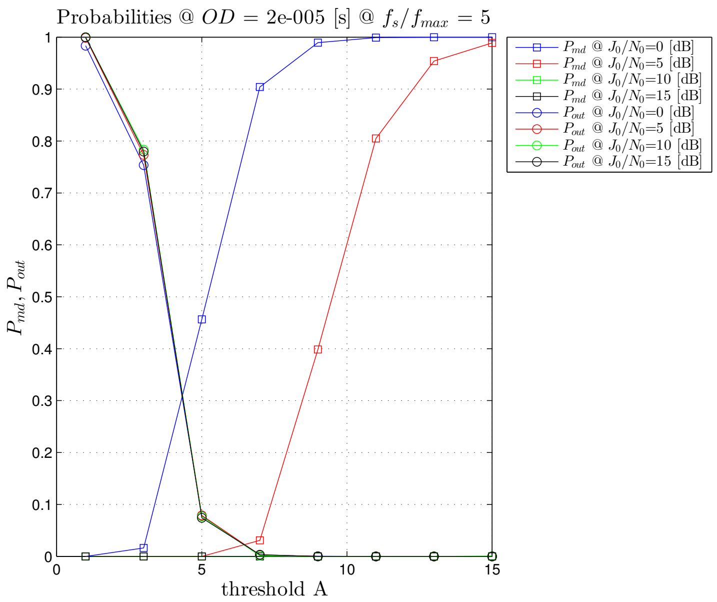


Figure 7: P_{md}, P_{out}@ Observation duration equal to 20[μs] and f_{max} = 4[MHz]

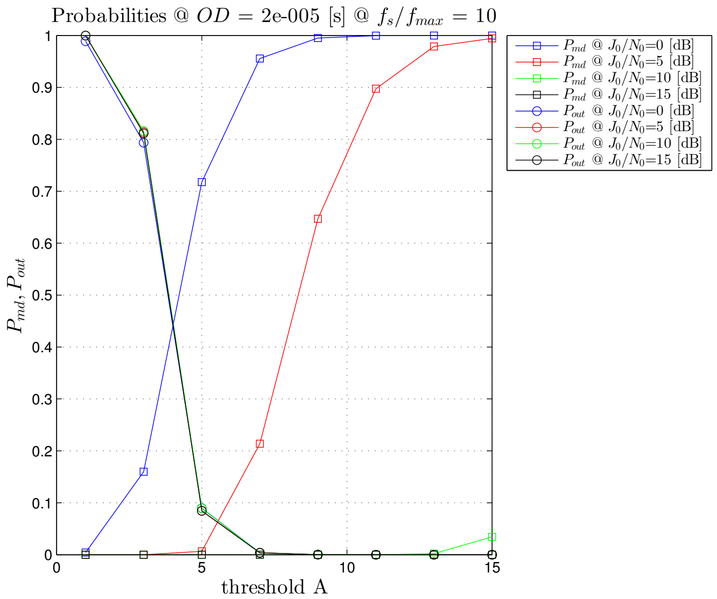


Figure 8: P_{md}, P_{out}@ Observation duration equal to 20[μs] and f_{max} = 2[MHz]

- $O_D N_s$ multiplications for calculation of the wavelet product array;
- O_D sums for the calculation of the band mean power spectral density.

1.4 INTERFERENCE DUTY-CYCLE ESTIMATION

A different approach for the characterization of a structured signal consists in identifying the duration of the activity period of the interferers. It is well known that for pulsed or short burst interferers,

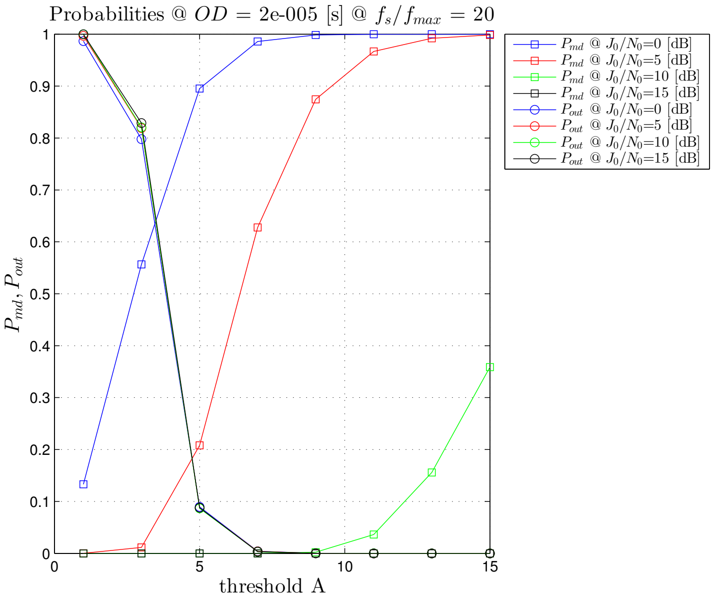


Figure 9: P_{md}, P_{out}@ Observation duration equal to $20[\mu s]$ and $f_{max} = 1[MHz]$

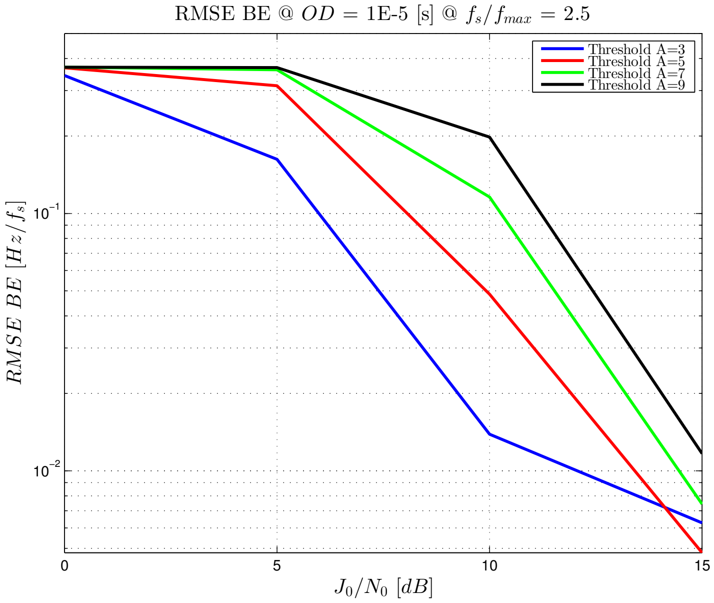


Figure 10: P_{md}, P_{out}@ Observation duration equal to $10[\mu s]$ and $f_{max} = 8[MHz]$

management techniques like blanking can be very effective; so the identification of the interfered time-intervals can be crucial for the proper success of these algorithms.

1.4.1 *Duty-Cycle Estimation*

The estimation of the interfering intervals in time domain is performed by the *Duty Cycle Estimation algorithm*. The duty cycle can be determined by estimating the period of the signal and the period of activity of the jamming source. The first task, as already shown, can be performed by exploiting the autocorrelation properties of the inter-

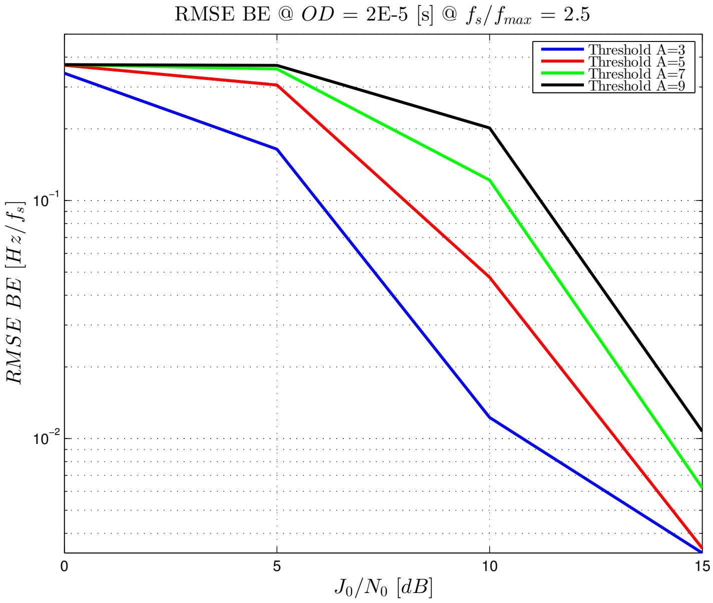


Figure 11: P_{md}, P_{out}@ Observation duration equal to 20[μs] and f_{max} = 8[MHz]

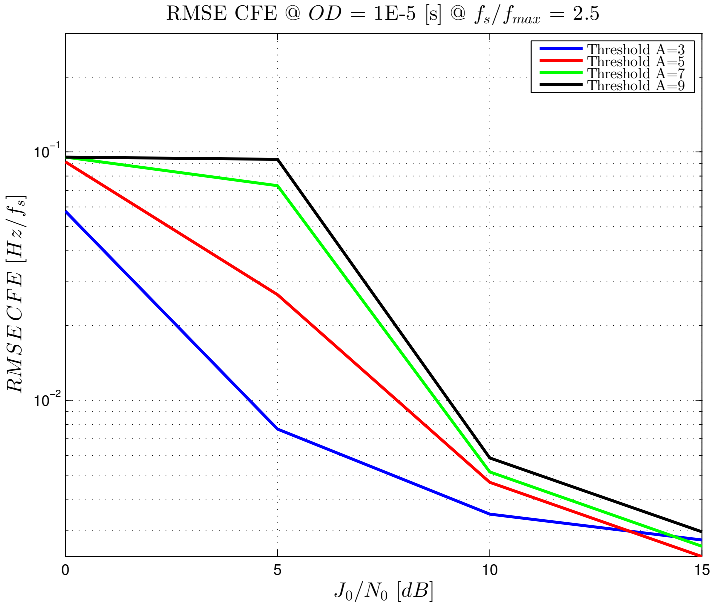


Figure 12: RMSE CFE @ Observation duration equal to 10[μs] and f_{max} = 8[MHz]

fering signals, thus by exploiting the results of the structure detection and of the waveform estimation algorithms. On the other hand, the estimation of the time-interval of activity of an interferer can be carried out by considering the approach proposed for the frequency characterization. The detection and measurement of an interfering signal time burst can be dealt with as for a limited band in the frequency domain. The proposed algorithm thus exploits the technique proposed for frequency characterization for the estimation of the activity period of the interfering signals.

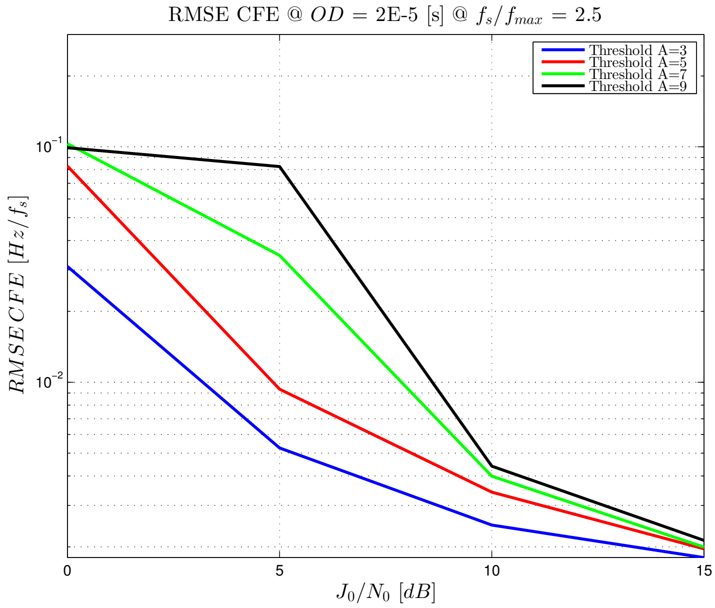


Figure 13: RMSE CFE @ Observation duration equal to 20[μs] and $f_{max} =$ 8[MHz]

Duty-Cycle Estimation;

1) $\hat{T}$;

2) $\bar{\mathbf{r}} = \{r(nT_s) : kT < nT_s < (k+1)T\}$;

3) $\bar{\mathbf{Y}} = |\bar{\mathbf{r}}|^2$;

4) $\bar{\mathbf{a}} = [a_1, \ldots, a_{N_s}] = [2^1, \ldots, 2^{N_s}]$;

5) $\mathbf{W}(n, a) = \left[\mathbf{W}_{\mathbf{a_1}} \star \bar{\mathbf{Y}}, \ldots, \mathbf{W}_{\mathbf{a_{N_s}}} \star \bar{\mathbf{Y}}\right]$;

6) $\mathbf{P}(n) = \prod_{a=1}^{N_s} |\mathbf{W}(n, a)|$;

7) $\mathbf{T} = \{n : \mathbf{P}(n) > \xi_{WT}\}$;

8) $\mathbf{I} = \{[\mathbf{T}(i), \mathbf{T}(i+1)] : \frac{1}{\mathbf{T}(i+1)-\mathbf{T}(i)}; \sum_{j=\mathbf{T}(i)}^{\mathbf{T}(i+1)} \bar{\mathbf{Y}}(j); > A\sigma^2\}$;

9) $\mathbf{DC} = \mathbf{I}/\hat{T}$;

Algorithmus 2 : Duty-Cycle Estimation

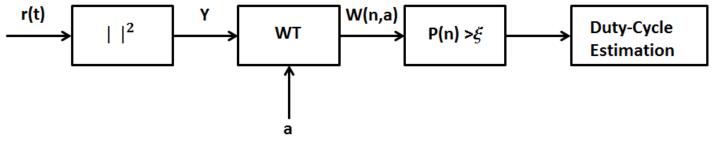


Figure 14: Duty Cycle Estimation - Block Diagram

As the *Band Detection* algorithm, the *Duty Cycle Estimation* can be described according to the pseudo-code in Algorithm 2 and shown in block diagram in Figure (14). Firstly, the period estimate from the AC analysis is considered (line 1) in order to define each signal period repetition. In line 3 the energy of the signal is computed. In order to perform WT it is necessary to select the scale factor, according to the resolution to be achieved. The scale factors have been chosen to be the set of powers of 2, ranging from 2 to 2^{N_s} (line 4). The time-scale transform is then evaluated for each scale factor (line 5) and the product of all the WT outputs is performed (line 6). In order to eliminate undesired measurements due to noise a comparison with a threshold is performed, as indicated in line 7. The power of each interfering interval is calculated and successively compared with a threshold proportional to the noise power. Finally, the duty-cycle of the interfering signal is estimated as the ratio between the detected intervals and the period estimate. The main difference with respect to the previously presented results consists in the evaluation of the power envelope of the signal, as indicated at line (3) since, in this case, the time characteristics must be obtained. The algorithm provides information on both the burst localization and on the duty-cycle values.

1.4.2 *Performance Analysis*

1.4.2.1 *Performance Evaluation Criteria*

As for the previous case performance has been evaluated in terms of probability of detection P_{md} and in terms of probability of outlier P_{out}. Moreover, in order to evaluate the accuracy of the proposed solution, the mean error

$$e_c = \sqrt{E\left(|\hat{t_c} - t_c|^2\right)} \tag{10}$$

defined as the difference between the estimated central instant of the interfering burst signal and the real instant, and the mean error

$$e_D = \sqrt{E\left(|\hat{I} - I|^2\right)} \tag{11}$$

defined as the difference between the duration estimation and the real burst duration, have been estimated.

1.4.2.2 *Scenario*

As for the previous case, simulation tests are carried out considering an interfering signal embedded in AWGN with an interfering signal power to noise ratio J/N ranging from 0 to 15 [dB]. We consider signals with a period equal to 10 and $20[\mu s]$. The generated signals are chirp signals with instantaneous frequencies rapidly growing over the receiver bandwidth, thus generating duty cycle values equal to $0.05, 0.5$ and 0.8. Parameters are shown in table 3.

Interference-to-Noise-Ratio	J/N	$[0, 5, 10, 15]$ [dB]
Signal Period	T	$10, 20[\mu s]$
Duty Cycle	DC	$[0.05, 0.5, 0.8]$

Table 3: Simulation parameters for duty cycle estimation

Sampling Frequency	f_s	20 [MHz]
Observation Duration	O_D	$10, 20[\mu s]$
Number of scales factors	N_s	round(($\log_2(O_D)$)-2)
Wavelet threshold	ξ_{WT}	$2(2\sigma^2)^{N_s}$
Mean PSD threshold	$A\sigma^2$	A=[1, 3, 5, 7, 9, 11, 15]

Table 4: Algorithm parameters for frequency characterization

1.4.2.3 *Algorithm Optimization*

The same criterion used for the optimization of the algorithm for the frequency domain characterization has been considered. The characteristic parameters are resumed in Table 4:

- The number of scales factors considered has been calculated according to the dimension of estimated signal period.
- A wavelet threshold equal to twice the variance of noise after the wavelet transform has been considered.
- Various values for the last verification threshold are selected, shown in table 4

1.4.2.4 *Numerical Results*

Figures [15,16,17] show the performance of the probability of missed detection and of the probability of false alarm, when an outlier is detected. As the results for the frequency domain, detection performance increases with increasing duty cycle since, with longer signal duration, the wavelet transform give rise to more relevant peaks. On the other hand, probability of false alarm can be easily controlled by selecting the appropriate threshold value.

The RMS for the duty cycle estimation is shown in Figures [18,19,20]. It can be noticed that the RMS is in the order of 10^{-2} for low J/N values when the duty cycle Duty Cycle (DC) is set to 0.05. This first value is lower than those obtained in the successive cases with DC values equal to 0.5 and 0.8, respectively. In these other cases, the RMS is in the order of 10^{-1} for low J/N values and in the latter case it is bigger than in the former one. The difference of the magnitude of RMS duty cycle estimation error between $0.05, 0.5, 0.8$ cases at low J/N values is due to the behavior of the proposed algorithm which is completely driven by noise: in fact, the false alarm probability due to the detection of narrow intervals is larger than that due to the detection of longer intervals. Taking into account these properties, the error in the

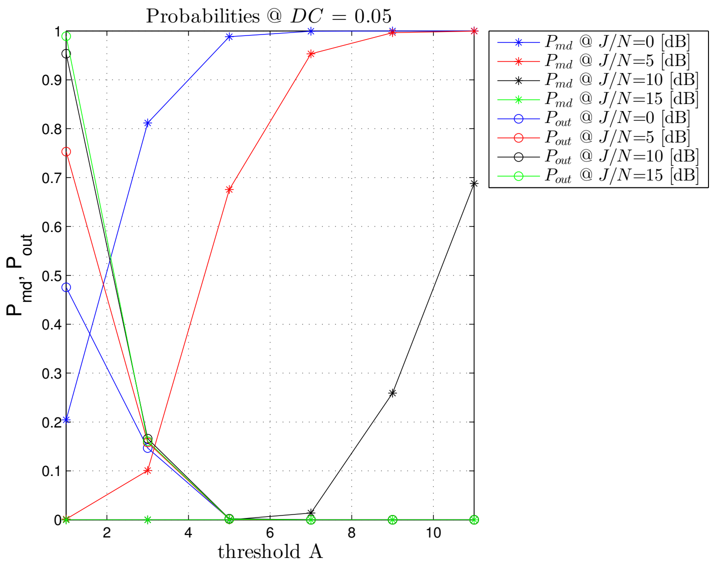


Figure 15: P_{md}, P_{out}@ Duty Cycle equal to 0.05

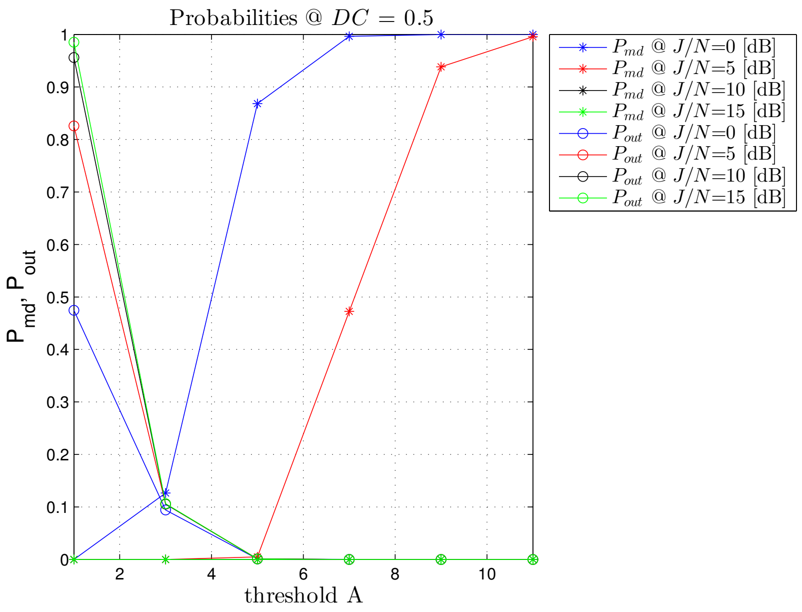


Figure 16: P_{md}, P_{out}@ Duty Cycle equal to 0.5

detection of narrow signals is smaller than that related to the detection of the longer ones. Looking at the figures, it can be observed that there is an intersection between the curves. We distinguished three threshold values A set as integer multiples of the noise power. Furthermore, we considered $A = 3, A = 5, A = 7$ represented with blue, red, and black lines, respectively. As it can be noticed, the blue line crosses the others for high J/N values. This is possible because the selected threshold value is always lower than the other two and so it is less selective, causing a higher RMS value.

In conclusion, the performance evaluations in terms of RMS of the central interfered instant estimation error Central Instant Error (CIE) are shown in Figures [21,22,23]. As it can be noticed, the RMSE become larger with the increasing of the duty cycle value. Thus, as seen for the

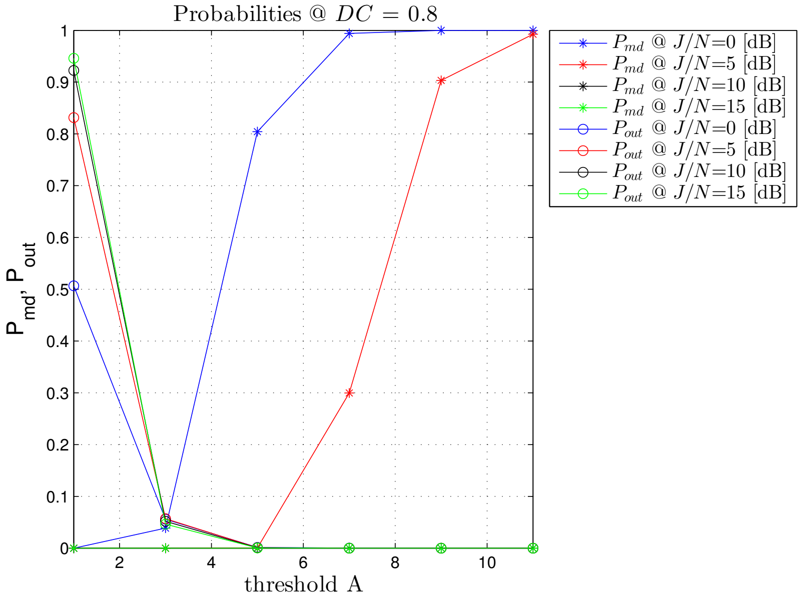


Figure 17: P_{md}, P_{out}@ Duty Cycle equal to 0.8

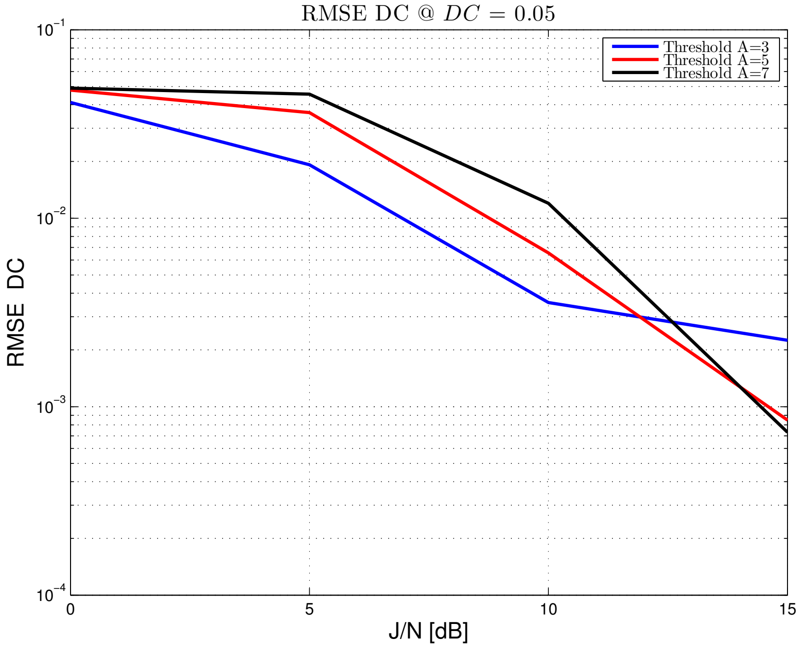


Figure 18: RMSE DC @ Duty cycle equal to 0.05

duty cycle error estimation, the RMSE is, with low J/N values, smaller for short signals than for larger ones. For high J/N values, the blue line, related to threshold $A = 3$, crosses the other two, related to threshold $A = 5$, $A = 7$, red and black line respectively, and it is due to the fact that the threshold is lower and so it is less selective than the other two, as seen in the duty cycle error estimation case.

1.5 BANDWIDTH DETECTION: UPDATE AND VALIDATION

As previously described in 1.3, the aim of the Bandwidth Detection algorithm is to identify the bands in which most of the interfering

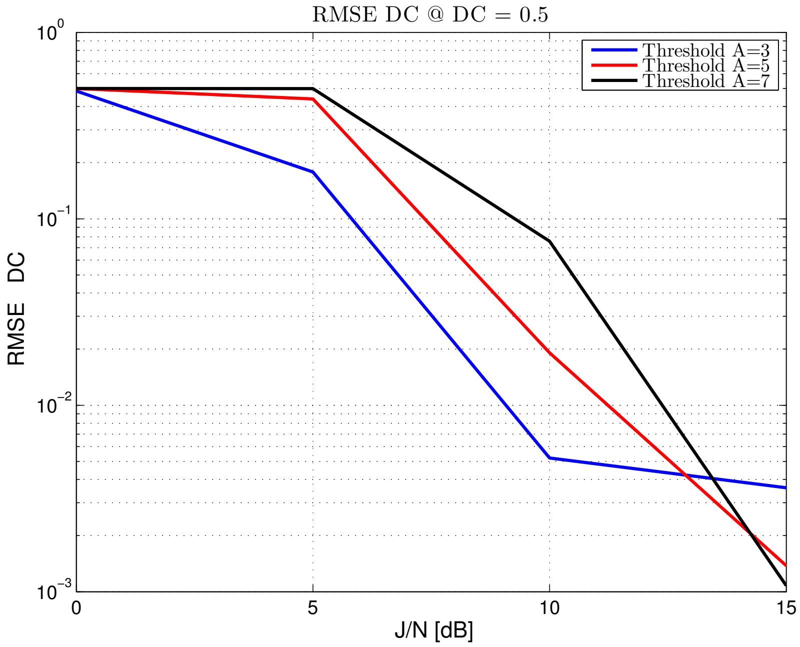


Figure 19: RMSE DC @ Duty cycle equal to 0.5

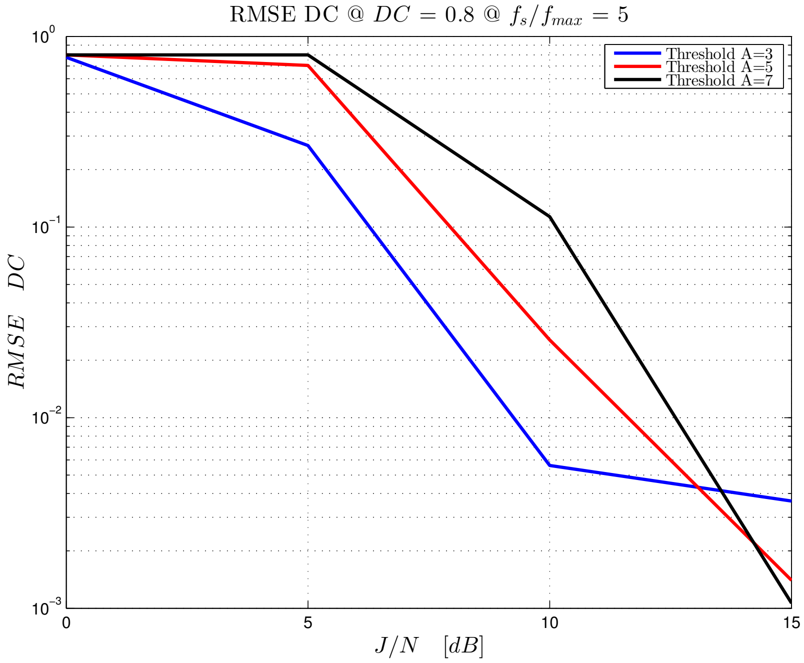


Figure 20: RMSE DC @ Duty cycle equal to 0.5

signal energy is concentrated. Such task is performed by applying the WT on the received signal PSD. By means of the WT, it is possible to identify the transient processes in the PSD envelope, thus allowing the localization of each discontinuity. In the following, a brief description of the algorithm is provided, with an update with respect to 1.3 due to the proper consideration of the RF front-end bandpass characteristics, and the results for a complete validation campaign are shown.

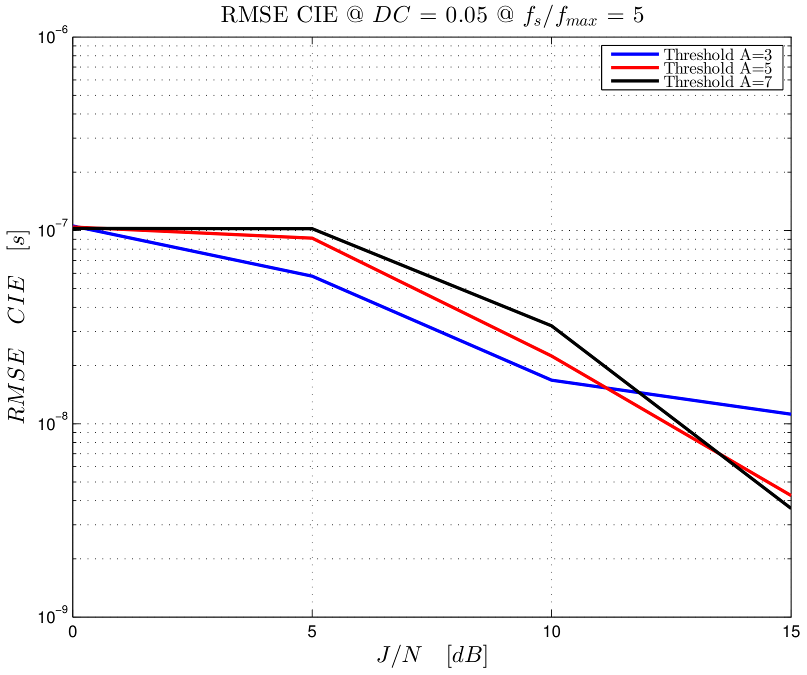


Figure 21: RMSE CIE @ Duty cycle equal to 0.05

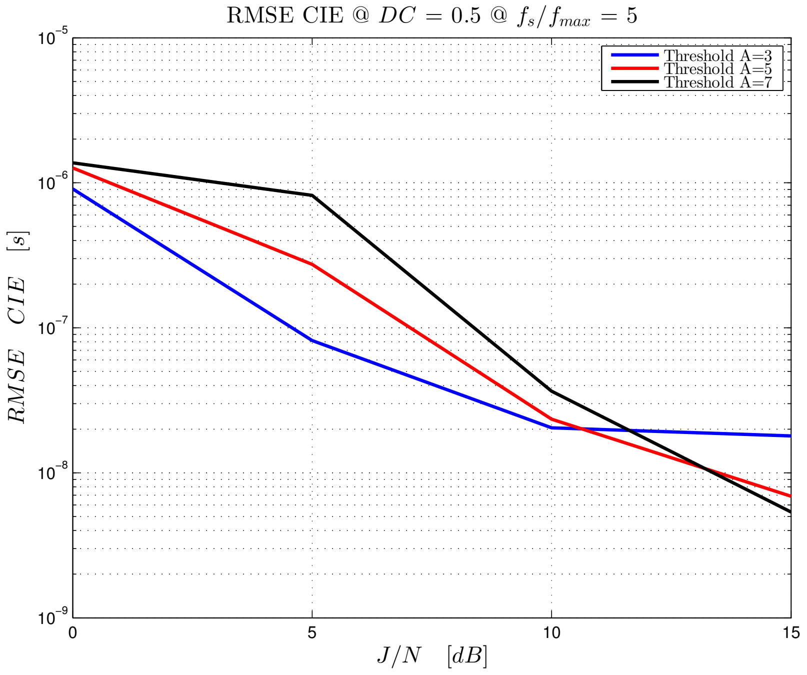


Figure 22: RMSE CIE @ Duty cycle equal to 0.5

1.5.1 *Bandwidth Detection Algorithm: Update Description*

The update algorithm is described by the pseudo-code in the algorithm 3:

The procedure consists in:

- Sampling the received signal on a time window of duration O_D as expressed in line (1). The obtained signal has a number of

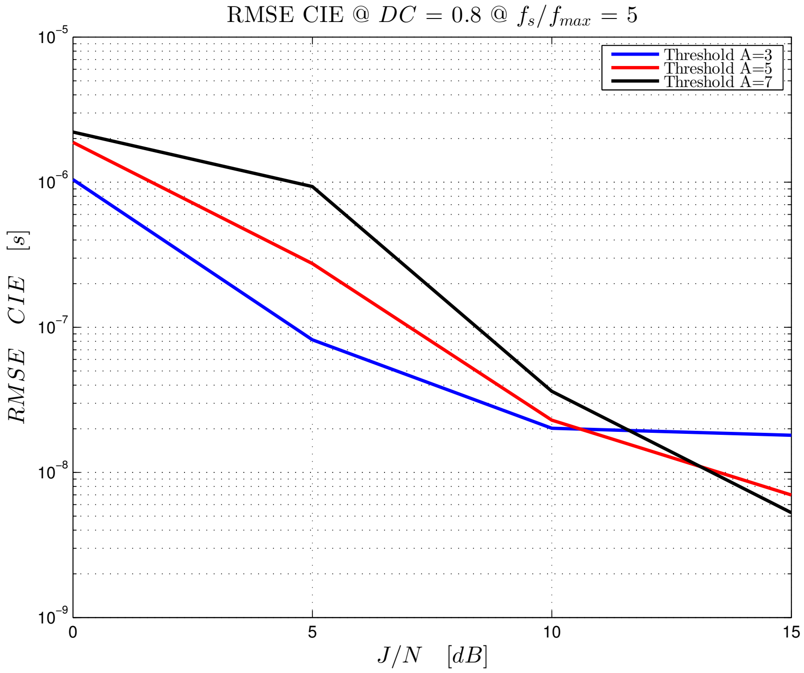


Figure 23: RMSE CIE @ Duty cycle equal to 0.8

samples define by the product $O_D * f_s$, , where f_s, is the sampling frequency.

- The PSD $\bar{S}(f)$ is calculated through the Fourier Transform, as defined in line (2).
- The PSD is limited to the front-end bandwidth B_N, where no attenuation is present, as shown in line (3).
- The noise energy level is estimated by averaging the received signal power over N successive non-interfered observation windows.
- The PSD is down-sampled, as shown in line (5), in order to transform the received signal power spectral density vector of length L_S, into a shorter vector, $S_R(f)$, of length L_{SP}, thus limiting the overall algorithm complexity. The new PSD vector has a shorter number of samples, which depends only on the desired signal length.
- The scale factors of the wavelet transform are selected as indicated at line (6). The scale factor have been chosen to be the set of powers of 2 ranging from 2 to 2^{N_s} .
- The WT of $S_R(f)$ is calculated as indicated at line (7) for each of the scale factors previously selected. The Haar wavelet function $\phi(t)$ was considered as mother wavelet, defined in eq.(**??**).For each scale factor the WT can be implemented as the convolution between the wavelet function $\phi(t)$ and $\bar{S}_R(f)$. The output of the WT is a matrix where the rows correspond to the scale factors and the columns to the time instants. If a discontinuity

```
Frequency Characterization & Band Detection;
1) $\bar{\mathbf{r}} = \{r(nT_s) : kO_D < nT_s < (k+1)O_D\}$;
2) $\bar{\mathbf{S}} = |\mathrm{fft}(\bar{\mathbf{r}})|^2$;
3) $\bar{s}(f) : \{f \in [-B_N, B_N]\}$;
4) $\hat{\sigma}^2 = \frac{1}{N} \sum_i \left( \frac{1}{N_f} \sum_f \hat{S_i}(f) \right)$;
5) $\hat{S_R}(f) = downsample\left(\bar{S}(f)\right)$;
6) $\bar{\mathbf{a}} = [a_1, \ldots, a_{N_s}] = [2^1, \ldots, 2^{N_s}]$;
7) $\mathbf{W}(n, a) = \left[\mathbf{W}_{\mathbf{a_1}} \star \bar{\mathbf{S}}, \ldots, \mathbf{W}_{\mathbf{a}_{\mathbf{N_s}}} \star \bar{\mathbf{S}}\right]$;
8) $\mathbf{P}(n) = \prod_{s=1}^{N_s} |\mathbf{W}(n, s)|$;
9) $\mathbf{F} = \{n : \mathbf{P}(n) > \xi_{WT}\}$;
10) $\mathbf{B} = \{[\mathbf{F}(i), \mathbf{F}(i+1)] :; \frac{1}{\mathbf{F}(i+1) - \mathbf{F}(i)}; \sum_{j=\mathbf{F}(i)}^{\mathbf{F}(i+1)} \bar{\mathbf{S}}(j); > A\sigma^2\}$;
```

Algorithmus 3 : Frequency Characterization & Band Detection

is present in the PSD envelope, the wavelet coefficient is very high. Through this analysis it is thus possible to identify any discontinuity of the signal, in particular when and also where (at which sample) the signal presents transients.

- For each time instant, the product of the absolute values of the WT corresponding to the different scale factors is calculated, as indicated at line (8). The rationale is that if a PSD discontinuity exists for a certain frequency value, this results in a high WT coefficient, for all the scale factors; taking the product of the absolute values helps eliminating undesired peaks due to noise.
- Those frequencies corresponding to peaks of the sequence obtained as result of the previous product are selected. In order to avoid peak selection triggered by noise, a comparison with a threshold is performed, as indicated at line (9).
- The power of each detected interferer band, included between two successive detected frequencies, is compared to a threshold, and only those bands in which the mean power spectral density is above the threshold are identified (line (10)).

1.5.2 *Bandwidth Detection: Validation Campaign*

The validation campaign has been performed considering real interference signals collected in an urban scenario. It has been possible to observe that these signals consist in different types of waveforms, such as single tones, chirps. As previously stated, the algorithm aims at detecting the interfered bandwidth inside the spectrum of the received signal.

1.5.2.1 *Bandwidth Detection: Algorithm Optimization*

In the following the parameters characterizing the algorithm are presented. In particular:

- An observation duration O_D equal to $1ms$ has been considered in order to track the envelope of the interference.
- The signal length is defined as the product between the observation window O_D and the sampling frequency f_s.
- The normalized bandwidth B_N is defined as the frequency interval not afflicted by the front-end filter attenuation.
- The shorter signal $\bar{S}_R(f)$ to be processed is evaluated through the down-sampling of the original signal $\bar{S}(f)$, extracting a sample every step interval: $\bar{S}_R(f) = \bar{S}(f)([1 : step : L_{SP}])$. The step parameter depends on the desired final signal length L_{SP}.
- The number of scale factors has been calculated according to the signal length after the down-sampling. In particular, a maximum wavelet duration equal to one fourth of the observable duration has been considered.
- A wavelet threshold, equal to twice the estimated noise level, after the wavelet transform has been considered. This is due to the fact that, according to the Central Limit Theorem, the distribution of the Haar wavelet transform of the square of a noise sequence with *i.i.d.* samples distributed as Gaussian random variables with zero mean and variance σ^2 $(\sim \mathcal{N}(0, \sigma^2))$, converges to a Gaussian random variable with zero mean variance equal to $2\sigma^2(\sim \mathcal{N}(0, 2\sigma^2))$.
- Different values for the power verification threshold have been selected as indicated in table 5.

1.5.2.2 *BD Numerical Results*

In this section, the results of the validation campaign for the Band Detector algorithm are presented by comparing the measured power spectral density functions with the detected bands. Moreover, the received signal spectrograms are shown in order to check the correct behavior of the detection algorithm. It is worth to highlight that detected interferer bandwidths are defined in terms of normalized frequencies

Sampling Frequency	f_s	16 [MHz]
Observation Duration	O_D	$1[ms]$
Signal Length	L_S	16000 samples
Number of Realizations	N	100
Normalized Bandwidth	B_N	$[-0.35, 0.35]$
Shorter Signal Length	L_{SP}	400 samples
Number of scales factors	N_s	$\text{round}((\log_2(L_{SP})) - 2)$
Wavelet threshold	ξ_{WT}	$2(2\sigma^2)^{N_s}$
Mean PSD threshold	$A\sigma^2$	$A = [2, 4, 8]$

Table 5: Update parameters for frequency characterization

reversed by the down-conversion. For example, an interferer normalized bandwidth equal to $[-0.3, 0.3]$ translates to an actual bandwidth of $[-4.8, 4.8]$MHz relative to the L1 central frequency 1575.42MHz. In Figure 24, the spectrogram of the signal *Urban_IF_Data_hr15_timeo 360_0380_B* is shown. Through the spectrogram it is possible to observe that the considered signal is a chirp waveform, with a normalized bandwidth of 0.7 (which corresponds to the RF Front-End bandwidth). More specifically, it is possible to observe that most of the interferer energy is contained in two frequency intervals, $[-0.3, 0.1]$ and $[0.1, 0.3]$.

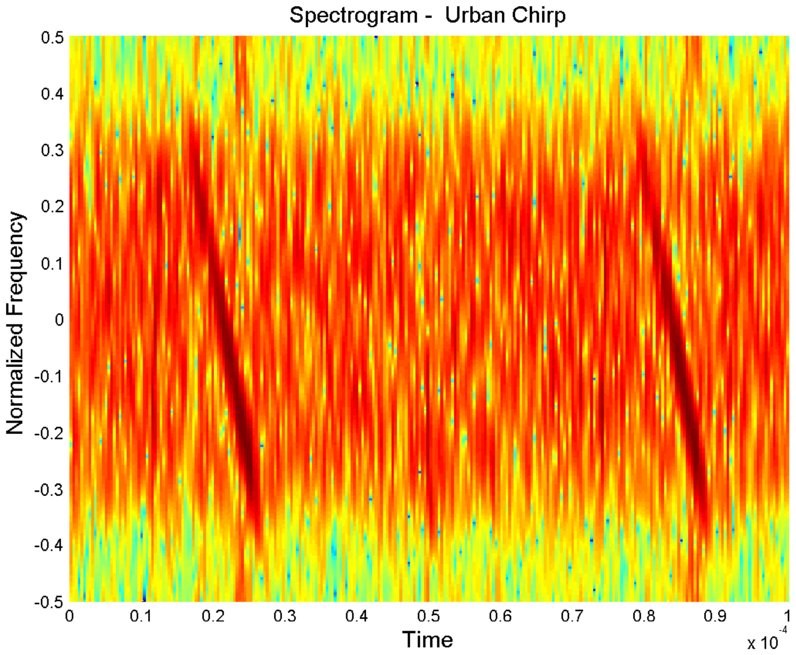


Figure 24: Spectrogram - Urban Chirp

In Figure 25, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It can be noticed that the algorithm recognizes the interferer bandwidth, and the detection becomes more and more accurate for increasing values of the power threshold. For a threshold $A = 2$ (green line), the recognized bandwidth ranges from $-0.35$to 0.35, and thus the whole bandwidth is detected. For a threshold $A = 4$ (black line), the detected bandwidth ranges from -0.3 to 0.28. For the last threshold, $A = 8$ (pink line), the bandwidth ranges from -0.28 to 0.26. It is worthwhile noticing that for increasing values of the power threshold the detected bandwidth decreases, thus enabling the detection of the most interfered part or the received signal.

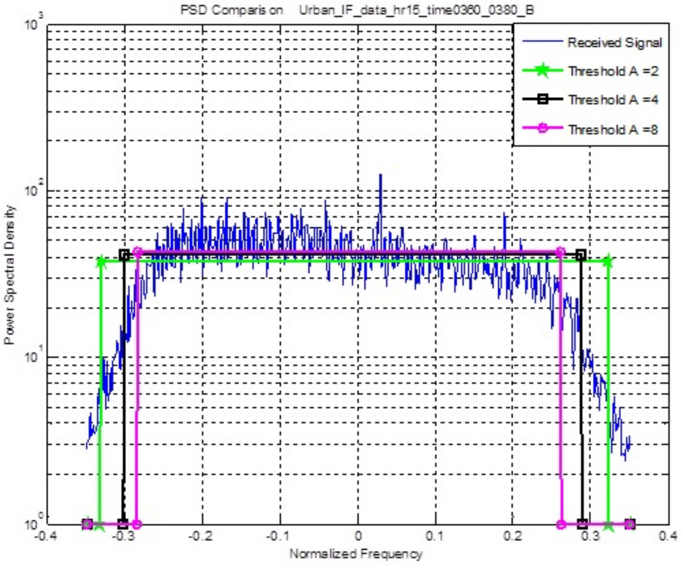


Figure 25: Comparison PSD with $L_{SP} = 400$

In Figure 26, the spectrogram of the signal *Urban_IF_Data_hr16_time0900_1000_B* is shown. In particular, four single tones with different powers are provided. The tones are in different frequency intervals: the most powerful is located in the interval $[0, 0.1]$ and the others, for decreasing power levels, are located in intervals $[-0.2, 0.1]$, $[0.2, 0.3]$, $[-0.3, -0.2]$, respectively.

In Figure 27, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. In this case, the detected bandwidths for each threshold value are overlapping, and only those corresponding to the highest threshold value, $A = 8$, are clearly visible. It can be noticed that the detected bandwidths are three, matching with those observable from the spectrogram. The most powerful single tone is detected inside the frequency interval $[0.02, 0.08]$, and the 2nd and 3rd in power single tone are recognized in the frequency intervals $[-0.15, -0.12]$ and $[0.2, 0.23]$, respectively. It is important to notice that only the lower power single tone is not detected. This behavior can be explained by noticing that its power does not cross over the considered lowest threshold value.

In Figure 28, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. In this case, the length of the shorter vector signal has been considered equal to 800 samples, corresponding to twice of that in the case shown in Figure 27. It is worth to notice that with a greater signal

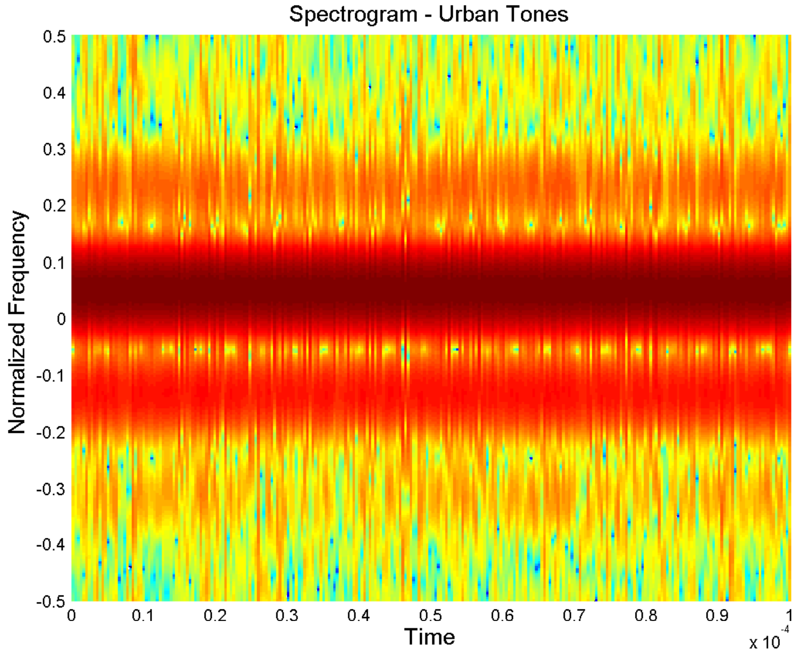


Figure 26: Spectrogram - Urban Tones

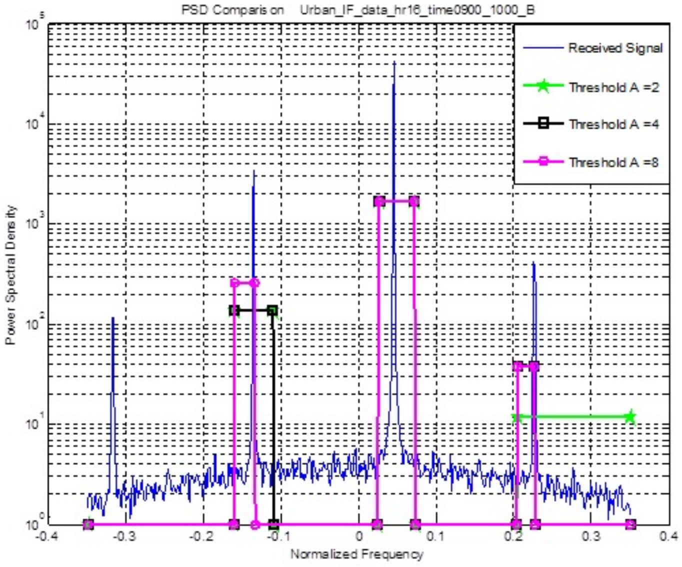


Figure 27: Comparison PSD with $L_{SP} = 400$

length the detection of the interferer bandwidth gets better than in the previous case. As a matter of facts, it is possible to define in a more accurate way the bandwidths of all the considered single tones and with respect to all the threshold values $A = [2, 4, 8]$, and consequently the detection errors decrease.

In Figure 29, the spectrogram of the signal *Urban_IF_Data_hr16_time3130_3330_B* is shown. Through the spectrogram it can be observed that the considered signal is a chirp waveform in the frequency interval $[-0.2, 0.45]$, with an uniform power.

In Figure 30, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. In

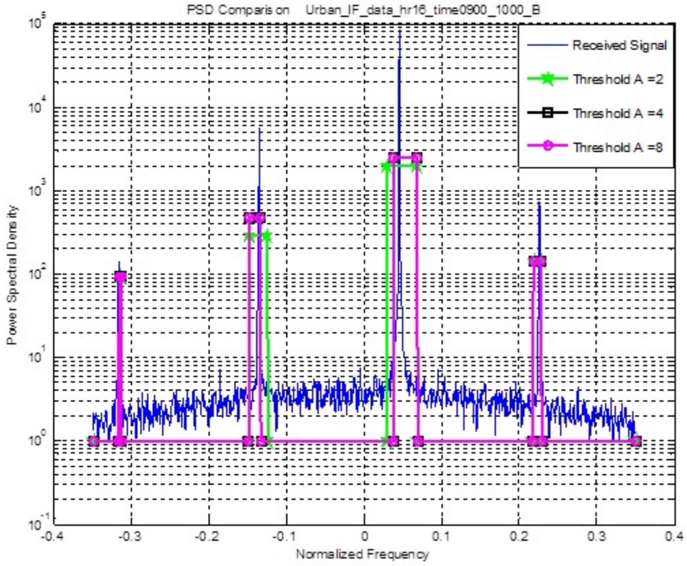


Figure 28: Comparison PSD with $L_{SP} = 800$

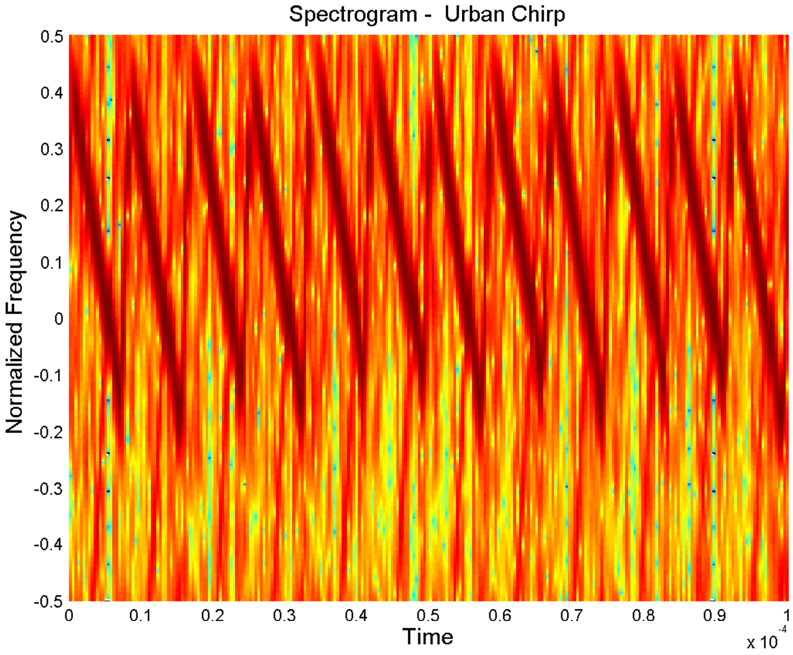


Figure 29: Spectrogram - Urban Chirp

this case, it must be taken into account that the signal is considered inside the interval $[-0.35, 0.35]$, which is twice the normalized bandwidth. Then, it can be noticed that for the threshold value $A = 8$ the algorithm accurately recognizes the interferer bandwidth, equal to $[-0.2, 0.35]$. The detection for the threshold value $A = 4$ is quite similar to the previous one with a small error in the lower bound of the interfered interval. For the threshold value $A = 2$ the detection is not reliable because the whole normalized bandwidth has been detected.

In Figure 31, the spectrogram of the signal *Urban_IF_Data_hr18_time2840_2860_B* is shown. Through the spectrogram it is possible to ob-

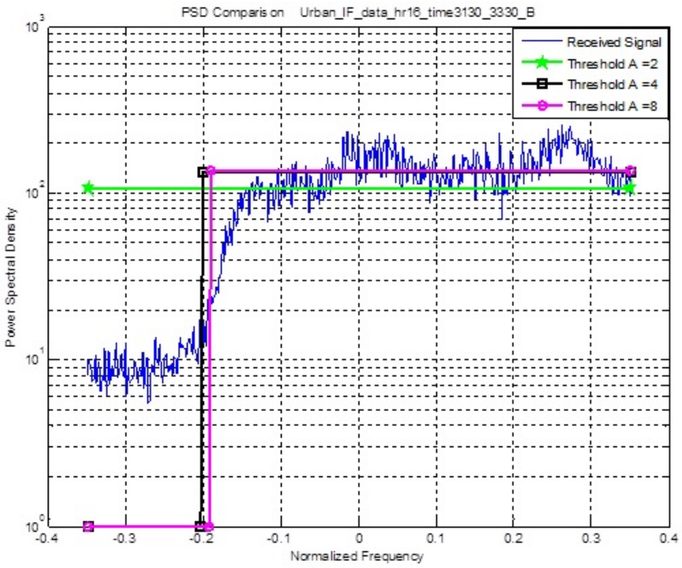


Figure 30: Comparison PSD with $L_{SP} = 400$

serve that the considered signal is a chirp waveform in the frequency interval $[-0.2, 0.45]$, with an uniform power.

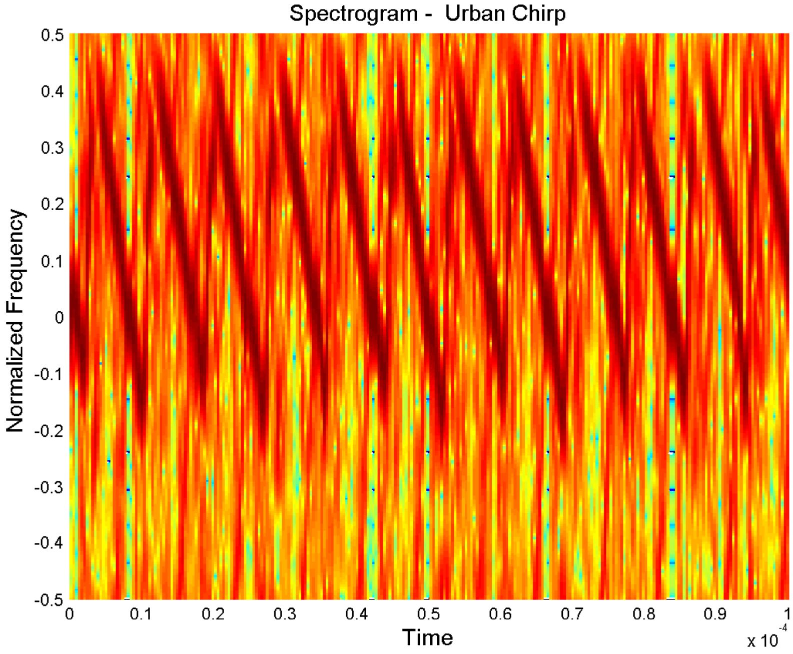


Figure 31: Spectrogram - Urban Chirp

In Figure 32, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. This case is similar to the previous one, and here it must be taken into account that the signal is considered inside the interval $[-0.35, 0.35]$ as well, which is fixed at twice the normalized bandwidth. Thus, for the threshold value $A = 8$ the algorithm accurately recognizes the interferer bandwidth, which is the range $[-0.2, 0.35]$. The result for the threshold value $A = 4$ is a slightly less accurate than the previous one. For the lowest threshold value $A = 2$ the detection is not reliable because the whole normalized bandwidth has been detected.

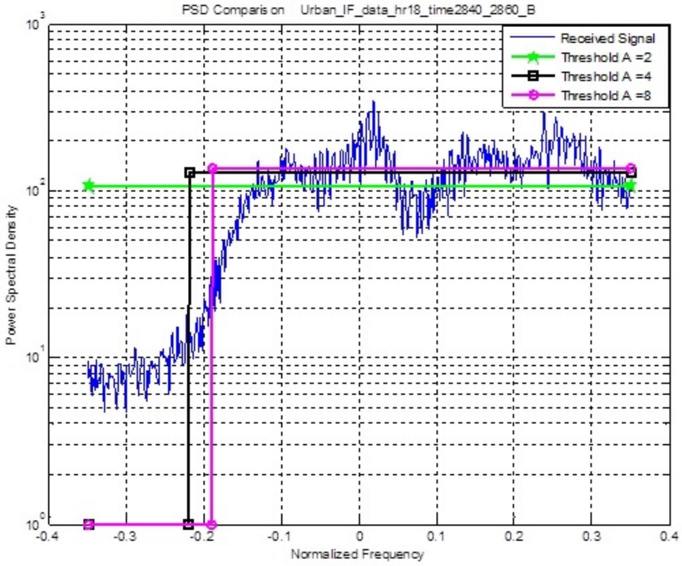


Figure 32: Comparison PSD with $L_{SP} = 400$

In Figure 33, the spectrogram of the signal *Urban_IF_Data_hr20 _time0065_0085_B* is shown. In this case, the spectrum is not clearly visible: there are several interferer events in two frequency intervals in the larger range $[-0.3, -0.1]$. Something else is present in the interval $[-0.1, 0.3]$. However, it has a lower power than the others interferer events.

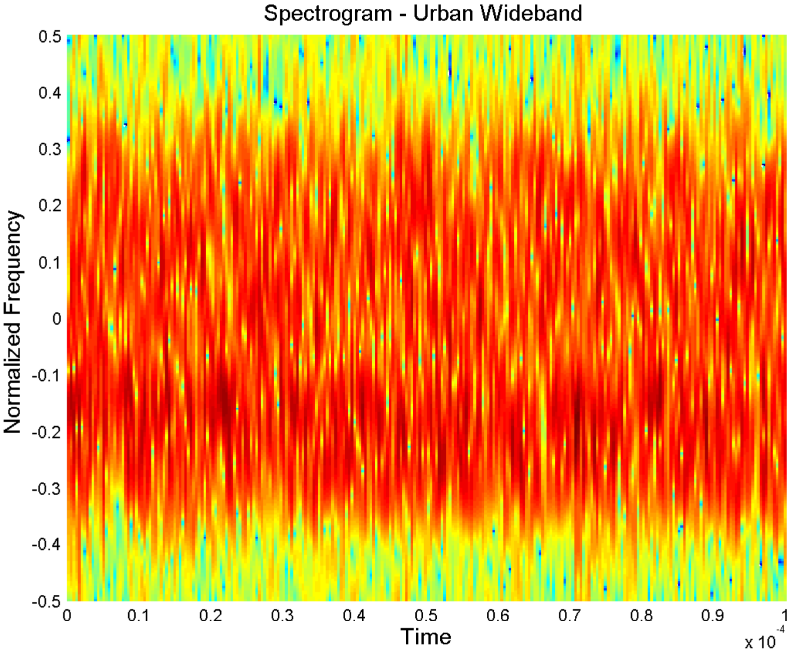


Figure 33: Spectrogram - Urban Wideband

In Figure 34, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown.

For the threshold value $A = 8$ the algorithm recognizes the interferer intervals $[-0.31, -0.24]$, $[-0.23, -0.12]$ and $[-0.11, 0.16]$, exception made for the pick due to the noise. The detection is reliable even if the interferer spectrogram is not clearly visible. For the threshold values $A = 4$ and $A = 2$ the identified interferer bandwidths are quite similar, and range from -0.32 to 0.28 and from -0.32 to 0.31, respectively. In these cases the results of the algorithm are not reliable.

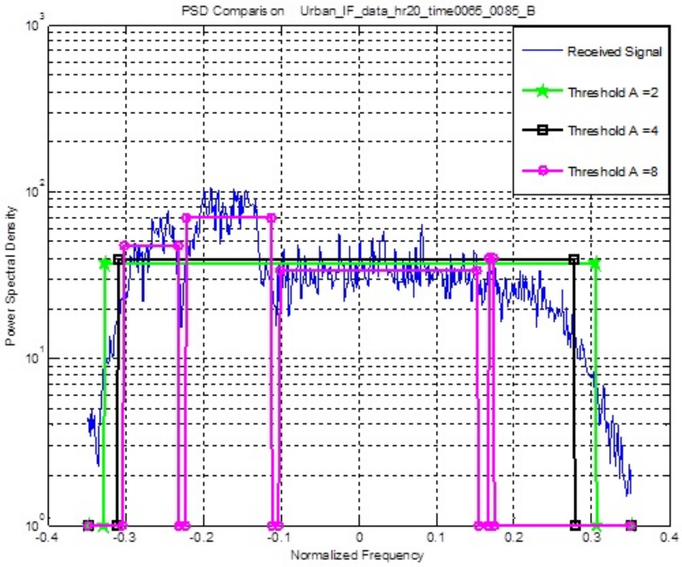


Figure 34: Comparison PSD with $L_{SP} = 400$

In Figure 35, the spectrogram of the signal *Urban_IF_Data_hr22 _time1560_1600_B* is shown. The represented spectrum is not clear: there are several interferer events distributed in the entire normalized bandwidth.

In Figure 36, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For all the threshold values, $A = [2, 4, 8]$, the algorithm detects only one interferer band, which becomes smaller by increasing the threshold value. In this case, as the previous one, the detection is not reliable due to the fact that the interferer behavior is not well defined.

In Figure 37, the spectrogram of the signal *Urban_IF_Data_hr24_ time2140_2200_B* is shown. Three principal interferer bands can be observed, in which the interferer power is higher than in the other frequencies belonging to the normalized bandwidth. These intervals are $[0.2, 0.3]$, $[0, 0.1]$, $[-0.25, -0.13]$.

In Figure 38, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For the threshold value $A = 8$ the algorithm recognizes only two interfered intervals $[-0.31, -0.12]$, $[-0.09, 0.34]$. For the lower threshold values $A = 4$ and $A = 2$ the algorithm results are not very accurate because the identified bandwidths cover the entire normalized bandwidth, thus not recognizing the interferer events.

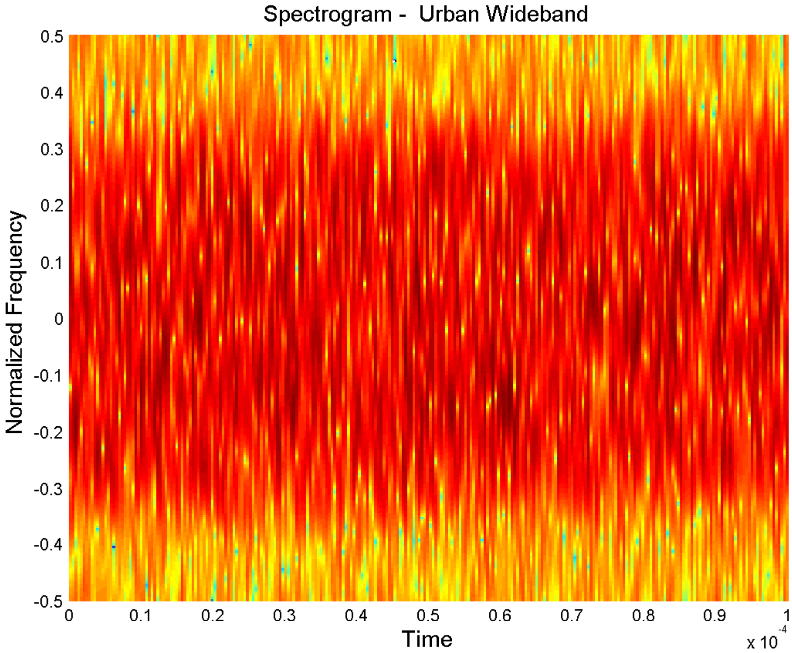


Figure 35: Spectrogram - Urban Wideband

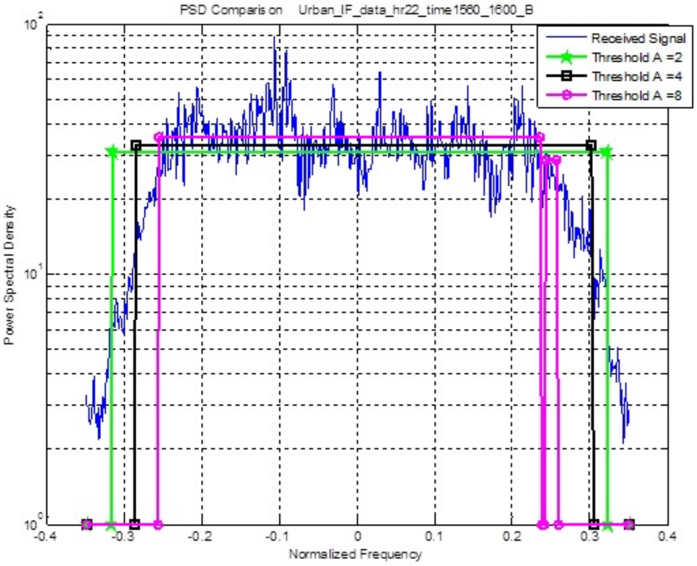


Figure 36: Comparison PSD with $L_{SP} = 400$

In Figure 39, the spectrogram of the signal *Urban_IF_Data_hr29_time1415_1455_B* is shown. Three single tones are present, each with different power. The tones are in different frequency intervals: the most powerful is located in the interval $[-0.09, 0.1]$ and the others, in decreasing order of power, are located in intervals $[0.15, 0.28]$, $[-0.35, -0.29]$, respectively.

In Figure 40, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For the threshold value $A = 8$ the algorithm detect only two interfered bands, the most powerful in the frequency interval $[-0.09, -0.04]$ and the second, in terms of power, in the interval $[0.18, 0.2]$. The single

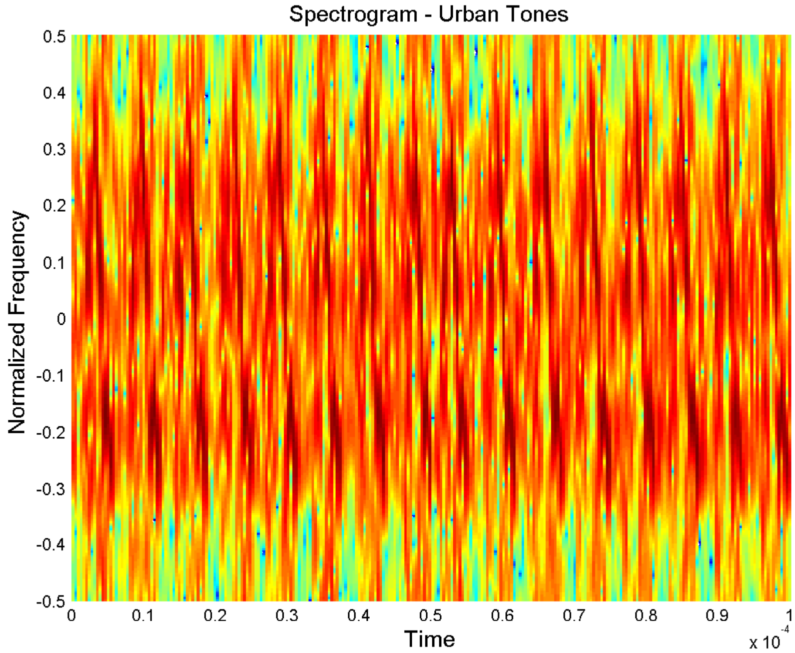


Figure 37: Spectrogram - Urban Wideband

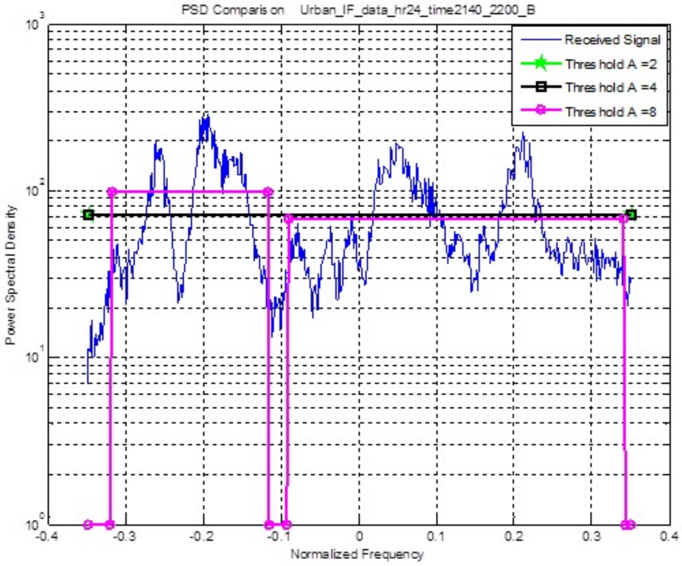


Figure 38: Comparison PSD with $L_{SP} = 400$

tone with lowest power is not detected. For threshold values $A = 2$ and $A = 4$ the results are quite similar to each other and are actually the same to which detected with the highest threshold value. Only the results for $A = 8$ can be noticed due to overlapping. The difference is that with a lower threshold it is also possible to detect the bandwidth of the lowest power single tone, which is recognized in the frequency interval $[-0.35, -0.32]$.

In Figure 41, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. In this case, the length of the shorter vector signal has been considered equal to 800 samples, corresponding to twice of the case shown in

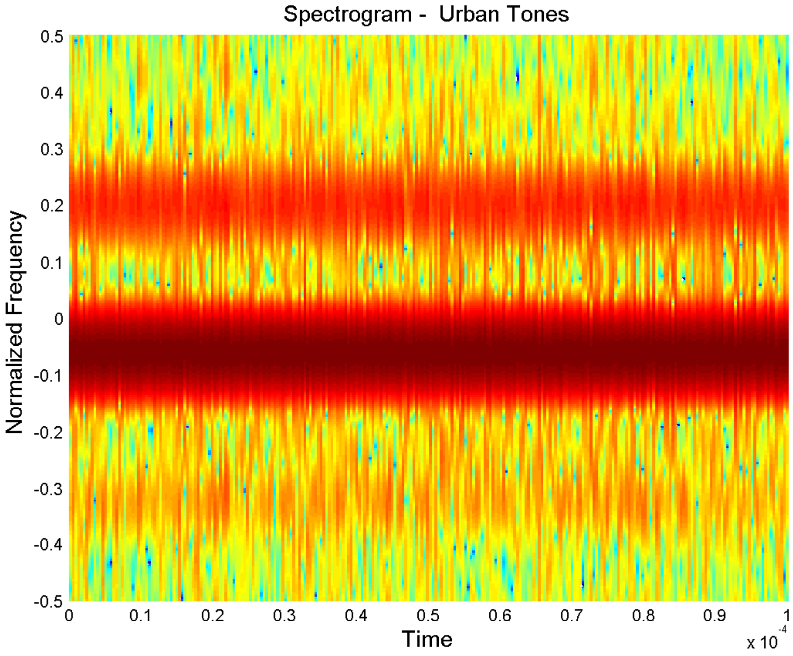


Figure 39: Spectrogram - Urban Tones

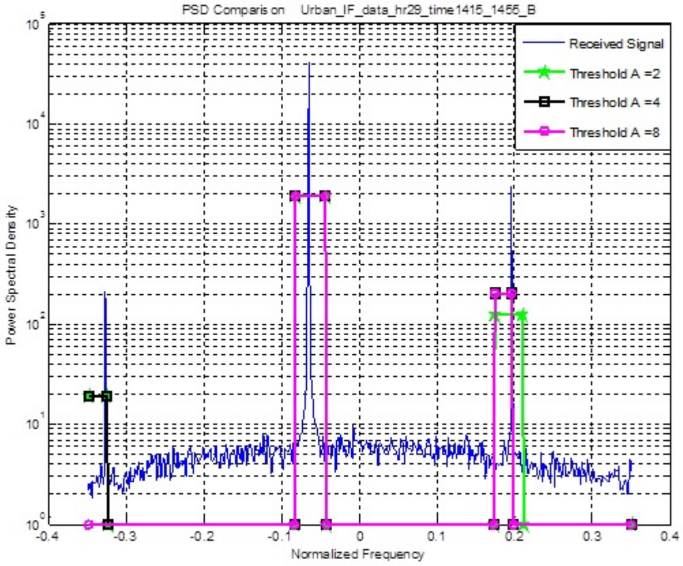


Figure 40: Comparison PSD with $L_{SP} = 400$

Figure 40. It is worth to notice that with a greater signal length, the detection of the interferer bandwidth gets better than in the previous case. As a matter of facts, it is possible to define in a more accurate way the bandwidths of all the considered single tones and with respect to all the threshold values $A = [2, 4, 8]$, and consequently the error in the detection decreases.

In Figure 42, the spectrogram of the signal *Urban_IF_Data_hr31 _time3260_3350_B* is shown. The represented spectrum is not clear: there are several interferer events distributed in all the normalized bandwidth.

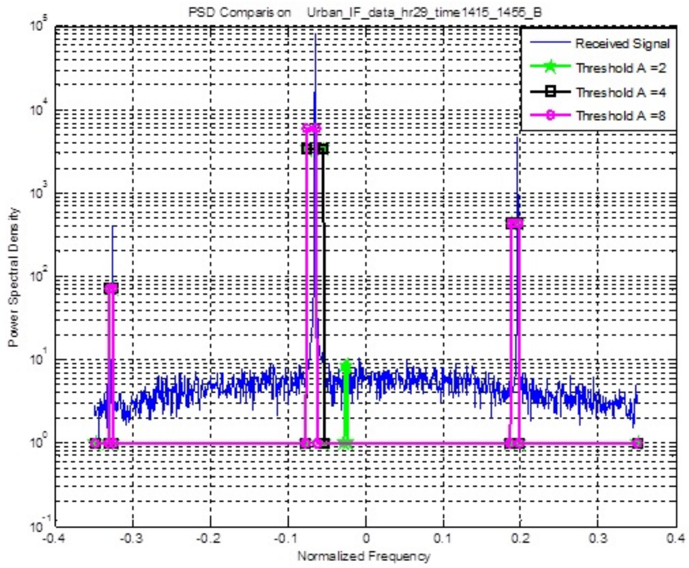


Figure 41: Comparison PSD with $L_{SP} = 800$

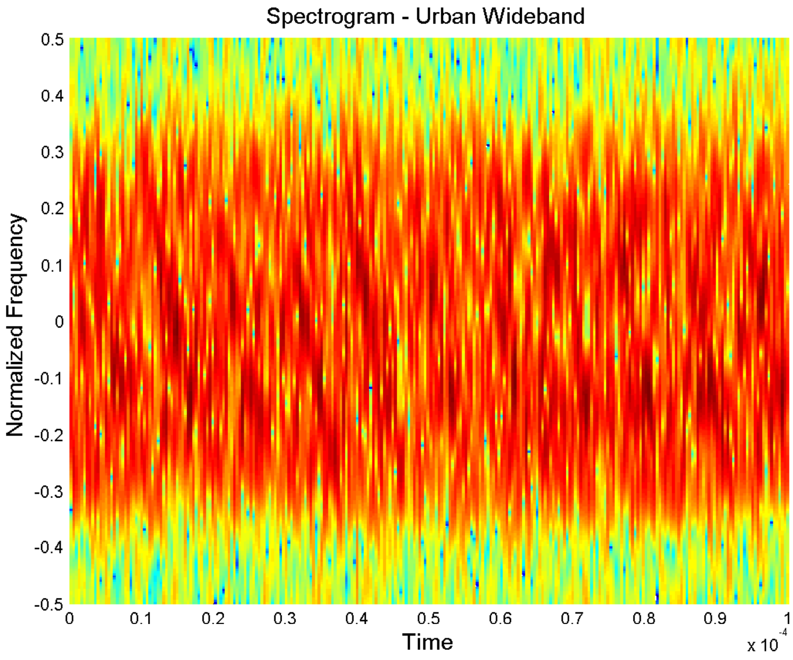


Figure 42: Spectrogram - Urban Wideband

In Figure 43, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For threshold values $A = [2, 4]$, the algorithm detects only one interferer band, which becomes smaller by increasing the threshold value. For the threshold value A=8 there are two detected interfered bands located in the intervals $[-0.28, -0.23]$ and $[-0.22, 0.22]$. In this case, as for the previous signals, the detection is not so reliable due to the fact that the interferer behavior is not well defined.

In Figure 44, the spectrogram of the signal *Urban_IF_Data_hr32_time3120_3220_B* is shown. Through the spectrogram it is possible to observe that the considered signal is a chirp waveform in the frequency

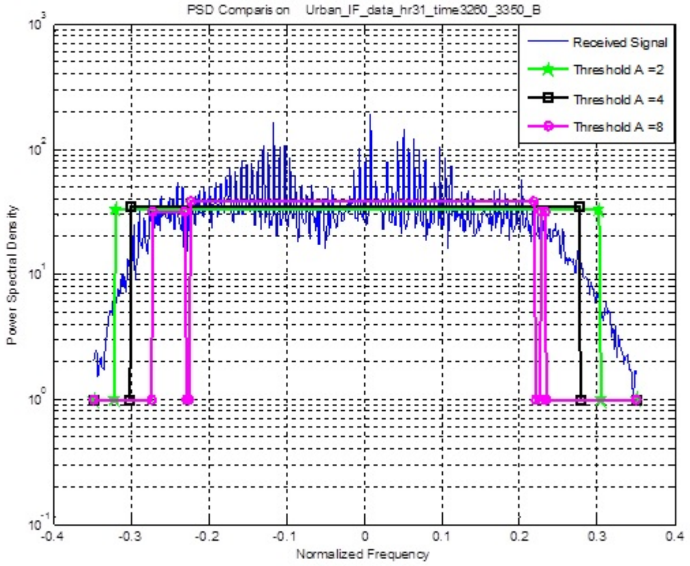


Figure 43: Comparison PSD with $L_{SP} = 400$

interval $[-0.35, 0.25]$, with an uniform power. Furthermore, a lower interferer event is present in the frequencies closer to the end of the normalized bandwidth.

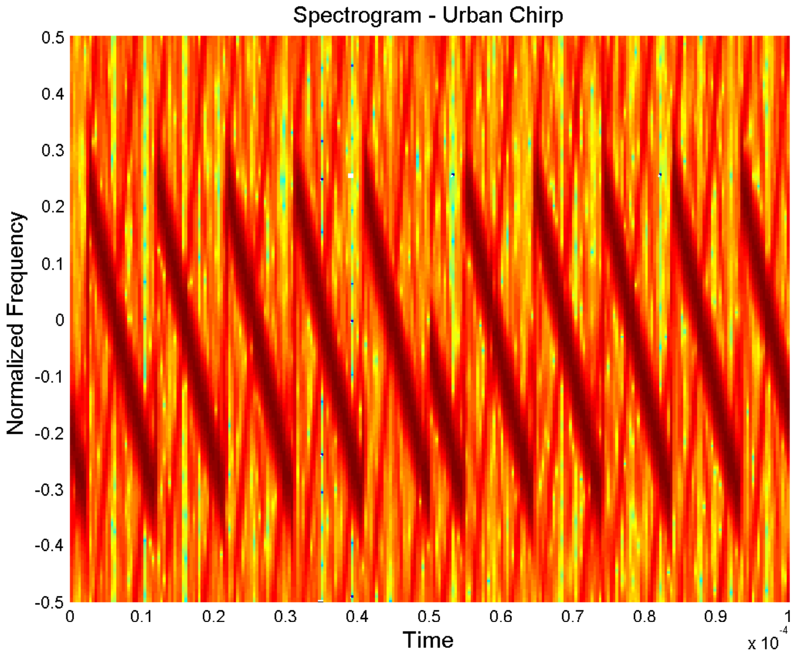


Figure 44: Spectrogram - Urban Chirp

In Figure 45, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It is possible to notice that for the threshold value $A = 8$ the algorithm accurately recognizes the interferer bandwidth in the interval $[-0.35, 0.25]$, while the lower interferer bandwidth is not recognized. The detection for the threshold value $A = 4$ is quite similar to the previous one. Moreover, the detection of the lower interference events in the frequency interval $[0.32, 0.34]$ is provided. For the threshold value $A = 2$ the detection is not reliable because the whole normalized bandwidth has been detected.

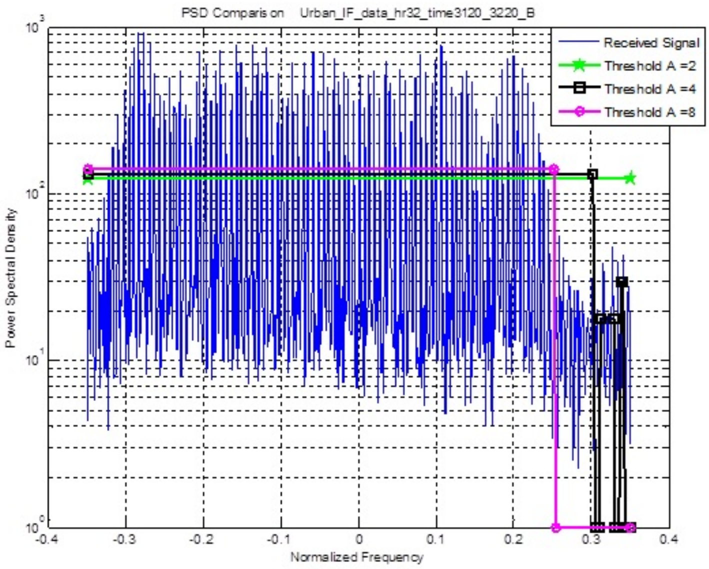


Figure 45: Comparison PSD with $L_{SP} = 400$

In Figure 46, the spectrogram for the signals *Urban_IF_Data_hr34_time0605_0625_B* is shown. The interferer signal is a chirp signal occupying the entire normalized bandwidth. It can also be noticed that the interference presents a light lack of power, thus determining three sub-bands in the intervals $[-0.35, -0.1]$, $[-0.09, 0.05]$ and $[0 - 06, 0.25]$.

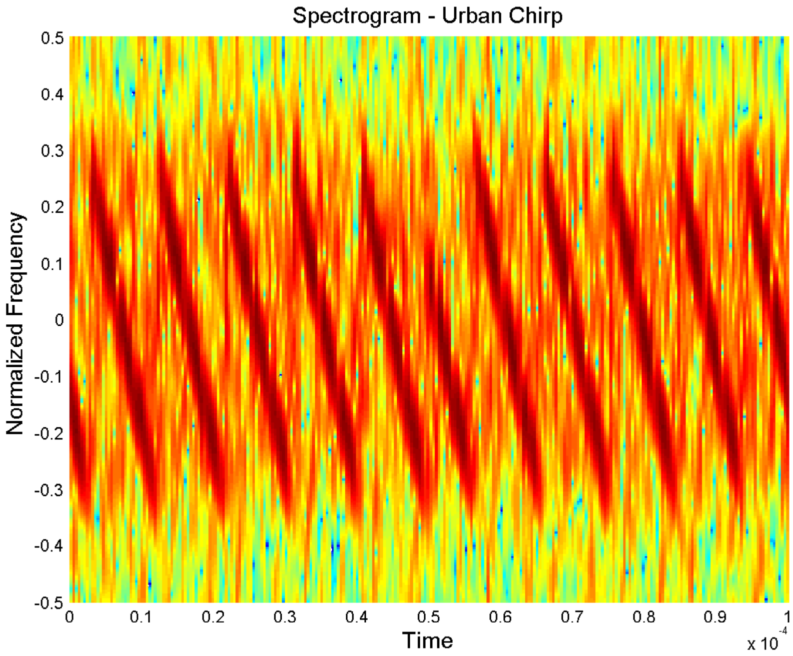


Figure 46: Spectrogram - Urban Chirp

In Figure 47, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It is possible to notice that for the threshold value $A = 8$ the algorithm recognizes, the interferer bandwidth in the three sub-intervals $[-0.28, -0.12]$, $[-0.09, 0.03]$ and $[0.06, 0.25]$, with limited errors. The results for threshold values $A = 4$ and $A = 2$ are similar, and the detection is not reliable because the entire normalized bandwidth has been detected.

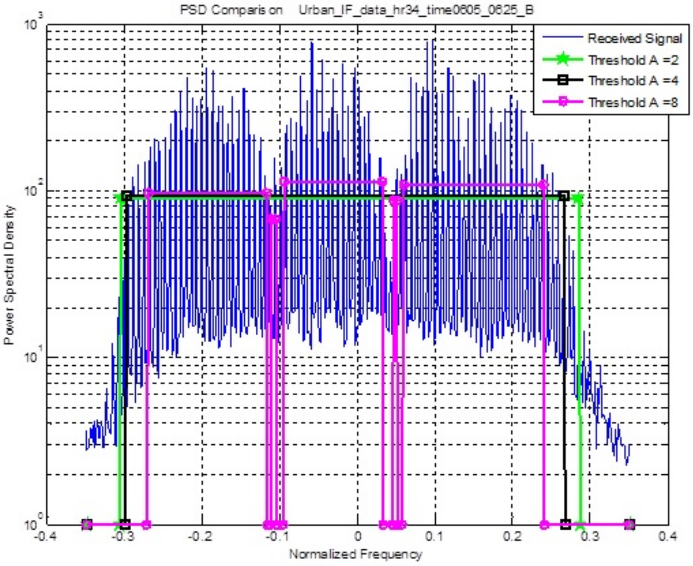


Figure 47: Comparison PSD with $L_{SP} = 400$

In Figure 48, the spectrogram of the signal *Urban_IF_Data_hr38 _time1850_1870_B* is shown. The represented spectrum is not clear: there are several interferer events distributed in all the normalized bandwidth.

In Figure 49, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For all the threshold values, $A = [2, 4, 8]$, the algorithm detects only one interferer band, which becomes smaller when increasing the threshold value. In this case, as seen for previous signals, the detection is not completely reliable due to the fact that the interferer behavior is not well defined.

In Figure 50, the spectrogram of the signal *Urban_IF_Data_hr3 8_time1900_1920_B* is shown. It is possible to look at three single tones, with different powers. The tones are in different frequency intervals: the most powerful is collocated in the interval $[-0.09, 0.02]$ and the others, in decreasing order of power, are collocated in intervals $[0.1, 0.25]$, $[-0.2, -0.3]$.

In Figure 51, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. For the threshold value $A = 8$ the algorithm detect only two interfered bands, the most powerful in the frequency interval $[-0.08, -0.04]$ and the second, in terms of power, in the interval $[0.14, 0.17]$. The

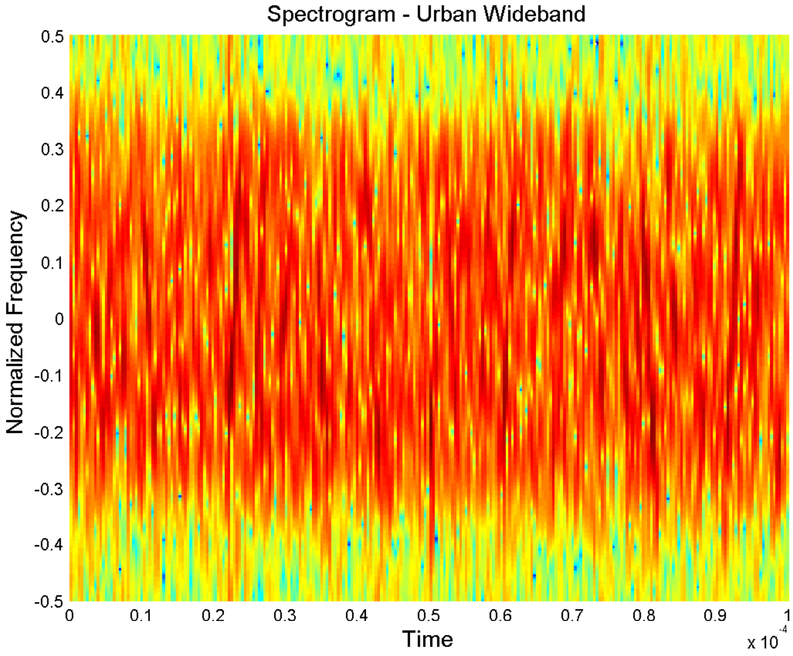


Figure 48: Spectrogram - Urban Wideband

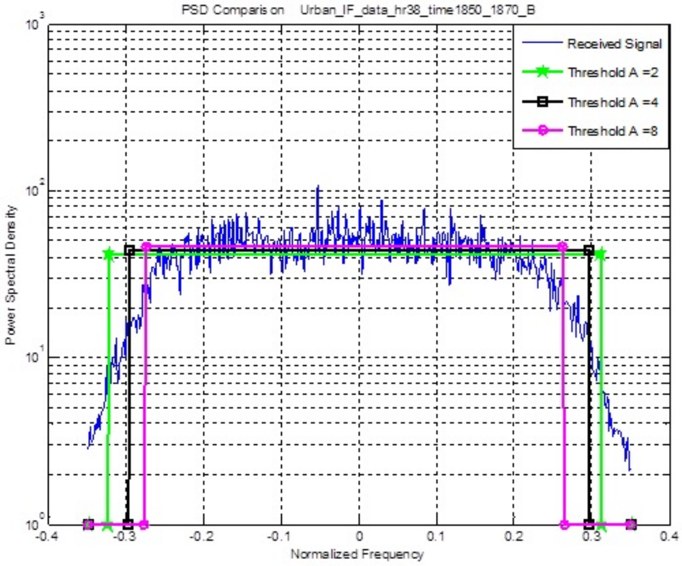


Figure 49: Comparison PSD with $L_{SP} = 400$

single tone with lowest power is not detected. For threshold values $A = 2$ and $A = 4$ the results are similar to each other, and are also the same to the highest threshold value case. Only the results for $A = 8$ can be noticed, because there is overlapping. The difference is that with lower thresholds it is also possible to detect the bandwidth of the lowest power single tone, which is recognized in the frequency interval $[-0.35, -0.26]$ with a larger band than that defined in the spectrogram.

In Figure 52, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. As in the previous cases, the length of the shorter vector signal has

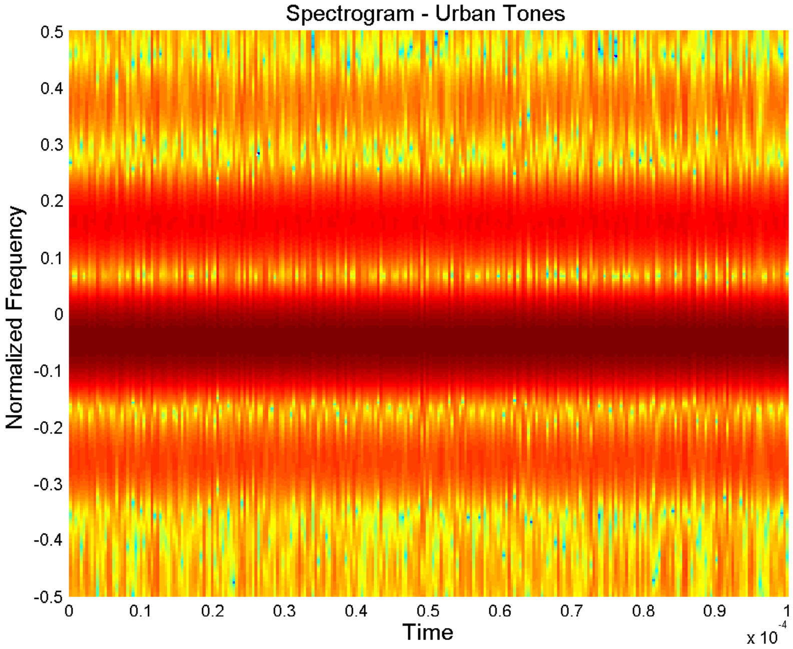


Figure 50: Comparison PSD with $L_{SP} = 400$

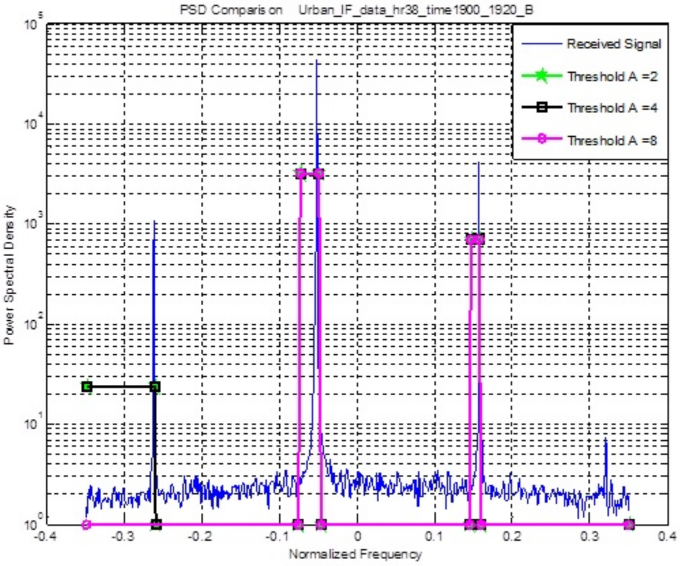


Figure 51: Comparison PSD with $L_{SP} = 400$

been considered equal to 800 samples, corresponding to twice of the case shown Figure 51. Also in this case, it is possible to notice that the detection of the interfered bandwidths gets better than the previous case. As a consequence, it is possible to define in a more accurate way the bandwidths of all the considered single tones and with respect to all the threshold values $A = [2, 4, 8]$, with smaller errors. In order to explicitly show the improvement on narrowband peak identification thanks to longer observation spans, detection performance has been tested with L_{SP} as a parameter, and results are shown in Figure 53.

The considered signal is the *Urban_IF_Data_hr38_time1900_1920_B* and the threshold value A has been set equal to 4. In this case the

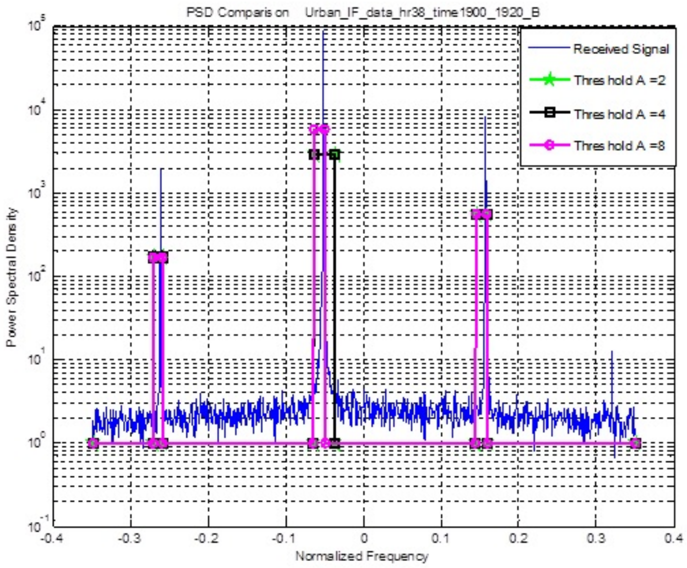


Figure 52: Comparison PSD with $L_{SP} = 400$

representation of graph lines is inverted with respect to the previous figures, so that it is possible to distinguish in a better way the lines representing the received signal with different lengths L_{SP}. It is worth to notice that increasing the parameter L_{SP} a more accurate estimation of the interfered bandwidths is evaluated. As shown in the figure, the bandwidth estimation with L_{SP} equal to 800 (red line with star marker) is closer to the real interferer bandwidths than those evaluated for L_{SP} equal to 400 (black line with square marker) and 200 (green line with asterisk marker). The detection performed with $L_{SP} = 800$ is accurate for the all interferer events. On the contrary, the detections evaluated with $L_{SP} = 400$ and $L_{SP} = 200$ are less precise, defining larger bandwidths than the real ones, in particular for the less powerful tone.

In Figure 54, the spectrogram for the signals *Urban_IF_Data_hr41_time2160_2190_B* is shown. The interferer signal is a chirp signal which occupies all the normalized bandwidth $[-0.3, 0.3]$.

In Figure 55, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It is possible to notice that for all the threshold values $A = [2, 4, 8]$ the algorithm recognizes the whole normalized bandwidth.

In Figure 56, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. As in the previous cases, the length of the shorter vector signal has been considered equal to 800 samples, corresponding to twice of the case show Figure 55. In this case, it is possible to notice that the detection of the interfered bandwidths is not particularly different to the case with 400 samples. Thus, it can be deduced that increasing the parameter L_{SP} does not affect the detection accuracy of the interfered bandwidths unlike single tones detection, as verified in Figure 28, Figure 41, Figure 52.

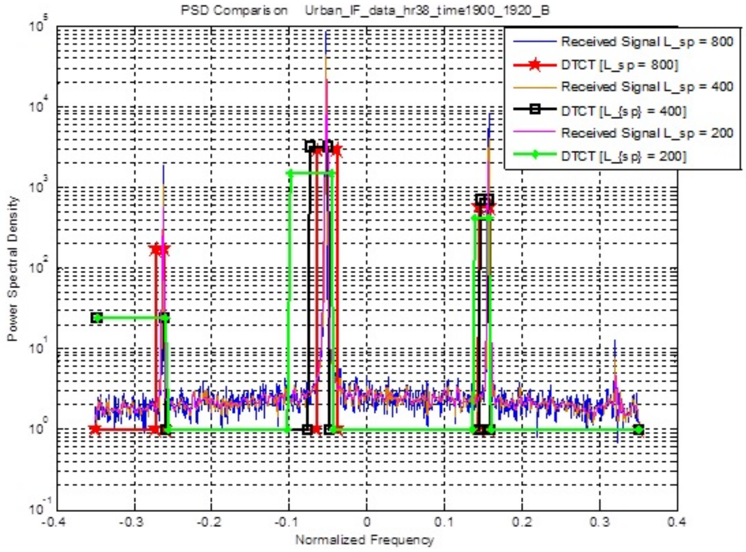


Figure 53: Detection Test with $A = 4$ and $L_{SP} = [200, 400, 800]$

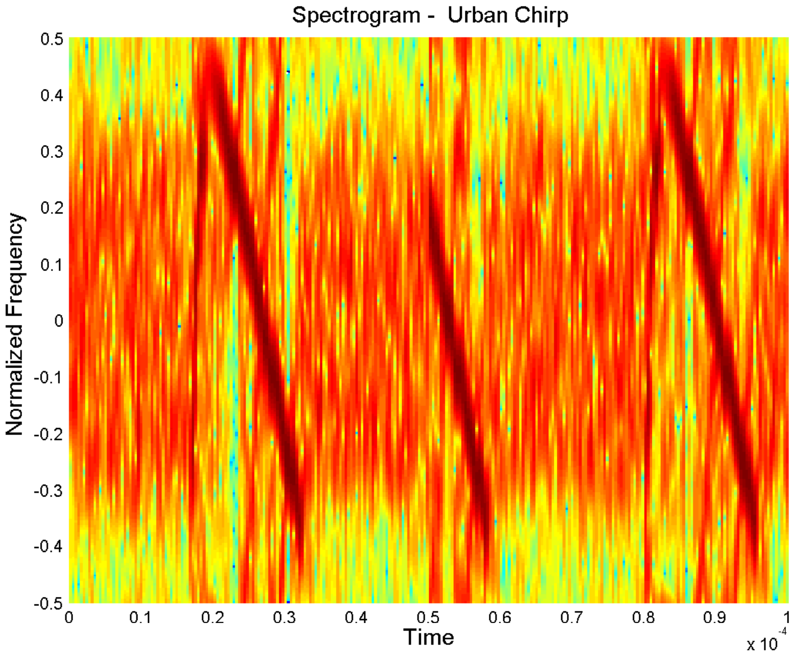


Figure 54: Spectrogram - Urban Chirp

In Figure 57, the spectrogram for the signals *Urban_IF_Data_hr42_time1810_1830_B* is shown. The interferer signal is uniformly distributed in the entire normalized bandwidth $[-0.3, 0.3]$, except for the interval $[0, 0.09]$ which seems to be a single tone.

In Figure 58, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It is possible to notice that for the threshold value $A = 8$ the detection is not much accurate because the identified interferer bandwidth ranges from -0.22 to 0.21. The performance gets worse with threshold values $A = 4$ and $A = 2$ because the recognized interferer band is quite equal to the normalized bandwidth.

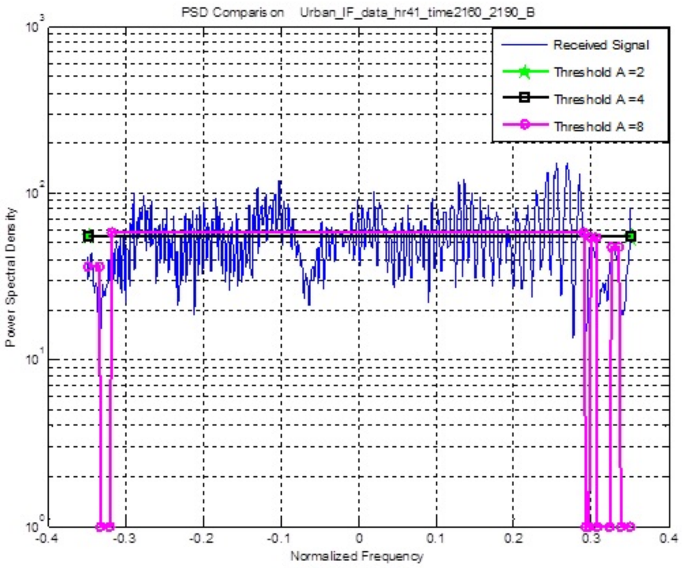


Figure 55: Comparison PSD with $L_{SP} = 400$

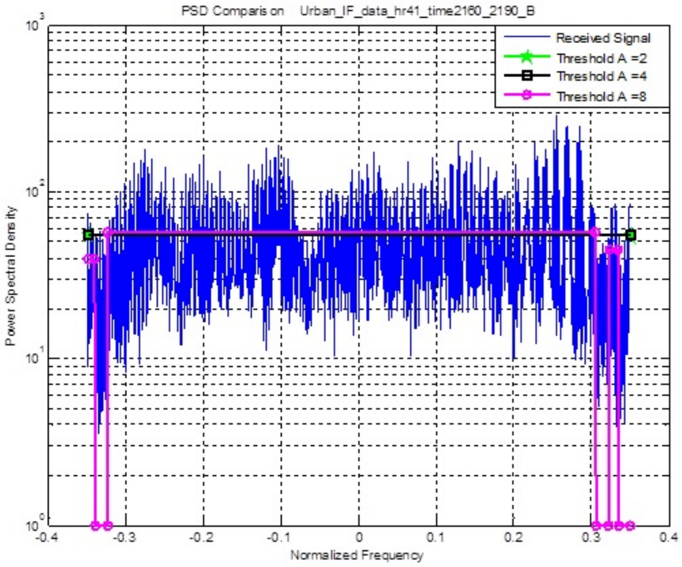


Figure 56: Comparison PSD with $L_{SP} = 400$

In Figure 59, the spectrogram for the signals *Urban_IF_Data_hr51_time2880_2900_B* is shown. The interferer signal is not clearly visible and it presents high power values in the frequency interval $[0, 0.3]$ and a lower power in the interval $[-0.3, 0]$.

In Figure 60, the comparison between the power spectral density of the signal and the results of the Burst Detector algorithm is shown. It is possible to notice that for threshold value $A = 8$ the detection is not more accurate than that for threshold values $A = 4$ and $A = 2$, but the detected bandwidth is quite similar in all the cases, without recognizing the most powerful interference bandwidth.

Finally, it can be stated that the Bandwidth Detection algorithm works properly in all the analyzed cases and that it can be efficiently

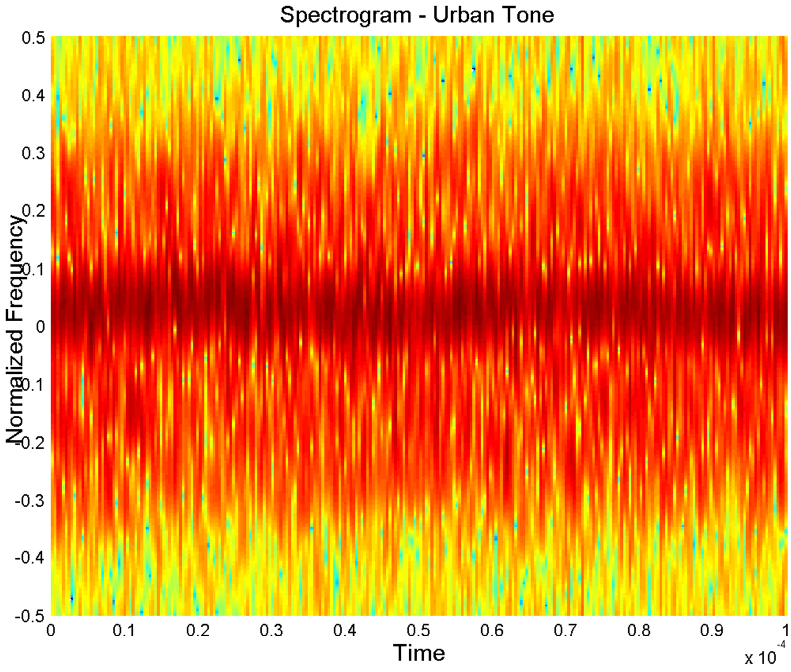


Figure 57: Spectrogram - Urban Wideband

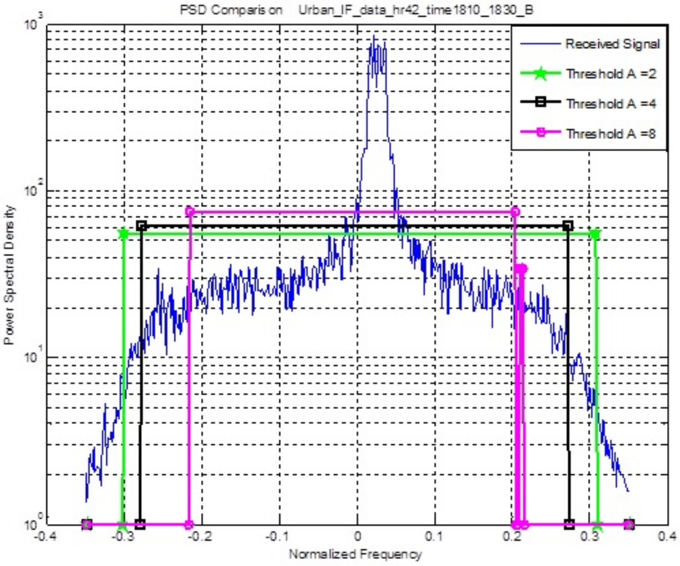


Figure 58: Comparison PSD with $L_{SP} = 400$

adopted to recognize the interfered bands inside the received signal spectrum. It is worthwhile noticing that the power threshold A significantly affects the performance of the algorithm: low thresholds often lead to better results for narrowband signals, but they are less accurate in case of wide bandwidth interferers. In general, the mean value $A = 4$ seems to constitute a valid trade-off, and it is recommended for future implementation purposes.

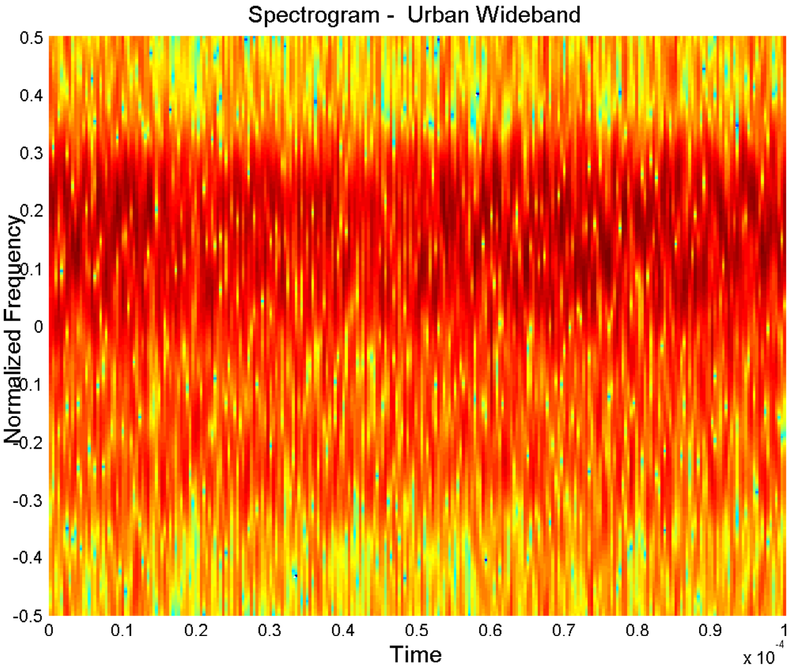


Figure 59: Spectrogram - Urban Chirp

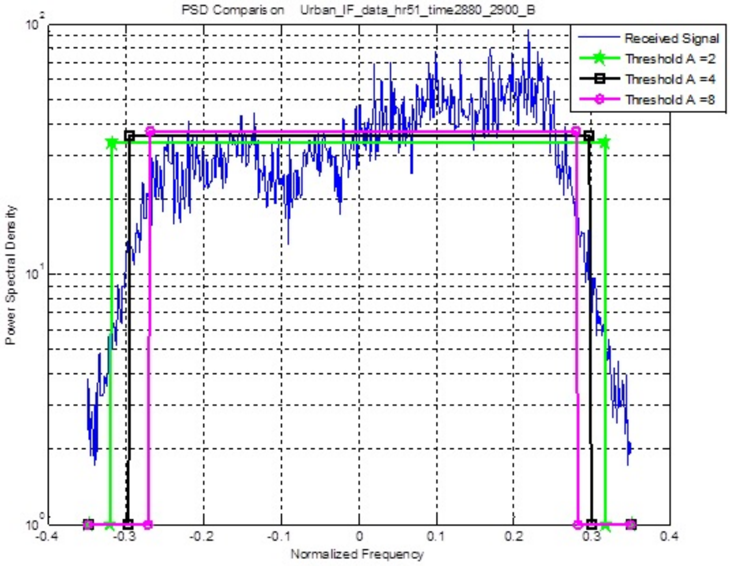


Figure 60: Comparison PSD with $L_{SP} = 400$

1.6 CONCLUSIONS

For the Bandwidth Detection algorithm an update has been provided in order to account for the front-end bandwidth limitation effects and for the sampling rate, which could excessively increase the computational complexity: by observing the spectrograms of the real interferer signals, it has been possible to verify that all the signals occupy 70% of the Front-End bandwidth, thus, only the most significant part of the spectrum $[-B_N, B_N]$, must be considered. Then, a down-sampling of the received signal is performed, obtaining a new shorter signal vector with a signal length equal to the desired L_{SP}, which allows the WT to be evaluated with a smaller complexity. The Band Detection algorithm has been tested with measured signals, collected in an urban scenario. Performance is evaluated through graphical results because prior knowledge on the interferer nature is lacking. It is possible to verify the correct behavior of the proposed algorithm comparing its result to the spectrogram. It is worth highlighting that the correct detection of the interferer bands strictly depends on two principal parameters: the threshold A and the length L_{SP}, which is the length of the observed signal after down-sampling. As shown in the numerical results, increasing the threshold value A leads to more accurate estimation of interfered bandwidths. Furthermore, for narrowband interference, the algorithm sensitivity on L_{SP} is stronger than that on the threshold A, and increasing this parameter significantly affects performance. This is due to the fact that the number of scale factors N_s depends on L_{SP}, and in particular the duration of the Haar wavelet function is inversely proportional to the square root of the maximum scale factor a_{max}, while the amplitude is proportional to its square root. In particular increasing L_{SP} leads to the following effects: a_{max} becomes larger; ii) the Haar function becomes more peaked; and iii) the scalar product inside the WT accordingly becomes more significant for peaked signals, allowing correct identification of frequency location of narrowband tones. Therefore, it is possible to state that increasing L_{SP} leads to the correct identification of frequency location of narrowband tones, with less errors in the estimation of interfered bandwidths.

The described WT based algorithm has been also applied in the time-domain in order to characterize the signal duty-cycle, i. e.the time interval in which the jamming signal is active or not. The main difference with respect to the previously presented application consists in the evaluation of the power envelope of the signal (instead of the PSD) and in this case the time characteristics must be obtained. The algorithm provides information on both the burst localization and on the duty-cycle values. Numerical results have shown that a good estimation of the signal duty cycle can be obtained, with an increasing reliability for shorter duty cycle values.

2 GNSS JAMMER IN MULTIPATH SCENARIO

2.1 INTRODUCTION

As explained previously in Chapter 1, the aim of GNSS jammers is to deny the correct reception of navigation signals, and as such they represent one of the dominant threats to GNSS services and in particular of their availability. There is a clear necessity for techniques and algorithms to enhance the robustness to jammers in GNSS receivers, the best option being the ability to isolate and cancel out the interfering signal. Considering land mobile GNSS applications, usually the jammer will be located on the earth surface and direct visibility to the target will only be sporadic, inasmuch as propagation will be enriched by multiple reflection, diffraction, and absorption effects. Therefore, the interfering signal will typically reach the GNSS antenna through a multipath channel, possibly without a line-of-sight, and the receiver will be faced with a number of malicious echoes generated by the channel power delay profile, which render interference cancellation a phenomenal task. In this chapter, starting from the Interference Characterization and Cancellation (ICC) algorithm proposed in [P4][Pr1] and exhaustively described in [28], we present a solution to the problem of cancelling GNSS jammer signals affected by multipath which is both effective and computationally efficient. Specifically, we refer to interfering attacks by means of personal devices, as evidenced in several measurement campaigns [30][48][12], which present a periodic and structured autocorrelation function. In the absence of multipath, this structure is static and can be exploited to estimate an effective interference reference period upon which the ICC algorithm can be applied. This is all very well, but assuming a non-frequency selective channel is rather optimistic, as we clarified above. Moving from these results, the extension to the multipath scenario can be an interesting case. Exploring the literature on multipath effects on GNSS receivers, it is immediate to observe that, while it is recognized that multipath is a critical issue in the development of high-performance GNSS applications and reducing its adverse effects is a priority, the attention has been focused almost entirely on the consequent impact on desired GNSS signals and/or on PVT calculation[84][1][64][3]. Extremely rare are those who considered the fragmentation of interference due to dispersed power delay profiles; in [2] space-time adaptive processing techniques are used to mitigate the presence of GNSS interference in a multipath environment. It could appear that the solution might entail a simple replication in parallel of the ICC algorithm into a sufficient number of branches to match the population of significant multipath components. This is one case where simplicity of ideation is opposed to simplicity of implementation. The main idea of this approach comes from recognizing that propagation through a time-dispersive channel will not destroy, but rather transform, the auto-correlation structure of a waveform. Certainly, the transformation will be dynamic, with characteristic time-constants that depend on the trajectory of both the jammer and its target receiver. However, it will always be possible to limit the observation window to time intervals characterized by the fact that the interference auto-correlation structure is quasi-static: here, estimation of an effective echoed-interference reference period is again possible, using approaches which are completely similar to the purely static case, without any resort to parallelization. Moving along these lines of thought, we have extended the already proposed ICC [P4] algorithm into an *Echoed-Interference Characterization and Cancellation* (EICC) version. The attention is mainly focused on the interfering signal affected by multipath propagation neglecting the useful GNSS signal.

The chapter is organized as follows. In Section 2.2 the system model is presented; in Section 2.3 the algorithm is described, highlightening its principal operations and functionalities and complexity evaluation; in Sections 2.4 and 2.5 the applications in LOS and *Multipath* scenarios are presented, both validated by numerical results. Finally, concluding remarks are reported in Section 2.6.

2.2 SYSTEM MODEL

Measurement campaigns described in literature have shown that the most common GNSS jamming signals are angle modulated carriers [48]. These interferers contain a core with a periodic behaviour,*i.e.* they have a waveform that repeat itself periodically in time. Thus, current interfering signals can be expressed as:

$$s_{FM}(t) = A\exp\left\{j2\pi\left(f_0 t + \int_{-\infty}^{t} z(\xi)d\xi\right)\right\} \tag{12}$$

$$s_{PM}(t) = A\exp\{j2\pi(f_0 t + z(t))\} \tag{13}$$

which correspond to FM and PM, respectively. For a generic and periodic modulation function

$$z(t) = \sum_k z_0(t - kT) \tag{14}$$

and consequently the previous equations can be rewritten as:

$$s_{FM}(t) = \sum_k A_k \bar{s}_{FM}(t - kT)e^{\Theta_{FM}(k)} \tag{15}$$

$$s_{PM}(t) = \sum_k A_k \bar{s}_{PM}(t - kT)e^{\Theta_{PM}(k)} \tag{16}$$

These models represent different types of interfering signals including chirp, single tone and frequency hopping signals. The periodical envelope due to the periodicity of the modulation function $z(t)$ confirms that these kind of interfering signals have a characteristic waveform that repeats in time. Consequently, detection, estimation and mitigation techniques of the signal waveform can be defined by exploiting this property. The analytical interfering baseband signal is:

$$s(t) = \sum_{k=-\infty}^{\infty} A_k s_0 \left(t - kT\right) e^{j\theta_k} \tag{17}$$

where $s_0 \left(t - kT\right)$ is the signal periodic core, A_k and θ_k are the signal amplitude and phase of each period, respectively.

Finally the received signal is:

$$r(t) = s(t) + w(t) \tag{18}$$

where $w(t)$ is the AWGN with zero-mean and variance equal to N_0 $(\sim \mathcal{N}(0, N_0))$.
In this work GNSS signal is neglected in order to focus the attention on the jamming signal.

2.3 ALGORITHM DESCRIPTION

In the previous section the most common interfering signals have been introduced. Their mathematical expressions have been shown pointing out their periodic envelope in time, which can be exploited for the design of techniques able to counteract the jamming signals. In this work we present a different algorithm which exploits these periodic characteristics in jamming waveforms, and above all AC function properties, in order to detect, to estimate and to mitigate interfering events. The algorithm has been already presented and described in [P4] and [28]:

- Interferer Detection
- Interferer Waveform Acquisition
- Interferer Waveform Estimation
- Interferer Mitigation

In the following the time-discrete version of the received signal in eq.(18) is considered, expressed as:

$$r(n) = s(n) + w(n) = \sum_{k=-\infty}^{+\infty} A_k s_0(nTs - kT)e^{j\Phi_k} + w(n) \tag{19}$$

where T_s is the sampling period and $w(n)$ are the noise sample of the time-continue noise process $w(t)$, which are distributed as indipendent Gaussian random variables.

2.3.1 *Interferer Detection*

The Detection consists in observing the received signal in order to find any interfering event that may occour. The detection procedure is based on the AC function of the received signal. If a structured interfering signal is present, the AC function presents several peaks in the considered time window. These peaks correspond to the repetition period T. Thus, it is possible to design a simple way in jamming detection by exploiting this periodic characteristic. Detection procedure presents three steps:

1. The AC function is evaluated according to the Wiener-Kintchine theorem by means of the Fourier Transform (FT) and then normalized in order to have unit power (at zero-lag).
2. The detection test variable is evaluated as the maximum asbsolute value of the AC function neglecting the zero-lag sample in order to find the next maximum value.
3. The test is compared against a set threshold ξ.

It is worthwhile to notice that due to the finite observation time, the AC function can be estimated, thus no true value can be carried out. The procedure is described also in Algorithm 4 and shown in Figure (61).

Interference Detection Algorithm

1) $R_{rr^*}(m) = \mathcal{F}^{-1}\left\{\mathcal{F}\{r(n)\}\cdot\mathcal{F}\{r(n)\}^*\right\}$;
$R_{rr}(m) = \frac{R_{rr^*}(m)}{R_{rr^*}(0)}$;

2) $\text{Test} = \max|R_{rr^*}(m)| \quad m \neq 0$;

3) $\text{Test} \gtrless \xi$;

Algorithmus 4 : Interference Detection Algorithm

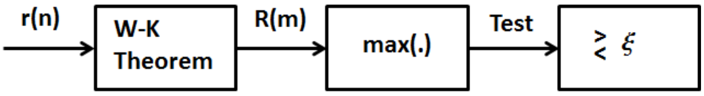


Figure 61: Interferer Detection - Block Diagram.

In the first step the circular correlation is performed by the Discrete Fourier Transform (DFT) where $\mathcal{F}\{\}$ and $\mathcal{F}^{-1}\{\}$ are the DFT and the inverse DFT, respectively. These operations can be calculated by the efficient numerical tools FFT and Inverse FFT (IFFT) for a large values of N, which is the signal samples in the observation windows. The AC function $R_{rr^*}(m)$ is defined for $m \in [M_{min}, M_{max}]$, i.e.for a limited number of lags. This interval has to be defined in order to be able to detect all the possible structured interferers, which could have different periods. Thus, it is necessary to properly define these parameters with the aim of detecting different jamming signal with different repetition period T.

2.3.1.1 *Statistical Parameter Setting*

Taking into account the Algorithm 4, it is necessary to set the lag-interval in which the AC function has to be evaluated. In [12] and [48] the measurement campaigns have highlightened that jamming signals have repetition periods varying usually from $1\mu s$ to $50\mu s$ with some longer exceptions ($\sim 70\mu s$). As stated before, the number of lags has to be larger enough in order to detect at least one repetition period, and so we have:

$$M_{max}T_s \geqslant T \tag{20}$$

The detection problem is defined as a binary decision problem, with two hypotheses:

- H_1 : the Test is greater than the threshold. The jammer is detected and the AC function peaks are located at each repetition period instant
- H_0 : the Test is lower than the threshold, meaning that any peak is present.

The AC function at the step 1 of the algorithm is defined by means of the product of FT transforms and it can be assumed as the results of average sum of products of the received signal samples, which are considered statistically indipendent each others. Neglecting the energy at the zero-lag ($m \neq 0$), at each repetition period the corresponding AC peak has energy equal to the average signal energy. The received signal $r(n)$ expressed in eq.(19) can be statistically expressed as a Gaussian random variable with mean equal to $\mu_r = A$ and variance $\sigma_r^2 = N_0$, due to the deterministic nature of $s(n)$ and $w(n) \sim \mathcal{N}(0, N_0)$. Considering that the evaluation of the mean and variance of a random variable defined as the product of two indipendent variables (a and b) are, respectively:

$$\begin{aligned} E[ab] &= E[a]E[b] \\ Var(ab) &= E^2[a]Var(b) + E^2[b]Var(a) + Var(a)Var(b) \end{aligned} \tag{21}$$

it is possible to define the statistical values of the single signal product as:

$$\mu_{rr^*} = A^2 \tag{22}$$

$$\sigma_{rr^*}^2 = \sigma_r^2\left(2\mu_{rr} + \sigma_r^2\right) \tag{23}$$

where the amplitude A is considered constant in each time period repetition. Consequently it is possible to define the statistical properties of the AC function, which can be expressed as:

$$\mu_R = \frac{A^2}{A^2+\sigma_r^2} = \frac{\frac{A^2}{\sigma_r^2}}{1+\frac{A^2}{\sigma_r^2}} \tag{24}$$

$$\sigma_R^2 = \frac{1}{M}\frac{\sigma_{rr^*}}{(A^2+\sigma_r^2)^2} = \frac{1}{M}\frac{1+2\frac{A^2}{\sigma_r^2}}{\left(1+\frac{A^2}{\sigma_r^2}\right)^2} \tag{25}$$

due to the Jammer-to-Noise Ratio (JNR) $\frac{A^2}{\sigma_r^2}$ and lags (M) normalization. Once statistical values of the AC have been defined, it is possible to evaluate the power value at the peak of the AC function as:

$$\begin{aligned} \mathrm{JNR}_{AC} &= \frac{\mu_R^2}{\sigma_R^2} \qquad (26) \\ &= M\frac{\frac{A^4}{\sigma_r^4}}{\left(1+\frac{A^2}{\sigma_r^2}\right)^2} \\ &= M\frac{\mathrm{JNR}^2}{1+2\mathrm{JNR}} \end{aligned}$$

At the same way, it is necessary to evaluate statistical properties for the hypothesis H_0, i. e.when the interfering signal is not present. Thus, it is possible to express with the same procedure as above the mean and variance values of the product of received signal samples:

$$\mu_{rr^*} = 0 \tag{27}$$

$$\sigma_{rr^*} = \sigma_r^4 \tag{28}$$

and the corresponding statistical properties for AC function under H_0 are:

$$\mu_R = 0 \tag{29}$$

$$\sigma_R = \frac{1}{M} \tag{30}$$

$$\mathrm{JNR}_{AC} = 0 \tag{31}$$

2.3.1.2 *Detector Design*

As previously stated, the detection of the interfering signal is modeled as a binary decision problem with two hypotheses H_1 the interfering signal is present, H_0 the interfering signal is absent. The decision test has been defined as the maximum of the absolute value of the AC function of the received signal, as described at the step 2 of the algorithm 4. The AC function has been evaluated by averaging a large number of products between random variables, thus it is possible to define the AC function Gaussian distributed random variable.

The considered variable is the AC function of the received signal, and the binary decision problem can be expressed as:

$$\begin{cases} R_{rr^*}(\tau) = R_{ss}(\tau) + R_w(\tau) & : H_1 \\ R_{rr^*}(\tau) = R_w(\tau) & : H_0 \end{cases} \tag{32}$$

where under H_1 the AC function is defined as the sum of the AC functions of the transmitted signal s and the noise w, instead under H_0 it is defined by the noise AC function. Assumed that the AC function is a Gaussian process, the probabilities density functions of the observable R under hypotheses can be written as following:

$$p_{\bar{R}|H_1}\left(\bar{R}|H_1\right) = \left(\frac{1}{\sqrt{2\pi\sigma_R^2}}\right)^N \exp\left\{-\frac{1}{2\sigma_R^2}\left\|\bar{R} - \bar{\lambda}^*(\tau,\Delta f)e^{j\theta}\right\|^2\right\} \tag{33}$$

$$p_{\bar{R}|H_0}\left(\bar{R}|H_0\right) = \left(\frac{1}{\sqrt{2\pi\sigma_R^2}}\right)^N \exp\left\{-\frac{1}{2\sigma_R^2}\left\|\bar{R}\right\|^2\right\} \tag{34}$$

The function $\lambda(\tau, \Delta f)$ represents the local replica of the AC function, and the derived expression represents the design of a generic decision binary problem including also the possibility of knowing the received signal waveform. The parameter τ represent the time instant in which the AC function is evaluated; Δf is the signal bandwidth and θ is the phase of the AC function. The likelihood ratio is:

$$\begin{aligned} \ell\left(\tau,\Delta f,\theta\right) &= \frac{p\left(\bar{R}|H_1,\tau,\Delta f,\theta\right)}{p\left(\bar{R}|H_0\right)} \\ &= \frac{\exp\left\{-\frac{1}{2\sigma_R^2}\left\|\bar{R} - \bar{\lambda}^*(\tau,\Delta f)e^{j\theta}\right\|^2\right\}}{\exp\left\{-\frac{1}{2\sigma_R^2}\left\|\bar{R}\right\|^2\right\}} \\ &= \exp\left\{-\frac{1}{2\sigma_R^2}\left\|\bar{\lambda}^*(\tau,\Delta f)e^{j\theta}\right\|^2\right\} \cdot \exp\left\{\frac{1}{\sigma_R^2}\Re\left\{\bar{R}\cdot\bar{\lambda}^*\left(\tau,\Delta f\right)e^{j\theta}\right\}\right\} \end{aligned} \tag{35}$$

The AC phase θ is unknown thus it is assumed uniformly distributed in $[0, 2\pi]$ with a pdf equal to

$$p(\theta) = \frac{1}{2\pi}$$

Taking into account the unknown phase, it is possible to neglect this value evaluating a mean function with respect to θ of the likelihood ratio, obtaining

$$\begin{aligned} \ell(\tau,\Delta f) &= \int_{-\pi}^{\pi} \ell(\tau,\Delta f,\theta)p(\theta)d\theta \\ &= \exp\left\{-\frac{\left\|\lambda^*(\tau,\Delta f)\right\|^2}{2\sigma_R^2}\right\} \cdot I_0\left(\frac{\left|\bar{R}\cdot\bar{\lambda}^*(\tau,\Delta f)\right|}{\sigma_R^2}\right) \end{aligned} \tag{36}$$

where $I_0(\cdot)$ is the modified zero-order Bessel function of the first kind. Calculating the natural logarithm of the average likelihood ratio, we have:

$$\Lambda(\tau, \Delta f) = \ln \ell(\tau, \Delta f) = -\frac{\|\lambda^*(\tau, \Delta f)\|^2}{2\sigma_R^2} + \ln I_0 \left(\frac{\left|\bar{R} \cdot \bar{\lambda}^*(\tau, \Delta f)\right|}{\sigma_R^2} \right) \quad (37)$$

Taking into account the monotone envelope of the $I_0(\cdot)$ it is possible to consider only its argument thus the average log-likelihood ratio test (ALLRT) becomes:

$$\Lambda(\tau, \Delta f) \simeq \ln \frac{\left|\bar{R} \cdot \bar{\lambda}^*(\tau, \Delta f)\right|}{\sigma_R^2} \underset{\hat{H}_0}{\overset{\hat{H}_1}{\gtrless}} \xi, \quad (38)$$

where the energy term, represented by the first addend in eq.(37), is not considered. The likelihood test expressed in eq.(38) depends on the time-shift τ and signal bandwidth Δf and it is difficult to compute without any theoretical assumption.

2.3.2 *Interferer Waveform Acquisition*

Once the jamming signal has been detected, the successive step is to acquire the malicious signal. This is necessary in order to mitigate and remove the interfering signal. The acquisition of the interferer waveform consists in estimating the repetition period $T = mT_s$ of the structured signal and in storing part of the received signal, of duration equal to the estimated repetition period. As stated before, it is possible to estimate the period by exploiting AC function properties of these kinds of signals, AC function that has to be calculated in a discrete set of lags which satisfies the condition $M_{lag}T_s > T$. Thus, the period estimation is carried out calculating the maximum absolute value of the AC function $R_{rr^*}(m)$ and selecting the lag m at which the evaluated maximum absolute value corresponds. Then, the local replica I of the jamming signal can be stored selecting part of the received signal of duration equal to the estimated repetition period. The procedure is reported in algorithm 5 and shown in Figure (62).

```
Interferer Waveform Acquisition
1) $R_{rr^*}(m) = \mathcal{F}^{-1}\left\{\mathcal{F}\{r(n)\} \cdot \mathcal{F}\{r(n+m)\}^*\right\}$ ;
$R_{rr}(m) = \frac{R_{rr^*}(m)}{R_{rr^*}(0)}$ ;
2) $\hat{m} = \max_m |R_{rr^*}(m)| \quad m \neq 0$;
3) $I = [r(1), ..., r(\hat{m})]$ ;
```

Algorithmus 5 : Interferer Waveform Acquisition

2.3.3 *Interferer Waveform Estimation*

Once the local replica I has been derived, it can be used to track and to estimate the malicious waveform. The estimation is carried out

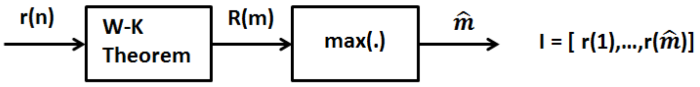


Figure 62: Interferer Acquisition - Block Diagram.

according to the Maximum Likelihood (ML) criterion, applied at each part of signal long as the estimated period $\hat{T} = \hat{m}T_s$. Then, parameters phase ϕ and amplitude A are estimated at each period. This step is performed defining N_D delayed version of the received signal, which are *very Early, Early, Prompt, Late, very Late* with one sample of time-spacing between each other. According to the ML criterion the phase and amplitude parameter estimations are defined as:

$$\begin{aligned} \phi_i &= \text{angle}\{\mathbf{r_i} \bullet \mathbf{I}\} & (39) \\ A_i &= \frac{\Re\{\mathbf{r_i} \bullet \mathbf{I}\}}{\mathbf{I} \bullet \mathbf{I}} & (40) \end{aligned}$$

where $i \in [vE, E, P, L, vL]$, $a \bullet b$ represents the scalar product between a and b. The Thus, the estimates of amplitude and phase parameters are defined as the real part of the scalar product between the received signal delayed version and the local replica and normalized by the local replica energy, and angle of the scalar product between considered version of the received signal and the local replica, respectively. Successively, the likelihood function $\boldsymbol{\Lambda}$ is maximized and the delay, phase and amplitude estimates are carried out. When these parameters are defined at each period the interfering signal $\mathbf{s}$ can be estimated and it can be expressed as:

$$\hat{s} = \hat{A} I e^{j\hat{\phi}} \quad (41)$$

Taking into account that the *Prompt* replica begins at time-sample $D = \hat{m}$, the other replicas correspond to $[-2, -1, +1, +2]$ with respect to the *Prompt* one. The procedure, for each period, is described in algorithm 6 and shown in Figure (63).

The delayed version, which maximizes the scalar product with the local replica, updates the local replica. The new local replica I, which will be used for the next signal period, is updated by evaluating the mean of the replicas, stored in a matrix of L rows.

In order to reconstruct the jamming waveform, a more accurate estimation of the parameters has to be performed. It is necessary to refine the estimated values starting from the initial coarse estimation through the ML criterion.

2.3.4 *Interferer Waveform Mitigation*

The last step of our algorithm is the cancellation of the interfering signal. Since that the interfering waveform has been estimated in the

Interferer Waveform Estimation

```
while 1 do
    for i = νE : νL;
    1) $r_i = [i + D, \dots, \hat{m} + i]$ ;
    2) $\phi_i = \text{angle}\{\mathbf{r_i} \bullet \mathbf{I}\}$;
    $\phi = [\phi, \phi_i]$ ;
    3) $\boldsymbol{\Lambda}_i = \Re\left\{(\mathbf{r_i} \bullet \mathbf{I})\, e^{-j\phi_i}\right\}$ ;
    $\boldsymbol{\Lambda} = [\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_i]$ ;
    end ;
    4) $(D, \phi) = [D + i, \phi_i]$   if   $max(\boldsymbol{\Lambda}) = \boldsymbol{\Lambda}_i$ ;
    5) $r = r_i$   if   $max(\boldsymbol{\Lambda}) = \boldsymbol{\Lambda}_i$ ;
    6) $A = \frac{\Re\{\mathbf{r} \bullet \mathbf{I}\}}{\mathbf{I} \bullet \mathbf{I}}$ ;
    7) $I = \text{mean}\,(r, I, L)$ ;
end
```

Algorithmus 6 : Interferer Waveform Estimation

previous step, the cancellation steps consists in subtracting the estimated interfering waveform in eq.(41) from the received signal, as:

$$\hat{r} = r - \hat{s} \tag{42}$$

Once the interfering signal is cancelled, and consequently the jamming effect is mitigated, it is possible to increase the reliability and the effectiveness of the GNSS signal transmission. Thus, the elaboration and calculation of the PVT solutions are computationally easier to be done.

In this section, we have shown our approach in interference detection and mitigation problem. The theoretical aspects of the algorithm have been described detailing the principal operations. The described algorithm has been also tested in two different scenarios, *Non Dispersive Channel* and *Multipath Channel*. The theoretical approach of both scenarios is described in section 2.4 and in section 2.5, respectively.

2.3.5 *Complexity Evaluation*

In the following, the complexity evaluation for the proposed algorithm is defined. As described before the algorithm is defined by four steps and for each of them a complexity evaluation has to be estimated. It is worthwhile to notice that all this analysis on the algorithm complexity hase been already described in [28] and [29], except for the detection step.

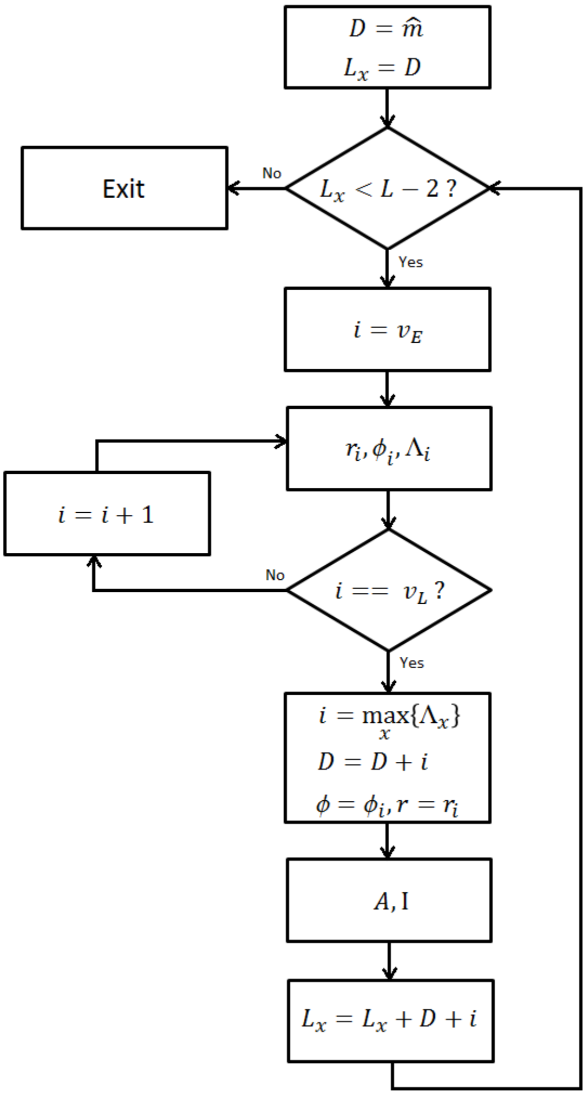


Figure 63: Interferer Estimation - Flow graph.

2.3.5.1 *ID & IWA*

In both detection and waveform acquisition the most complex operation is the evaluation of the AC function by exploiting the FFT and the IFFT. As well known, the complexity of one FFT operation is $\mathcal{O}\left(N \log_2 N\right)$.

2.3.5.2 *IWE*

The interferer waveform estimation step is the most complex of the proposed algorithm. The complexity is evaluated in terms of number of operations to be performed at each signal period repetition.

1. For each delayed signal replica, phase estimation is performed. This task is evaluated by the correlationbetween two sequence of length $\hat{m}$. Thus, this calculation requires: $\hat{m}N_D$ products, $\hat{m}N_D$ sums and N_D angle functions

2. Likelihood function $\boldsymbol{\Lambda}$: delayed replicas are de-rotated by products with the conjugate phase. evaluated before. Thus, N_D complex products are implemented.

3. Amplitude estimation is performed as a the real part of the correlation between the delayed version which satisfies the maximum $\boldsymbol{\Lambda}$ and the normalization by the local replica energy. Thus, only two products are implemented.

4. Updating of the Local replica $\mathbf{I}$: the last step is to update the local replica. It is necessary to average L sequences of length $\hat{m}$, requiring $\hat{m}L$ sums and L products.

2.3.5.3 *IWM*

The last step is the cancellation of the estimated jamming signal. This part consists in the difference between the received signal and the reconstructed interfering waveform. Thus, a simple difference is performed.

Finally, the total computational complexity of the algorithm can be estimated. The proposed procedure needs a number of sums and products equal to:

$$N_{sums} = \hat{m}\,(N_D + 1 + L) \qquad (43)$$

$$N_{prod} = \hat{m}\,(N_D + 1 + 1) \qquad (44)$$

which highlight that the complexity is proportional to the lag $\hat{m}$, which defines the estimated repetition period.

2.4 NON-DISPERSIVE CHANNEL

Due to the increasing widespread of GNSS applications in human life activities, it is necessary to define techniques able to counteract the malicious events that wants to deny the correct operation of the GNSS receiver. As explained previously, the jamming threat in GNSS system is a very hot topic and several research studies have been done. Most of these results regard to detection and mitigation of the interfering event in a non dispersive channel scenario. The jammer is in earth surface and direct visibility to the target, thus the received signal is defined as the jamming signal embedded in noise process, assumed to be a additive gaussian statistical process. In [29] an algorithm able to cope with all the interfering signals with a structured envelope, is proposed. As extensively described in [28], the algorithm consists of four stages: i) waveform acquisition, ii) waveform tracking, iii) effective interference parameter estimation, iv) interference cancellation. The performance is evaluated in terms of residual of cancellation and it has been carried out for three different types of signal, continuous waveform, chirp and CDMA.

2.4.1 *Jamming Chirp*

In our study we consider a jamming chirp signal. Chirp signals are defined as FM signals in which the frequency increases or decreases with time, called "up-chirp" and "down-chirp", respectively. They are also called as sweep signals. The modulation function can be classified in two main categories, linear chirp modulation and exponential chirp modulation, i. e.the swept in frequency is defined by a linear function or an exponential one, respectively. In the following, a chirp signal with a frequency varying linearly in time is considered. The jamming signal is expressed as:

$$\begin{aligned} s(t) &= A\mathrm{rect}_T(t)\cos\left(2\pi\int_0^t f(r)dr\right) = \\ &= A\mathrm{rect}_T(t)\cos\left(2\pi\int_0^t \left[f_0 \pm \frac{\rho}{2\pi}r\right]dr\right) \\ &= A\mathrm{rect}_T(t)\cos\left(2\pi f_0 t \pm \rho\frac{t^2}{2}\right) \end{aligned} \qquad (45)$$

where $\rho = \frac{2\pi\Delta f}{T}$ is the frequency variation rate, T is the pulse period, f_0 is the carrier frequency and Δf is the frequency excursion during a pulse period.

Taking into account eq.(17) and considering one signal period, the jamming basic waveform is:

$$s_0(t) = \exp\left\{\pm j\rho\frac{t^2}{2}\right\}\mathrm{rect}\left(\frac{t}{T}\right) \qquad (46)$$

In the following, an "up-chirp", with a positive frequency slope, is considered.

2.4.2 *Jamming Chirp Autocorrelation Analysis*

As highlighted in the previous section, the most common jamming signals are structured and present a periodic envelope. Among them, one of the interesting case-study is represented by the chirp signal, which expression is shown in eq.(46). In order to exploit this periodic characteristics, a complete analysis of the AC function is carried out. The spectrum of the chirp signal is evaluated through the FT of the signal which is expressed as:

$$\begin{aligned} S(f) &= \int_{-\infty}^{+\infty} s(t)e^{-j2\pi ft}dt \qquad (47) \\ &= \int_{-T/2}^{T/2} e^{j\frac{\rho}{2}t^2}e^{-j2\pi ft}dt \\ &= \int_{-T/2}^{T/2} e^{j(\frac{\rho}{2}t^2-2\pi ft)}dt \end{aligned}$$

The argument of the exponential function can be considered as the square of a difference without the square of the second term. Thus, we have:

$$\begin{aligned} \frac{\rho}{2}t^2 - 2\pi ft &= (a-b)^2 - b^2 \\ &= a^2 - 2ab \end{aligned} \tag{48}$$

From eq.(48) it is possible to define $a = \sqrt{\frac{\rho}{2}}t$ and $b = \pi f\sqrt{\frac{2}{\rho}}$ and so the exponent in eq.(47) can be written as:

$$\frac{\rho}{2}t^2 - 2\pi ft = \left(\sqrt{\frac{\rho}{2}}t - \pi f\sqrt{\frac{2}{\rho}}\right)^2 - \frac{2}{\rho}(\pi f)^2 \tag{49}$$

Thus, the chirp spectrum expression is:

$$\begin{aligned} S(f) &= e^{-j\frac{2(\pi f)^2}{\rho}} \int_{-T/2}^{T/2} e^{j\left(\sqrt{\frac{\rho}{2}}t - \pi f\sqrt{\frac{2}{\rho}}\right)^2} dt \\ &= \sqrt{\frac{\pi}{\rho}} e^{-j\frac{2(\pi f)^2}{\rho}} \int_{Z_1}^{Z_2} e^{j\pi\frac{y^2}{2}} dy \end{aligned} \tag{50}$$

The last expression is obtained through the substitution

$$\sqrt{\frac{\rho}{2}}t - \pi f\sqrt{\frac{2}{\rho}} = \sqrt{\frac{\pi}{2}}y$$

and the derivation of the corresponding integration interval

$$Z_1 = \sqrt{\frac{\rho}{\pi}}T\left(-\frac{1}{2} - \frac{f}{\Delta f}\right) = \sqrt{2\Delta fT}\left(-\frac{1}{2} - \frac{f}{\Delta f}\right) = \sqrt{2\Delta fT}\left(\frac{-\Delta f - 2f}{2\Delta f}\right) \tag{51}$$

$$Z_2 = \sqrt{\frac{\rho}{\pi}}T\left(\frac{1}{2} - \frac{f}{\Delta f}\right) = \sqrt{2\Delta fT}\left(\frac{1}{2} - \frac{f}{\Delta f}\right) = \sqrt{2\Delta fT}\left(\frac{\Delta f - 2f}{2\Delta f}\right) \tag{52}$$

The last expression of the chirp spectrum can be considered as a linear combination of Fresnel integral functions. It is possible to notice that the expression of eq.(50) is the Fresnel integral $E(x) = C(x) + jS(x)$, where

$$C(x) = \int_0^x \cos\left(\frac{\pi y^2}{2}\right) dy$$

$$S(x) = \int_0^x \sin\left(\frac{\pi y^2}{2}\right) dy$$

Finally, the chirp spectrum can be expressed as:

$$\begin{aligned} S(f) &= \sqrt{\frac{\pi}{\rho}} e^{-j\frac{2(\pi f)^2}{\rho}} \{C(Z_2) + C(-Z_1) + j\,[S(Z_2) + S(-Z_1)]\} \\ &= \sqrt{\frac{\pi}{\rho}} e^{-j\frac{2(\pi f)^2}{\rho}} \{E(Z_2) + E(-Z_1)\} \end{aligned} \tag{53}$$

where the properties $C(-x) = -C(x)$ and $S(-x) = -S(x)$ are considered.

The amplitude spectrum is defined as:

$$|S(f)| = \sqrt{\frac{\pi}{\rho}\{[C(Z_2) + C(Z_1)]^2 + [S(Z_2) + S(Z_1)]^2\}} \tag{54}$$

and the phase spectrum is:

$$\Phi(f) = \frac{(2\pi f)^2}{2\rho} + \tan^{-1}\left\{-\frac{S(Z_2) + S(Z_1)}{C(Z_2) + C(Z_1)}\right\} \tag{55}$$

where the first term is a quadratic contribution and the second term is the phase shift due to Fresnel integrals. Taking into account that Fresnel integrals are complex functions, it is possible to derive an approximation of the eq.(53) studying the asymptotic behaviour of the Fresnel integrals:

$$C(x)_{x\to\pm\infty} = \pm\frac{1}{2} \tag{56}$$

$$S(x)_{x\to\pm\infty} = \pm\frac{1}{2} \tag{57}$$

Let us consider an interfering signal with large period T. According to eq. (56) and (57), Fresnel Integral becomes:

$$E(Z_2) = C(Z_2) \pm jS(Z_2) = \pm\frac{1}{2} \pm j\frac{1}{2} \tag{58}$$

$$E(Z_1) = C(Z_1) \pm jS(Z_1) = \pm\frac{1}{2} \pm j\frac{1}{2} \tag{59}$$

where Z_1 and Z_2 depend on frequency, thus it is necessary to define the Fresnel equation behavior with varying frequency f. Let us consider $-Z_1$ and Z_2 one at a time, always taking into account a large interfering period T. According to eq.(51), when $2f < 0$ and $|2f| > \Delta f$, $-Z_1$ tends to $-\infty$ thus $E(-Z_1) \to -\frac{1}{2} - j\frac{1}{2}$; otherwise, $-Z_1$ tends to $+\infty$ thus $E(-Z_1) \to +\frac{1}{2} + j\frac{1}{2}$. Similarly, according to eq.(52) when $|2f| > \Delta f$ then Z_2 tends to $-\infty$ thus $E(Z_2) \to -\frac{1}{2} - j\frac{1}{2}$; otherwise Z_2 tends to $+\infty$ thus $E(Z_2) \to +\frac{1}{2} + j\frac{1}{2}$. Through these studies and concerning eq.(53), it is possible to derive an approximation of chirp spectrum defined by the sum of Fresnel integral $E(Z_2) + E(-Z_1)$. Chirp spectrum can be considered as a rectangular function within the bandwidth Δf, obtaining

$$S(f) \to (1 + j)\text{rect}\left\{\frac{f}{\Delta f}\right\}$$

In Figure(64) Fresnel integral approximations are shown: in (a), (b), (c), $E(Z_2)$, $E(-Z_1)$ and $E(Z_2) + E(-Z_1)$ asymptotic behaviors are shown, respectively.

Tanking into account the previous approximation regarding Fresnel integral, chirp spectrum can be expressed as:

$$S(f) \simeq \sqrt{\frac{\pi}{\rho}} e^{-j\frac{2(\pi f)^2}{\rho}} [1 + j] \,\text{rect}\left(\frac{f}{\Delta f}\right) \tag{60}$$

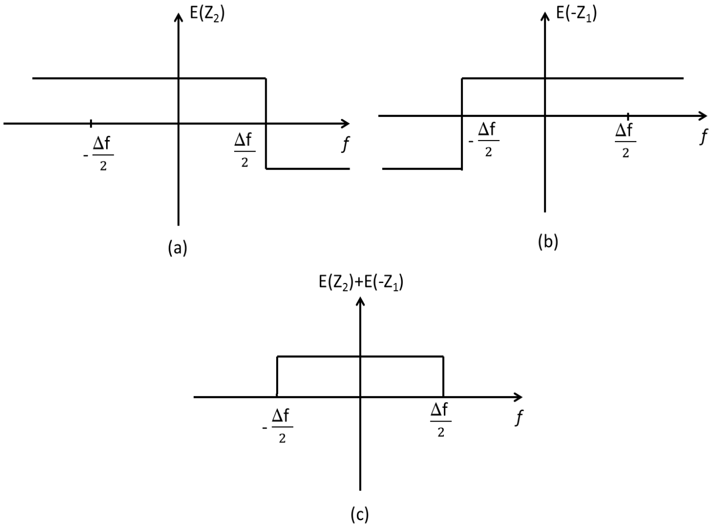


Figure 64: Fresnel integral approximation.

It is well known that the autocorrelation function of a signal is the inverse Fourier transform of its Energy Spectral Density (ESD). In this case, the chirp ESD is:

$$E_{ss}(f) = |S(f)|^2 = 2\frac{\pi}{\rho}\text{rect}\left(\frac{f}{\Delta f}\right) \tag{61}$$

and, according to the Wiener-Khintchine Theorem, the autocorrelation function of the chirp signal can be expressed:

$$R_{ss}(t) = \mathcal{F}^{-1}\left\{E_{ss}(f)\right\} = 2\frac{\pi}{\rho}\Delta f \text{sinc}\left(\Delta f t\right) = T\text{sinc}\left(\Delta f t\right) \tag{62}$$

Taking into account the eq.(18), AC function of the received signal is written as:

$$R_{rr}(t) = R_{ss}(t) + R_W(t) \tag{63}$$

in which the $R_N(t)$ represents the AC function of the noise process, considered independent from the jamming signal.

2.4.3 *Numerical Results*

2.4.3.1 *Approximation Validation*

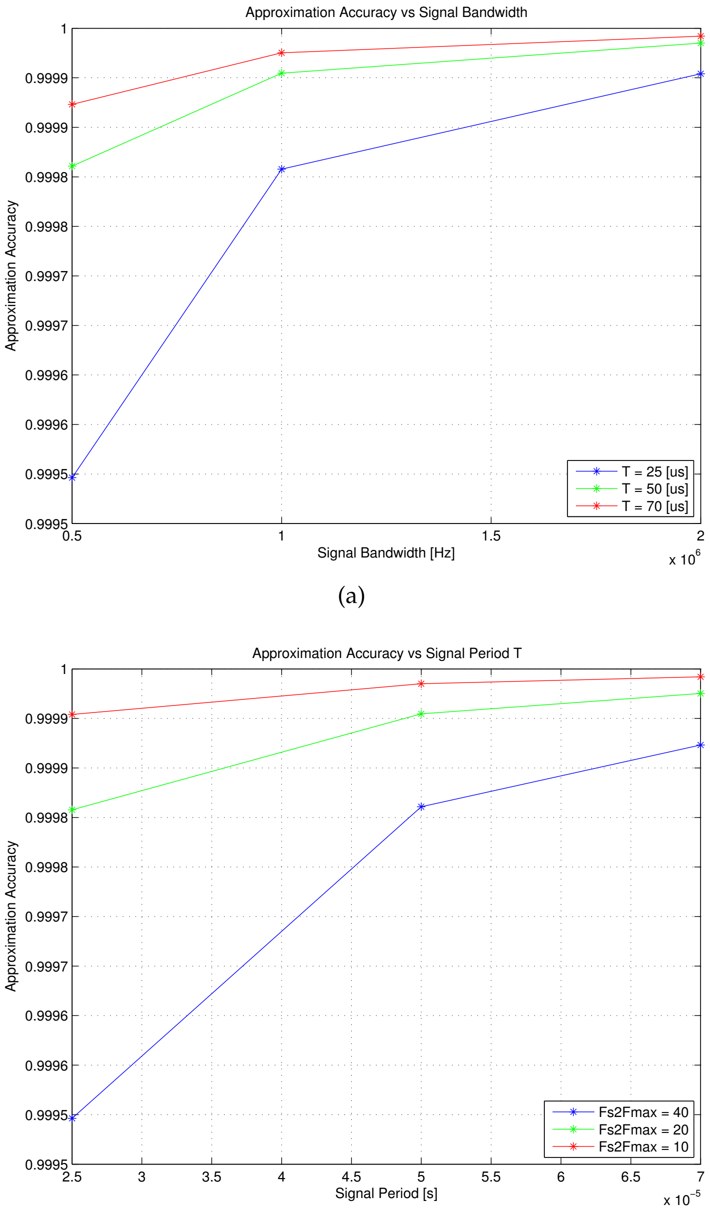
The parameter used is this validation are:

- Interferer bandwidth: 500[KHz],1[MHz],2[MHz]. These values are derived by the ratio between the sampling frequency $f_s = 20[\text{MHz}]$ and the maximum frequency of the chirp signal. So that $\text{Fs2Fmax} = [40, 20, 10]$ correspond to 500[KHz],1[MHz],2[MHz], respectively.

- Interferer period: $25, 50, 70[\mu s]$

- Observed signal length equal to three periods.

In eq.(62) an approximation of the autocorrelation function of the chirp signal is expressed. In order to validate this approximation, a comparison between the AC function in eq.(62) has been done.



(a)

(b)

Figure 65: (a)Approximation accuracy vs. interfering signal bandwidth; (b) approximation accuracy vs. interfering signal period.

In figures 2.65(a) and 2.65(b) the results of the accuracy of this approximation are shown, varying interfering signal bandwidth and interfering signal period, respectively.

It is possible to notice that the approximation in eq.(62) almost matches the AC function expressed in the algorithm 4 in both cases. Thus, it is possible to consider valid the approximation of the chirp AC function carried out in the section 2.4.2.

2.4.3.2 *ID: Probability of Detection*

In section 2.3.1.2 the theoretical analysis of the binary decision problem has been derived. The detection test has been defined exploiting the ML criterion. As stated before, the likelihood ratio in eq.(38) depends on the time-shift τ and the bandwidth Δf and it is not simple to compute without any assumption. Thus it is possible to distinguish two different approaches:

- Classic Detector: $\bar{\lambda}(\tau) = \bar{\lambda}(\tau, \Delta f) \mid_{\Delta f \to \infty}$. In this case the autocorrelation replica becomes a Dirac delta and so the product $\left|\bar{r} \cdot \bar{\lambda}^*(\tau)\right|$ is not zero when the replica is not null.
- Optimize Detector: $\bar{\lambda}(\tau, \Delta f) \propto \text{sinc}\,(\Delta f \tau)$. In this case the product is between the received autocorrelation function $\bar{r}$ and the analytical expression of the autocorrelation function, which is proportional to a sinc.

In the Classic case, the detection test is defined as the product between the AC function and a Dirac delta; on the other hand,in the Optimize case, the detection test is defined as the product between the AC function R and the analytical formula of the AC function of a chirp signal. This last approach seems as a matched filter due to the fact that the received signal is elaborated with the analytical waveform that is expected.

The performance of the interferer detection algorithm, described in section 2.3.1, has been carried out in terms of probability of correct detection , i. e.the probability that the interfering signal is present in the received signal, and in terms of probability of false alarm, i. e.the probability that the interfering signal is present when it should not be. The results have been obtained by means of Monte Carlo simulations. In the following, the performance is characterized in terms of the probability of detection, since, for the considered simulation settings, a $P_{fa} = 0$ is always obtained also for a large number of Monte Carlo iterations(10^6). The simulation parameters are listed in table 6.

Type of Signal	Chirp Signal
Min frequency	-5MHz
Max frequency	5MHz
Sampling frequency	16MHz
Signal period	$[10, 25, 50]\mu s$

Table 6: Detection - Simulation Parameter

In Figure (66) and in Figure (67) the probability of detection for the classic detector and for the optimize detector are shown in function of the normalized threshold, evaluated according to eq.(24), with a value of $J/N = 0[dB]$.

In both cases, a chirp signal, generated with three different periods $[10, 25, 50]\mu s$ and represented by blue, red, green lines respectively, has been tested in the detection algorithm. The performance show

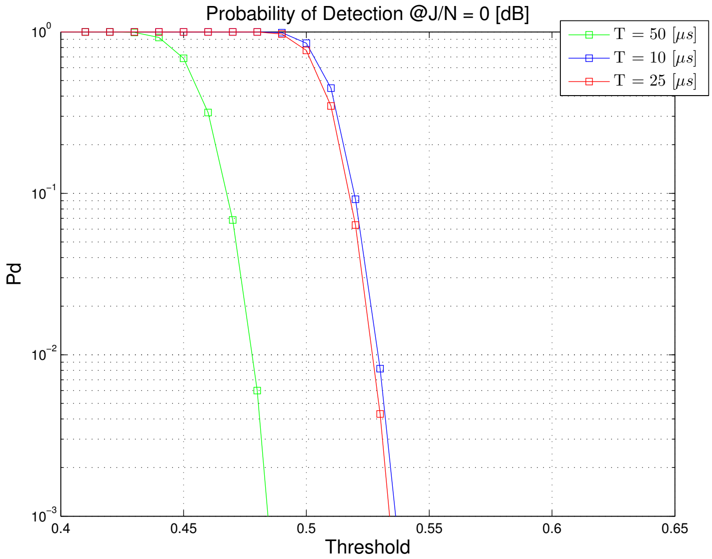


Figure 66: Probability of Detection - Classic Detector.

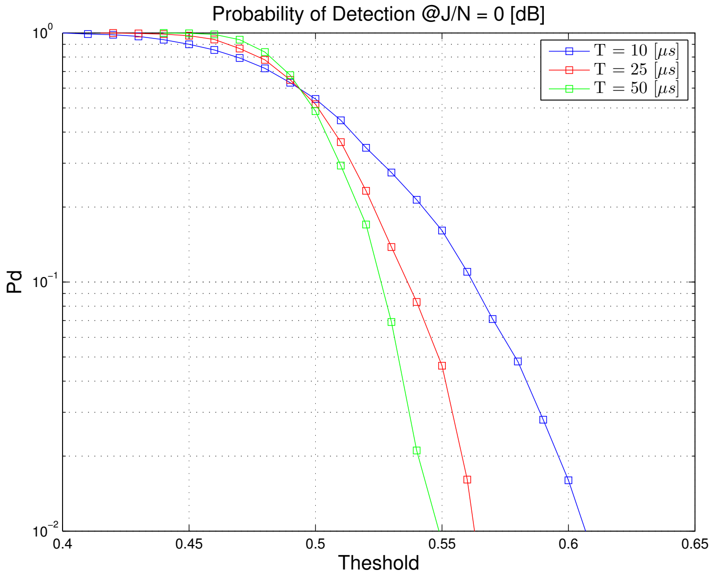


Figure 67: Probability of Detection - Optimize Detector.

that the probability of detection is higher for the case of shorter repetition period, i. e.for the chirp signal with period equal to 10μs (blue line). According to our knowledge, this is due to the fact that on equal terms, as J/N and observation time-window, the interfering signal with the shorter repetition period presents more AC function peaks and consequently the events that cross the thresholds set are more than in the case of longer repetition period. The same happens comparing the performance of periods 25μs and 50μs, in both detector cases.

2.4.3.3 *IWE: Parameters Estimation*

In order to test the capability of the Interferer Waveform Estimation step described in section 2.3.3, the estimates of the signal parameter $\hat{T}, \hat{\phi}, \hat{A}$ have been evaluated by means of the Mean Square Error (MSE).

In order to improve the jamming waveform reconstruction, it is necessary to refine parameter estimates starting from the initial coarse value through the ML criterion. The coarse estimation of the period is carried out by evaluating the maximum of the AC function and selecting the corresponding lag. Exploiting the discrete time AC function, the coarse value T is calculated as an integer value since the corresponding lag $\hat{m}$ is determined as an integer value depending on the sampling rate T_s. But, the AC peak could not fall on a discrete sample and so it is necessary to interpolate among AC function samples close to the main peak for an increased precision. From this analysis, the time-delay is defined by two quantities, the coarse value $\hat{m}$ and the shift δ obtained from interpolation, and expressed as:

$$\hat{m}_\delta = \hat{m} + \delta \tag{64}$$

The shift δ can be evaluated exploiting one of the existing subsample delay estimation techniques, described in [85],[22],[23],[63]. Once a discrete delay is obtained, the fractional part of this delay is carried out by means of the cited approaches. In our study we use the *parabolic fit interpolation* that belongs to the family of the three point fit interpolation methods. The estimation of the fractional part of the delay is determined by fitting a curve with the two closer samples around the main peak $\hat{m}$. The parabolic fit is a widely used methods to improve the precision of the AC peak location estimation. The sample delay δ is determined as [16][52]:

$$\hat{\delta} = \frac{R_{rr^*}(\hat{m}+1) - R_{rr^*}(\hat{m}-1)}{2\left[-R_{rr^*}(\hat{m}+1) + 2R_{rr^*}(\hat{m}) - R_{rr^*}(\hat{m}-1)\right]} \tag{65}$$

The parabolic fit is a widely used method to estimate the fractional part of the sample lag. This method consists in fitting a parabola curve among the closest samples $R_{rr^*}(\hat{m}-1)$ and $R_{rr^*}(\hat{m}+1)$ around the AC peak $R_{rr^*}(\hat{m})$, where $\hat{m}$ is carried out from the acquisition step.

From eq.(64) then the refined jamming period estimate is expressed as:

$$\hat{T} = \hat{m}_\delta T_s \tag{66}$$

Successively, it is possible to refine the estimation of the parameter ϕ. It is worthwhile to underline that in our study the initial phase is consider equal to zero. Thus, the parameter ϕ represents the chirp rate ρ which is evaluated as:

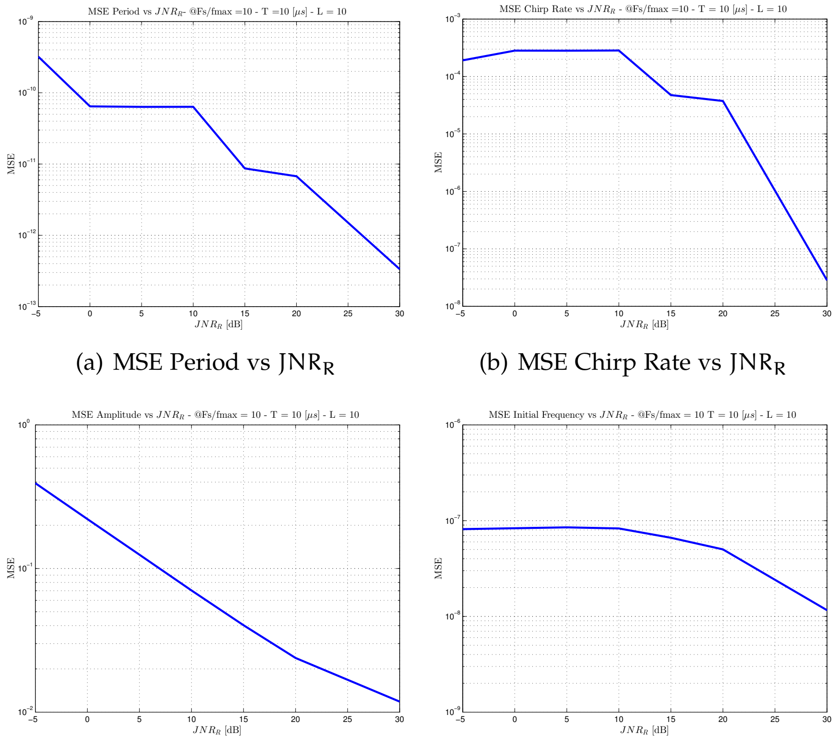
$$\hat{\rho} = \frac{\hat{B}}{\hat{T}} \tag{67}$$

where $\hat{B}$ is the estimated bandwidth evaluated through the algorithm described in Chapter 1 and $\hat{T}$ is expressed in eq.(66). Successively, the received signal is dechirped, i. e.it is multiplied for the conjugate of the estimated $\hat{\rho}$ in order to balance the FM factor. After that,

the amplitude estimate $\hat{A}$ can be evaluated as explained in the algorithm 6. In addition, it could be possible to estimate also the initial frequency of the chirp signal by means of the FT. After de-chirping multiplication, the FT of the received signal is performed and the initial frequency is estimated as the frequency bin corresponding to the maximum value of the PSD of the signal. Due to the structure characteristics of the considered jamming signal, all these estimation procedures are performed each repetition period. Through the refined parameters a more accurate estimation and reconstruction of the jamming waveform can be determine with an increased accuracy in the mitigation step.
The parameter used in the parameter estimation step are listed in table 7.

Type of Signal	Chirp Signal
Sampling Frequency	16[MHz]
Min frequency	0MHz
Max frequency	1.6MHz
Signal period	$[10, 25, 50]\mu s$
JNR_R	$[-5, 0, 5, 10, 15, 20, 25, 30]$
M	1600

Table 7: Estimation - Simulation Parameter



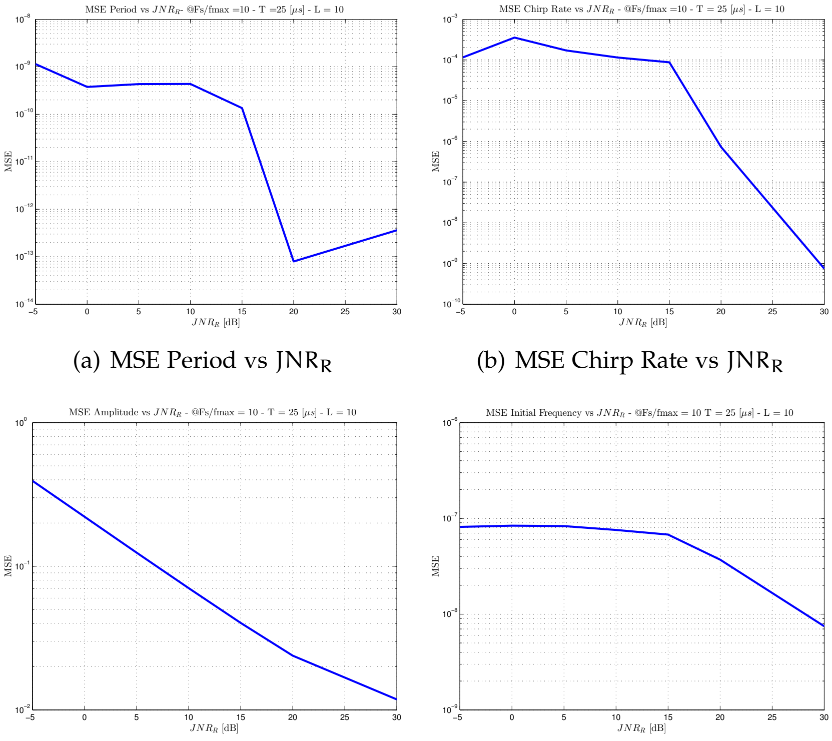
(a) MSE Period vs JNR_R

(b) MSE Chirp Rate vs JNR_R

(c) MSE Amplitude vs JNR_R

(d) MSE Initial frequency vs JNR_R

Figure 68: MSE vs JNR_R - $F_s/f_M = 10 - T = 10[\mu s] - L = 10$



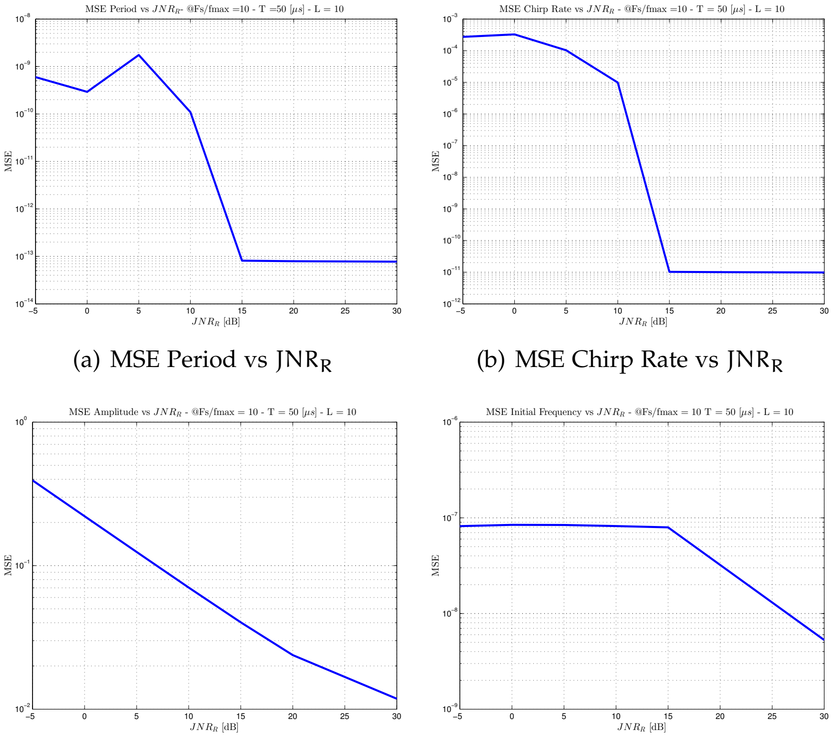
(a) MSE Period vs JNR_R

(b) MSE Chirp Rate vs JNR_R

(c) MSE Amplitude vs JNR_R

(d) MSE Initial frequency vs JNR_R

Figure 69: MSE vs JNR_R - $F_s/f_M = 10 - T = 25[\mu s] - L = 10$



(a) MSE Period vs JNR_R

(b) MSE Chirp Rate vs JNR_R

(c) MSE Amplitude vs JNR_R

(d) MSE Initial frequency vs JNR_R

Figure 70: MSE vs JNR_R - $F_s/f_M = 10 - T = 50[\mu s] - L = 10$

It is necessary to underline that due to the fact that the nature of the jamming signal is not known a priori thus parameters cannot be considered as deterministic values. In real scenarios it is not possible to know which kind of jamming signal can disrupt the correct GNSS functionality and consequently it is not possible to define a deterministic estimator and to perform the comparison with the Cramer Rao Bound (CRB). For this reason, parameter estimates are evaluated in terms of MSE versus the JNR_R at the AC function peak (the same of JNR_{AC} expressed in eq. (26)). Accordingly, the correspondent value of the JNR can be calculated inverting eq.(26) and solving a second order problem. Consequently, the JNR value is lower than the JNR_R strongly depending on the number of samples M considered in the AC function evaluation. Higher is M lower is JNR, with a strong difference between jamming and noise power.
In Figure 2.68(a), Figure 2.68(b), Figure 2.68(c) and Figure 2.68(d) the MSE of parameter estimates $\hat{T}, \hat{\varphi}, \hat{A}, \hat{f}_0$ for a signal period of $T = 10\mu s$ are shown respectively. For all the parameters, increasing the value JNR_R the error in the estimation decreases rapidly. For the parameter T the estimation error goes from 10^{-9} to 10^{-13} [s], for the parameter A the range is 10^0 to 10^{-2}, and for the parameter ρ the interval is from 10^{-4} to 10^{-8} $[1/s^2]$. The exception is represented by the MSE envelope for the parameter $\hat{f}_0$ that remains quite constant for all the JNR_R around the value 10^{-7}[Hz].
In Figure 2.69(a), Figure 2.69(b), Figure 2.69(c) and Figure 2.69(d) the MSE of parameter estimates $\hat{T}, \hat{\varphi}, \hat{A}, \hat{f}_0$ for a signal period of $T = 25\mu s$ are shown respectively. Also in this case, increasing the value JNR_R the error in the estimation decreases rapidly. For the parameter T the estimation error goes from 10^{-9} to 10^{-13}, for the parameter A the range is 10^0 to 10^{-2}, and for the parameter ρ the interval is from 10^{-4} to 10^{-9}. The exception is represented by the MSE envelope for the parameter $\hat{f}_0$ that remains quite constant for all the JNR_R around the value 10^{-7}[Hz].
In Figure 2.70(a), Figure 2.70(b), Figure 2.70(c) and Figure 2.70(d) the MSE of parameter estimates $\hat{T}, \hat{\varphi}, \hat{A}, \hat{f}_0$ for a signal period of $T = 50\mu s$ are shown, respectively. As for the previous case, increasing the value JNR_R the error in the estimation decreases rapidly. For the parameter T the estimation error goes from 10^{-9} to 10^{-13}, for the parameter A the range is 10^0 to 10^{-2}, and for the parameter ρ the interval is from 10^{-4} to 10^{-11}. The exception is represented by the MSE envelope for the parameter $\hat{f}_0$ that remains quite constant for all the JNR_R around the value 10^{-7}[Hz].

The parameter estimation errors in function of the power at the AC function peak for three different jamming period values have been carried out. It can be noticed that increasing the jamming period performance slightly improves as expected, but in particular for high JNR_R values. However, for all the considered parameters, the MSE is very low, defining an efficient estimation.

2.4.3.4 *IWM: Cancellation Residual*

The performance of the cancellation algorithm depends on the correct parameter estimation results. With accurate parameter estimations a reliable signal reconstruction is possible and consequently an effective cancellation can be performed, and a successful mitigation action can be done reducing the malicious effect.
As indicated in table 8, we considered a chirp signal with three differents repetition periods, and with two different values of mean tracking memory, i. e.$L = [10, 100]$

Type of Signal	Chirp Signal
Bandwidth	2MHz
Sampling frequency	16MHz
Signal period	$[10, 25, 50]\mu s$
Mean Tracking Length	$L = [10, 100]$
J/N	$[-20, -15, -10, -5, 0]dB$

Table 8: Cancellation Parameter

As expressed in section 2.3.4, the cancellation is performed according to eq.(42), but the performance evaluation is carried out in terms of residual power, that can be written as:

$$\boldsymbol{\epsilon} = |\mathbf{r} - \hat{\mathbf{s}}|^2 \tag{68}$$

In eq.(68) the left hand side $\boldsymbol{\epsilon}$ is the residual power evaluated as the square difference between the received signal $\mathbf{r}$ and the estimated and reconstructed signal $\hat{\mathbf{s}}$.

In Figure (71) - Figure (76) the residual power after cancellation for a chirp signal generate with three different repetition period is shown. The performance have been evaluated ad different values of J/N. Higher is the J/N value lower is the residual power $\boldsymbol{\epsilon}$. In addition, for all the tested cases, the higher the mean tracking length L the lower the residual power $\boldsymbol{\epsilon}$.

These results show that the jamming waveform is strongly mitigated in all the tested cases. The residual power value depends on the adopted mean tracking memory L. At $J/N = 0[dB]$, the residual power value decreases and fixes his own value at 10^{-1} and 10^{-2} for value $L = 10$ and $L = 100$, respectively, defining a difference of ten units. This is quite valid for the other J/N values, except for the lowest ones. The gap of one decade between different values of L is due to the fact that with a larger number of memory stack it is possible to perform a more accurate waveform estimation and consequently a more effective jamming mitigation. In addition, the length of the repetition period affects the results of the mitigation. As the same of the L value, with longer repetition period it is possible to better estimate waveform parameter and then the residual power is lower. By observing Figure(72) and Figure(76), for the value $J/N = 0[dB]$ in case of a

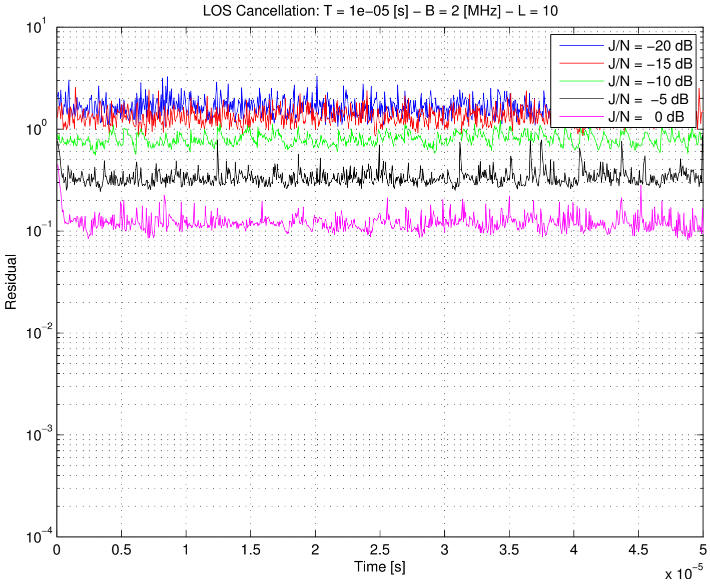


Figure 71: Residual power after cancellation: $T = 10\mu s$, $L = 10$

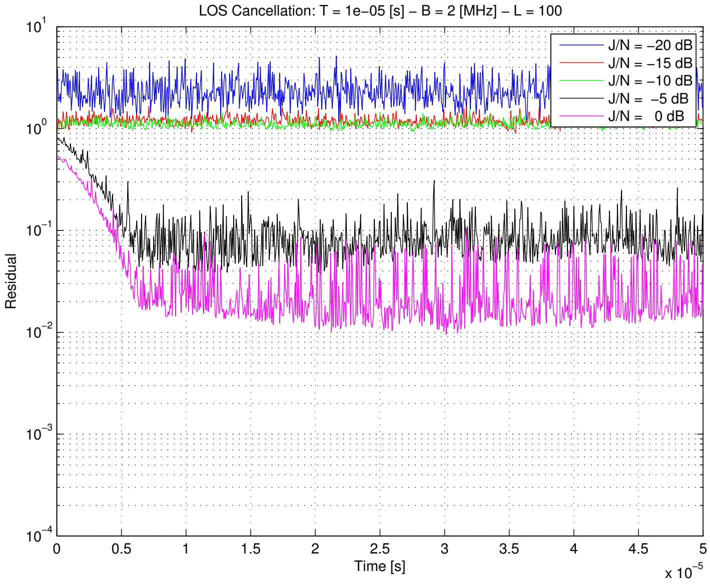


Figure 72: Residual power after cancellation: $T = 10\mu s$, $L = 100$

signal repetition period of $50\mu s$ the residual power is slightly lower and less noisy than the case with a repetition period of $10\mu s$.

2.4.4 *Complexity Evaluation*

The complexity evaluation of the algorithm has been described in Section 2.3.5. In this section the study case of the received signal composed by a single path has been considered, and thus the computational complexity has been defined according to the first version of the algorithm. Consequently, complexity computation in the case of the LOS scenario is perfectly equal to the one reported in the full description of the proposed algorithm in Section 2.3.

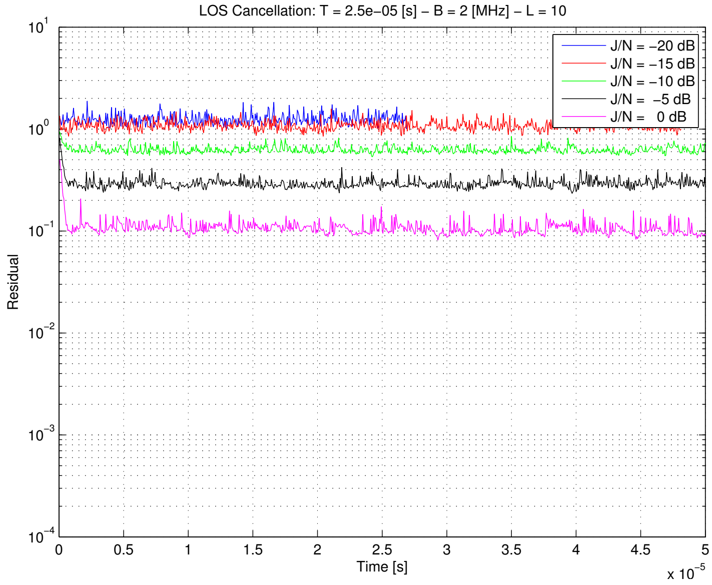


Figure 73: Residual power after cancellation: $T = 25\mu s$, $L = 10$

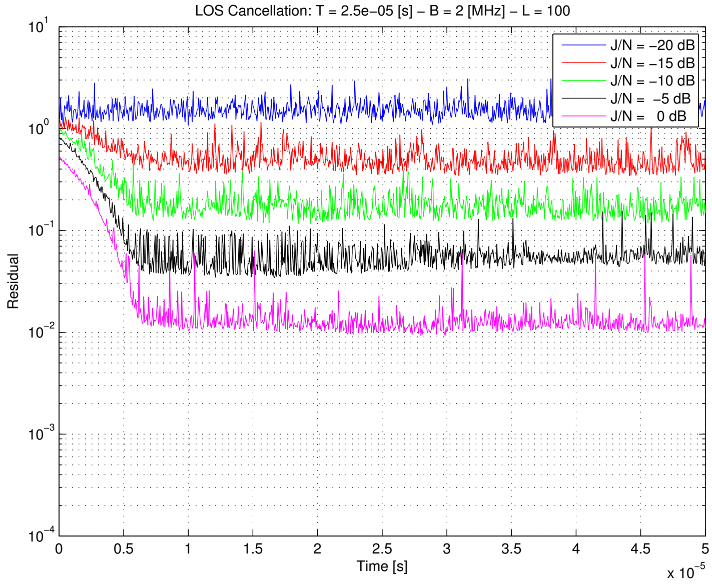


Figure 74: Residual power after cancellation: $T = 25\mu s$, $L = 100$

2.5 MULTIPATH CHANNEL

In the following, a chirp signal is considered and detection and mitigation techniques are described for these signals affected by multipath, *i.e* the interfering signal is subjected by different reflections and the receiver is affected by a jamming made of more contributions.

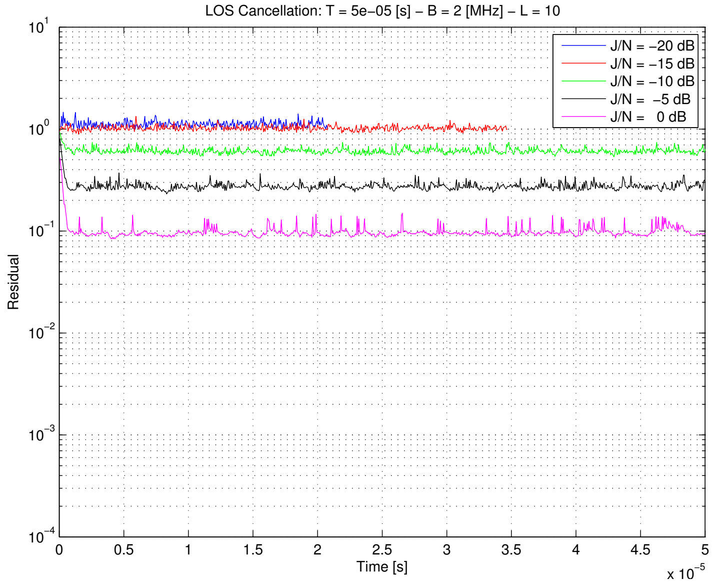


Figure 75: Residual power after cancellation: $T = 50\mu s$, $L = 10$

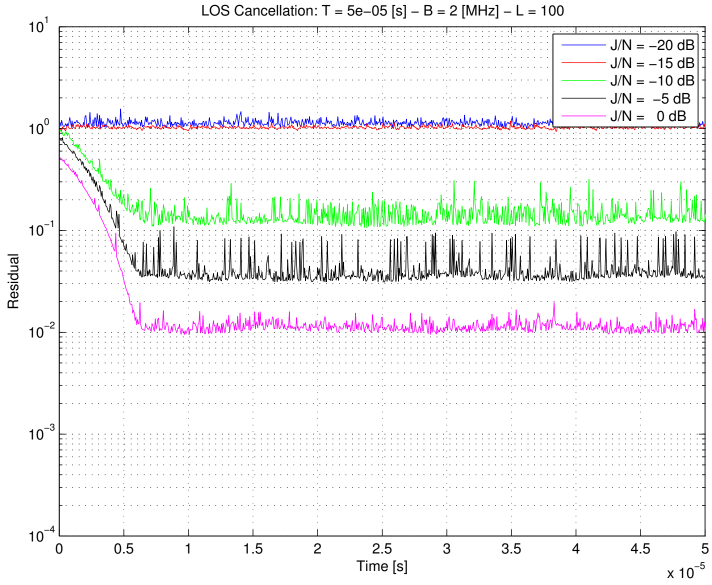


Figure 76: Residual power after cancellation: $T = 50\mu s$, $L = 100$

2.5.1 *System model*

The considered transmitted signal is the same chirp signal used in the non dispersive channel, expressed in eq.(46), which can be written as:

$$s_0(t) = \exp\left\{\pm j\rho\frac{t^2}{2}\right\}\text{rect}\left(\frac{t}{T}\right)$$

and as in the previous case of study only the frequency up-slope case is considered in the following. Successively, the chirp signal is modeled by the multipath channel, which creates several delayed replicas and the received signal is then defined as the sum of this delayed contributions. Thus, the lowpass output signal, generate through the multipath channel, is:

$$\tilde{y}_k = \tilde{s}_k \star \tilde{h}_k = \sum_{i=1}^{N_p} \gamma(m_i)\tilde{s}\,(k - m_i)\exp\{-j\varphi_{k,i}\} \tag{69}$$

where N_p number of replicas, m_i delay of i-th replica at the k-th sampling instant, $\varphi_{k,i} = 2\pi(f_c + f_i)m_i - f_i k$ is the phase offset due to the replica delay and of the Doppler shift $f_i = \frac{v}{\lambda}\cos(\theta_i)$, v is the jamming source velocity, λ is the wavelength and θ_i is the angle of arrival of i-th replica. The equivalent baseband channel is:

$$\tilde{h}_k = \sum_{i=1}^{N_p} \gamma(m_i)\delta(k - m_i)\exp\{-j\varphi_{k,i}\} \tag{70}$$

where $\gamma(m_i) = |\gamma(m_i)|e^{j\arg\{\gamma(m_i)\}}$ is the channel coefficient distributed as complex Gaussian random variable with zero-mean and variance equal to σ_γ^2 $\left(\sim \mathcal{N}_C\left(0, \sigma_\gamma^2\right)\right)$. It is possible to deduce that the channel output $\tilde{y}_k$ is a complex Gaussian random variable equal to the sum of N_p complex Gaussian random variables $\left(\sim \mathcal{N}_C\left(0, N_p\sigma_\gamma^2\right)\right)$. Finally, it is possible to express the received signal as:

$$\tilde{r}_k = \tilde{y}_k + \tilde{w}_k \tag{71}$$

where $\tilde{w}_k$ are complex additive Gaussian white noise i.i.d samples $\left(\sim \mathcal{N}_C\left(0, N_0\right)\right)$.

2.5.2 *Autocorrelation Analysis*

As in the previous section, in order to design a jammer detector the AC function of the received signal is evaluated. It is well known that a structured signal exhibits a periodic envelope and particular AC properties. The AC function is expressed as:

$$\begin{aligned} R_{\tilde{r}\tilde{r}}[k, k+\ell] &= E[\tilde{r}_k, \tilde{r}^*_{k+\ell}] \qquad (72) \\ &= E\left[(\tilde{y}_k + \tilde{w}_k), (\tilde{y}_{k+\ell} + \tilde{w}_{k+\ell})^*\right] \\ &= E\left[\tilde{y}_k, \tilde{y}^*_{k+\ell}\right] + E\left[\tilde{y}_k, \tilde{w}^*_{k+\ell}\right] + E\left[\tilde{w}_k, \tilde{y}^*_{k+\ell}\right] + E\left[\tilde{w}_k, \tilde{w}^*_{k+\ell}\right] \end{aligned}$$

The first term represents the useful term of the AC function, and the others are cross-terms between signal and noise samples which are independent each others. These terms can be considered part of an random variable $z_{k,l}$ with zero-mean and variance equal to the sum of variance of each random variable, that are independent complex Gaussian random variable. The mean is equal to zero because the mean value of each random variable is zero due to the presence of noise; instead, the variance is equal to the sum of variances of the product of independent random variables. Taking into account two independent random variable a, b as in Section 2.3.1.1, the variance of their product is evaluated as:

$$Var\{ab\} = Var\{a\}Var\{b\} + E^2[a]Var\{b\} + E^2[b]Var\{a\} \tag{73}$$

The variance of each product is:

$$\begin{aligned} Var\{\tilde{y}_k \tilde{w}^*_{k+\ell}\} &= \sum_{i=1}^{N_p} \sigma^2_{\gamma,i} * N_0 \\ Var\{\tilde{w}_k \tilde{y}^*_{k+\ell}\} &= \sum_{i=1}^{N_p} \sigma^2_{\gamma,i} * N_0 \\ Var\{\tilde{w}_k \tilde{w}^*_{k+\ell}\} &= N_0^2 \end{aligned} \tag{74}$$

and the variance of the total random variable $z_{k,l}$ is

$$Var\{z_{k,l}\} = N_0(2\sum_{i=1}^{N_p} \sigma^2_{\gamma,i} + N_0) \tag{75}$$

It is worthwhile to notice that assuming the channel coefficients γ independent each others then the variance $Var\{\tilde{y}_k\}$ can be expressed as

$$Var\{\tilde{y}_k\} = \sum_{i=1}^{N_p} \sigma^2_{\gamma,i}$$

; on the other hand if coefficients are not independent the variance is expressed as

$$Var\{\tilde{y}_k\} = Var\{\sum_{i=1}^{N_p} \gamma_i\}$$

The first term of the AC function is defined as the product of two independent complex Gaussian random variables:

$$\begin{aligned} R_{\tilde{y}\tilde{y}}[k, k+\ell] &= E\left[\tilde{y}_k, \tilde{y}^*_{k+\ell}\right] \\ &= E\left[\sum_{i=1}^{N_p} \gamma(m_i)\tilde{s}(k-m_i)e^{-j\varphi_{k,i}}\right. \\ &\quad \left.\cdot \sum_{q=1}^{N_p} \gamma^*(m_q)\tilde{s}^*(k-m_q+\ell)e^{j\varphi_{k+\ell,q}}\right] \end{aligned} \tag{76}$$

Taking into account that the channel is static and that into the time-period T the Doppler shift due to the jamming source velocity is not relevant, then the estimated AC function can be evaluated through the arithmetic mean:

$$\begin{aligned} \hat{R}_{\tilde{y}\tilde{y}}[\ell] &= \frac{1}{L-\ell}\sum_{k=1}^{L-\ell}\left[\sum_{i=1}^{N_p} \gamma(m_i)\tilde{s}(k-m_i)e^{-j\varphi_{k,i}}\right. \\ &\quad \left.\cdot \sum_{p=1}^{N_p} \gamma^*(m_p)\tilde{s}^*(k-m_p+\ell)e^{j\varphi_{k+\ell,p}}\right] \end{aligned} \tag{77}$$

Thus:

$$\begin{aligned}\hat{R}_{\tilde{y}\tilde{y}}[\ell] &= \frac{1}{L-\ell}\sum_{k=1}^{L-\ell}\left[\sum_{i=1}^{N_p}\tilde{h}(m_i)\tilde{s}(k-m_i)\cdot\sum_{q=1}^{N_p}\tilde{h}^*(m_q)\tilde{x}^*(k-m_q+\ell)\right] \quad (78)\\ &= \sum_{i=1}^{N_p}\sum_{q=1}^{N_p}\tilde{h}(m_i)\tilde{h}^*(m_q)\cdot\frac{1}{L-\ell}\sum_{k=1}^{L-\ell}\tilde{s}(k-m_i)\tilde{s}^*(k-m_q+\ell)\\ &= \sum_{i=1}^{N_p}\sum_{q=1}^{N_p}\tilde{h}(m_i)\tilde{h}^*(m_q)R_{\tilde{s}\tilde{s}}[\ell-m_q+m_i]\end{aligned}$$

According to eq.(78) the estimated AC function $\hat{R}_{\tilde{y}\tilde{y}}[\ell]$ of the received signal can be expressed as the linear combination of the AC of the transmitted signal affected by multipath $R_{\tilde{s}\tilde{s}}$ weighted by channel coefficients. In order to estimate the period of the transmitted signal, it is necessary to evaluate the maximum value of the correlation function, rejecting the first maximum corresponding to the beginning of the signal: the correspondent instant is equal to the value of the signal period. In this case with a signal affected by N_p paths the number of all the contributions in eq.(78) are N_p^2: the maximum value corresponds to the case of perfect alignment of the received signal and its delayed replicas, while the other combinations contribute to secondary lobes in the AC function. The expression in eq.(78) is a closed form but it is not an explicit form, so in order to demonstrate the behavior of the AC function it is necessary to evaluate empirically all the possible cases of alignment of the paths.

2.5.3 *Detector Design*

The next step is to define the analytic expression of the decision problem regarding the detection of the correct signal period. The detection problem is defined as a binary decision problem, which is composed by two hypotheses:

- H_1:maximum pick of the AC function. The time instant ($\neq 0$) corresponding to the maximum pick is a multiple of the signal period, obtained when the replicas are perfectly aligned.
- H_0:maximum pick is absent. There are secondary picks due to the several cross-overlapping of the replicas. The assumption is that the AC function is 0.

The AC function of the received signal in eq.(72), can be rewritten as:

$$R_{\tilde{r}\tilde{r}}(\ell) = \sum_{i=1}^{N_p}\sum_{q=1}^{N_p}\tilde{h}(m_i)\tilde{h}^*(m_q)R_{\tilde{s}\tilde{s}}[\ell-m_q+m_i] + R_W(\ell) \quad (79)$$

where the term $R_W(\ell)$ represents all the contributions due to the cross-correlation between signal and noise and the noise autocorrelation function. It is necessary to evaluate the expression of this function under both hypotheses. Under H_1 we consider the perfect alignment of the received signal and its local replicas. According to this, it is possible to derive:

$$\left|\sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^2 R_{\tilde{s}\tilde{s}}(\ell) + R_W(\ell)\right|^2 \tag{80}$$

where:

- $R_W(\ell)$ can be modeled as a Gaussian random variable: $R_W(\ell) \sim \mathcal{N}(0, N_0)$
- $R_{\tilde{s}\tilde{s}}(\ell)$ is deterministic equal to the signal energy E under H_1 and equal to 0 under H_0
- $|h(m_i)|^2$ can be considered as a random variable o a deterministic value
  - deterministic value: each term represents the energy of the i-th delay;
  - random variable: the sum of all these quadratic terms can be modeled as a non central chi-square distribution.

2.5.3.1 *Deterministic Channel Distribution*

In this paragraph the analytic expression of the decision problem in a deterministic case is evaluated. Assuming that $|h(m_i)|^2$ is a deterministic value, the sufficient statistics, under H_1 hypothesis, is expressed as a non central chi-square random variable with $2L$ degrees of freedom $\chi^2_{2L}(d)$, with non centrality parameter given by:

$$\begin{aligned} d &= \left|\sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^2 R_{\tilde{s}\tilde{s}}(\ell|H_1)\right|^2 \\ &= \left|\sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^2 E e^{j\phi}\right|^2 \\ &= \sum_{\substack{i=1^{N_p}\\i=q}} |h(m_i)|^4 E^2 + 2\left(\sum_{j=1}^{N_p}\sum_{\substack{i=1\\j\neq i}}^{N_p} |h(m_i)|^2 \left|h(m_j)\right|^2 E^2\right) \end{aligned} \tag{81}$$

Under H_0 hypothesis the sufficient statistic is expressed as a central chi-square random variable with $2L$ degrees of freedom $\chi^2_{2L}(0)$. Taking into account that under H_0 the AC function of the interfering signal $R_{\tilde{s}\tilde{s}}(\ell)$ is equal to 0, then the sufficient statistic is composed by noise contribution R_W which is modeled as a complex Gaussian random variable.

2.5.3.2 *Random Channel Distribution*

In this paragraph the analytic expression of the decision problem in a random case is evaluated. According to eq.(70), $h(m_i)$ is a complex Gaussian random variable with zero mean and variance equal to σ_γ^2 $(\sim \mathcal{N}(0, \sigma_\gamma^2))$. Thus, the sufficient statistics, under H_1 hypothesis, is expressed as a non central chi-square random variable with N_p degrees of freedom $\chi^2_{N_p}(d)$, with non centrality parameter given by:

$$\begin{aligned} d &= \left| \sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^2 R_{\tilde{s}\tilde{s}}(\ell|H_1) \right|^2 \qquad (82) \\ &= \left| \sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^2 Ee^{j\phi} \right|^2 \\ &= \sum_{\substack{i=1\\i=q}}^{N_p} |h(m_i)|^4 E^2 + 2\left(\sum_{i=1}^{N_p} \sum_{\substack{j=1\\j\neq i}}^{N_p} |h(m_i)|^2 \left|h(m_j)\right|^2 E^2 \right) \end{aligned}$$

It is worthwhile to notice that in this case the non centrality parameter is a random variable due to the presence of $|h(m_i)|^2$. Thus, the non-centrality parameter has a probability density function and the evaluation of the decision problem becomes more complex and difficult to be solved in an analytical way. On the other hand, as for the deterministic case, under H_0 hypothesis taking into account that under H_0 the AC function of the interfering signal $R_{\tilde{s}\tilde{s}}(\ell)$ is equal to 0, then the sufficient statistic is composed by noise contribution R_W which is modeled as a complex Gaussian random variable.

2.5.4 *Numerical Results*

As stated in the previous section, in order to confer effectiveness to our study, empirical simulations have been carried out. In this section all the numerical results of the analytical study carried out in the previous sections are shown as results of several simulations. The performance have been carried out in the same way as the *Non Dispersive Channel*scenario. In the following a multipath scenario is considered according to the *UMTS* standard [26]. In Figure (77) the considered scenario is shown.

In Section 2.5.4.1 the validation of the hypotheses on AC function in a multipath scenario are reported. In Section 2.5.4.2 the result of the detection of an interfering signal in a multipath scenario is shown in terms of probability of detection. In Sections 2.5.4.3 and 2.5.4.4 results on parameter estimation and cancellation residual are shown, respectively.

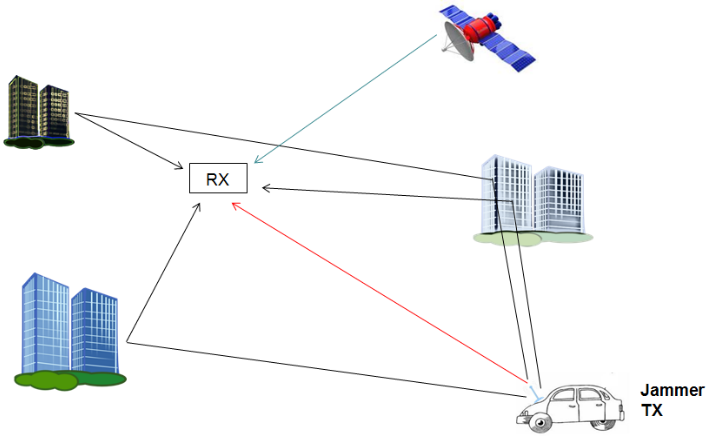


Figure 77: Multipath Scenario

2.5.4.1 *Approximation Validation*

According to eq.(78), the AC function is defined by the sum of $N_p^2 = 36$ terms (6 paths in *UMTS* standard), and as explained before, the maximum value of the AC function corresponds to the perfect alignment between received signal and its delayed replicas, and the other peaks are due to the cross-overlaps between the paths. Let us consider a received signal composed by the sum of three paths with delays $0, 600, 300[ns]$ corresponding to sample delays equal to $0, 10, 48[samples]$, respectively; the other simulation parameters in table 9 are the same.

Type of Signal	Chirp Signal
Min frequency	$0MHz$
Max frequency	$8MHz$
Sampling frequency	$16MHz$
Signal period	$25\mu s$
Signal period	400 [samples]
Time-window	$0.1s$
Number of paths	6
Path Delays	$[0, 310, 710, 1090, 1730, 2510]ns$
Path Powers	$[0, -1, -9, -10, -15, -20]dB$

Table 9: Simulation Parameters

In figure (78) the estimated AC function of a multipath signal with 6 paths is shown. The multipath channel is defined according to the *UMTS* standard model [26]. It is possible to observe the periodic behavior of the AC function with equally spaced peaks, which represent the periodicity of the signal.

In figure (79) a zoom of the previous figure is shown. It is possible to notice that the peaks of the AC function correspond to the signal period in samples and its multiples.

In figure (80) the AC function is shown and it is possible to notice that the major peaks are located in the first $\pm 50[samples]$.

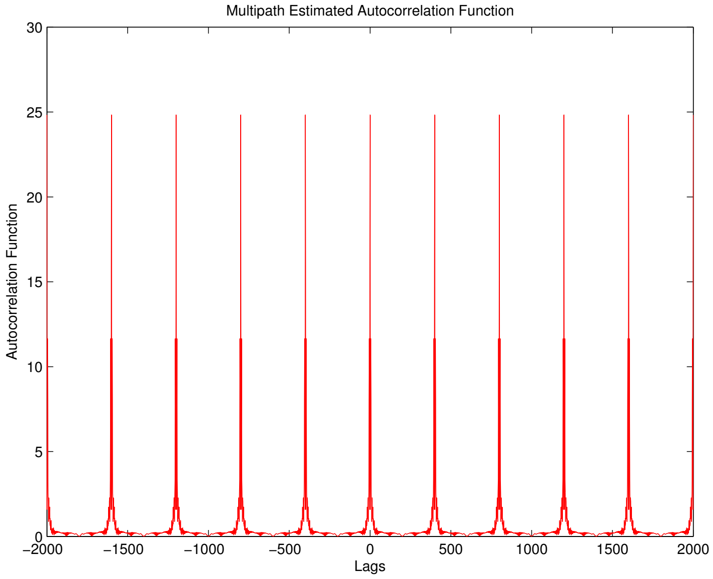


Figure 78: Estimated Autocorrelation function of Multipath signal with 6 paths.

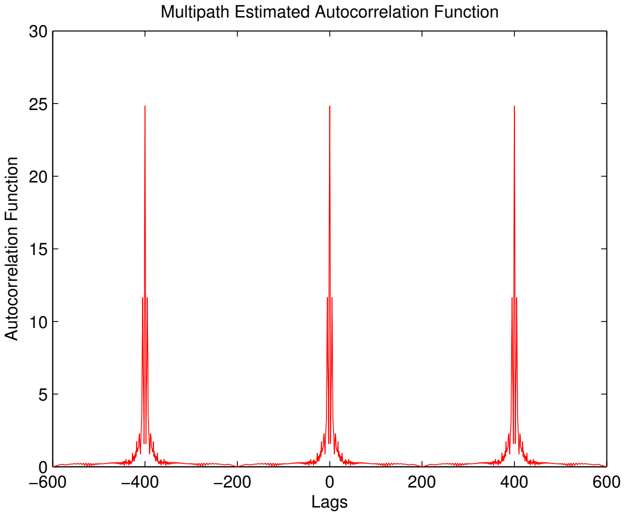


Figure 79: Zoom on Estimated Autocorrelation function of Multipath signal with 6 paths.

In figure (81) a more detailed AC function is shown. It is possible to observe that the major peaks, except that one in 0, are located on lags $\pm 10, \pm 38, \pm 48[samples]$. These peaks are due to the overlapping of the received signal and the local replica. In particular, when the local replica is shifted of :

- $+10[samples]$ the major contribution is due to the overlapping between the second path of the received signal and the first path of local replica (plus other minor contributions);

- $+38[samples]$ the major contribution is due to the overlapping between the third path of the received signal and the second path of the local replica (plus other minor contributions);

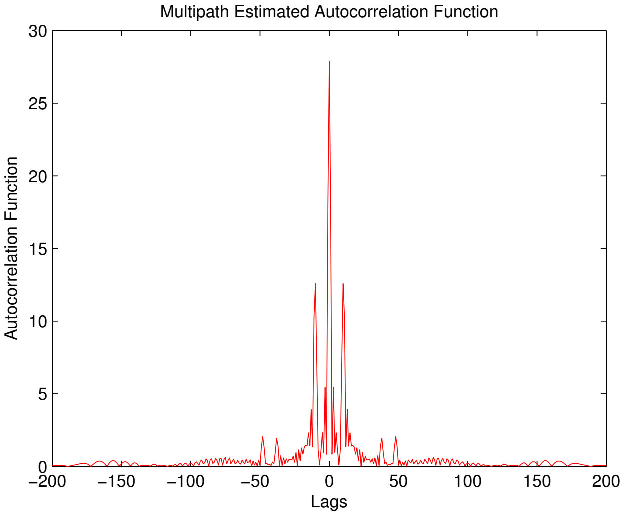


Figure 80: Zoom on Estimated Autocorrelation function of Multipath signal with 3 paths.

- $+48[samples]$ the major contribution is due to the overlapping between the third path of the received signal and the first path of the local replica (plus other minor contributions);

Thus, it is possible to deduce that the maximum value of the AC function corresponds to the perfect alignment of the received signal and the local replica.

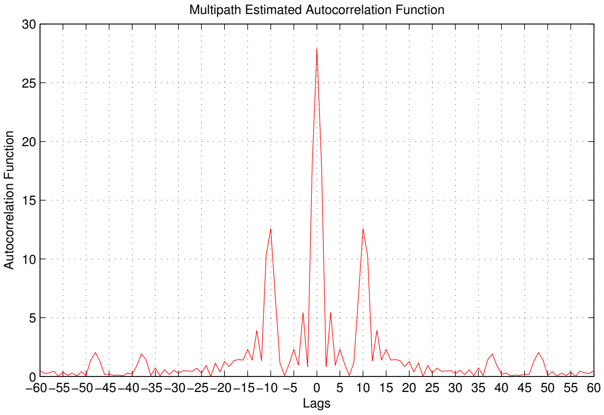


Figure 81: Zoom on Estimated Autocorrelation function of Multipath signal with 3 paths.

2.5.4.2 *ID: Probability of Detection*

According to the theoretical analysis of the binary decision derived in section 2.3.1.2, the detection test has been defined exploiting the ML criterion. The likelihood ratio in eq.(38) depends on the time-shift τ and the bandwidth Δf and it is not simple to compute without any assumption. In *Multipath* scenario the probabilities density functions for both hypotheses are quite different with respect to the LOS case, due to the characteristics of the received signal. For this reason, the analytical expression of the likelihood ratio is different and not simple to derive.

However, the performance of the interferer detection algorithm, described in section 2.3.1, has been carried out in terms of probability of correct detection , i. e.the probability that the interfering signal is present in the received signal, and in terms of probability of false alarm, i. e.the probability that the interfering signal is present when it should not be. The results have been obtained by means of Monte Carlo simulations. Only the probability of detection is shown, since, for the considered simulation settings, a $P_{fa} = 0$ is always obtained due to a large number of Monte Carlo iterations(10^6).

The simulation parameters used in the detection step of the algorithm are listed in table 10.

Type of Signal	Chirp Signal
Min frequency	$-5MHz$
Max frequency	$5MHz$
Sampling frequency	$16MHz$
Signal period	$[10, 25, 50]\mu s$
Number of paths	6
Path Delays	$[0, 310, 710, 1090, 1730, 2510]ns$
Path Power	$[0, -1, -9, -10, -15, -20]dB$

Table 10: Detection - Simulation Parameter

In Figure (82) and Figure (83) the probability of detection in a*Multipath* scenario is reported, in both classic and normalized received power, respectively . It is worthwhile to notice that the probability of detection in Figure (82) is slightly better than the LOS case in Figure (66). This is due to the fact that there is more input energy thus also the secondary peaks are detected when the AC main peak crosses the set threshold. On the other hand, in Figure (83) the performance is worse, due to the normalization in terms of the received power and consequently the AC peaks result powerful without crossing set thresholds. However, the reference threshold is the same used for the LOS case evaluated according to eq.(24), with a value of $J/N = 0[dB]$. As for the LOS case, the performance improves for interferer signal with shorter repetition period.

2.5.4.3 *IWE: Parameters Estimation*

The evaluation of the performance of the parameter etimation algorithm has been deeply described in Section 2.4.3.3 for the LOS scenario. For the *Multipath* scenario the evaluation in terms of MSE for each considered parameters it is quite analytically difficult. This is due to the fact that the received signal is composed by several delayed replicas that complicate the estimation of the true parameter at each repetition period. In addition, in order to define a correct estimation it is necessary to take into account the channel coefficients that characterize the

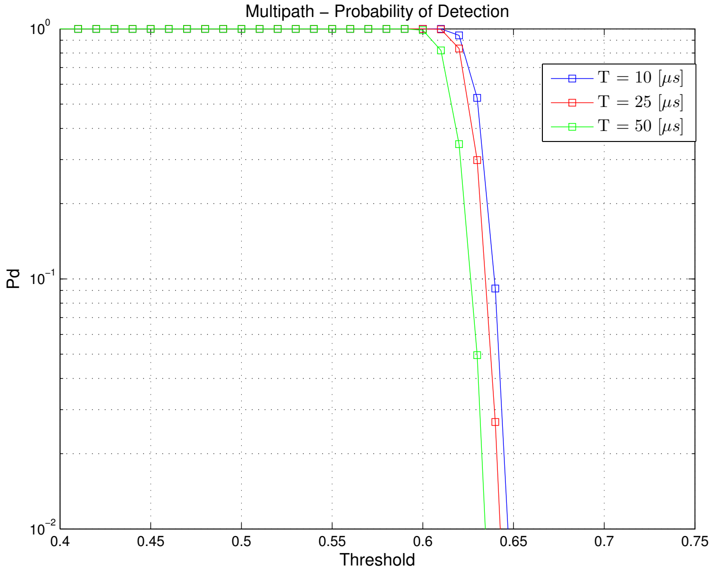


Figure 82: Multipath - Probability of Detection.

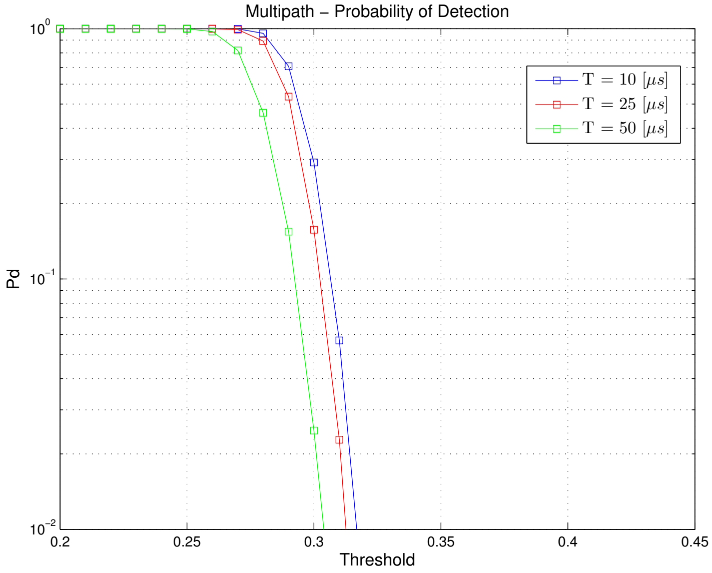


Figure 83: Multipath - Probability of Detection.

considered scenario. All these aspects have to be evaluated at each repetition period and it could be computationally expensive, taking into account that the proposed algorithm does note include any rake receiver method, used to acquire in a fast way the signal affected by multipath.
For these reasons, the parameter estimation evaluation in a multipath scenario is not carried out in our study.

2.5.4.4 *IWM: Cancellation Residual*

As already stated, the performance of the cancellation algorithm depends on the correct parameter estimation results: an accurate parameter estimation determines a reliable signal reconstruction and consequently an effective cancellation can be performed, and a successful

mitigation action can be done reducing the malicious effect. In the following, two different kinds of simulations are shown. First, cancellation residual on varying of time is presented, as already carried out in the LOS case. Successively, cancellation residual in frequency domain is shown, also performing the cancellation in presence of the useful GNSS signal.
For time-varying cancellation results, parameters listed in table 8 are considered, adding the multipath channel model. In Figure (84) - Figure (89) the residual power after cancellation for a chirp signal affected by multipath and generated with three different repetition period is shown. The performance have been evaluated at different values of J/N: the higher the J/N value the lower the residual power ϵ. In addition, as for the LOS scenario, for all the tested cases, the higher the mean tracking length L the lower the residual power ϵ.

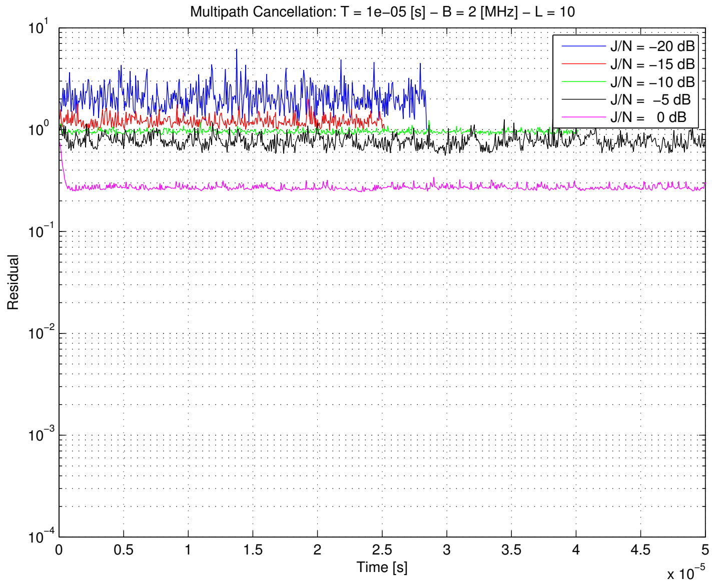


Figure 84: Residual power after cancellation: $T = 10\mu s$, $L = 10$

These results show that the jamming waveform is strongly mitigated in all the tested cases even if the jamming is affected by multipath propagation. The residual power value depends on the adopted mean tracking memory L. At $J/N = 0[dB]$, the residual power value decreases and fixes his own value at $3 * 10^{-1}$ and $4 * 10^{-2}$ for value $L = 10$ and $L = 100$, respectively, defining a difference of quite ten units. This is quite valid for the other J/N values, except for the lowest ones. However, it is possible to notice that the performance are worse than the LOS scenario, as expected. As already stated in the LOS case, the gap of one decade between different values of L is due to the fact that with a larger number of memory stack it is possible to perform a more accurate waveform estimation and consequently a more effective jamming mitigation. In addition, the length of the repetition period affects the results of the mitigation. As the same of the L value, with longer repetition period it is possible to better estimate waveform parameter and then the residual power is lower.
Moving from these results, in the following the performance of the

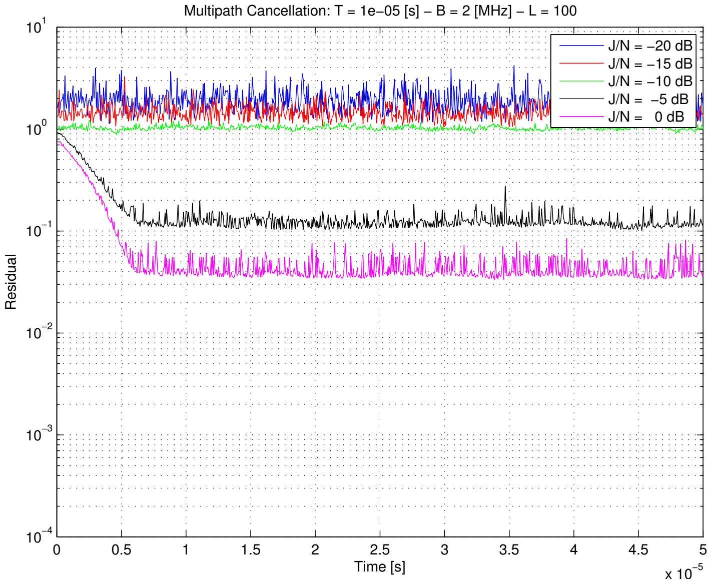


Figure 85: Residual power after cancellation: $T = 10\mu s$, $L = 100$

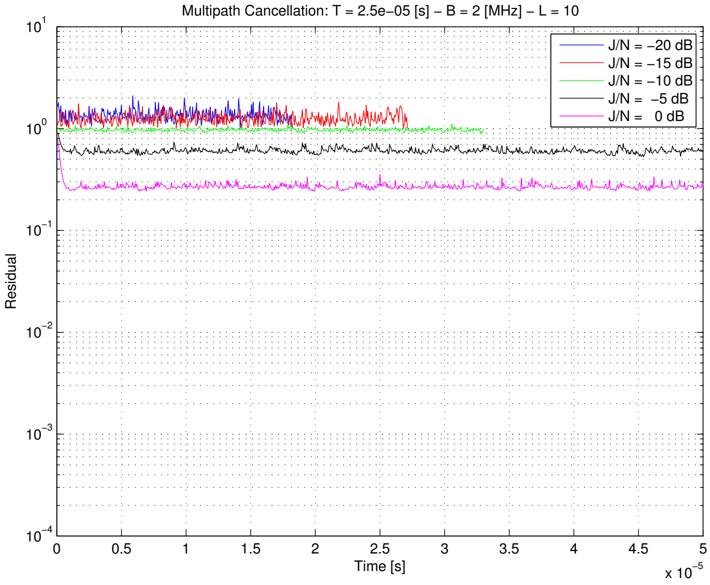


Figure 86: Residual power after cancellation: $T = 25\mu s$, $L = 10$

jamming cancellation in frequency domain is shown. The parameters characterizing the cancellation simulation in the frequency domain are reported in table 11.

In Figure 90, Figure 91, Figure 92 cancellation results are shown. The considered jamming signal is generated with a bandwidth of 8[MHz], a period $T = 10[\mu s]$ and then passes form the multipath channel, defined by 6 taps (according to *UMTS* model). The simulations have been carried out considering a variation of the JNR, for values in the range $-10, 10[dB]$. For value $JNR = -10[dB]$ the residual after the cancellation (red line), evaluated as the difference between the received signal (blue line) and the estimated waveform (green line), is equal to 10^1. For value $JNR = 0[dB]$ and $JNR = 10[dB]$ the residual stops itself at value 10^0 and 10^{-1}, respectively. The residual decreases from 10^1 to 10^{-1} increasing the JNR from $-10[dB]$ to $10[dB]$, thus

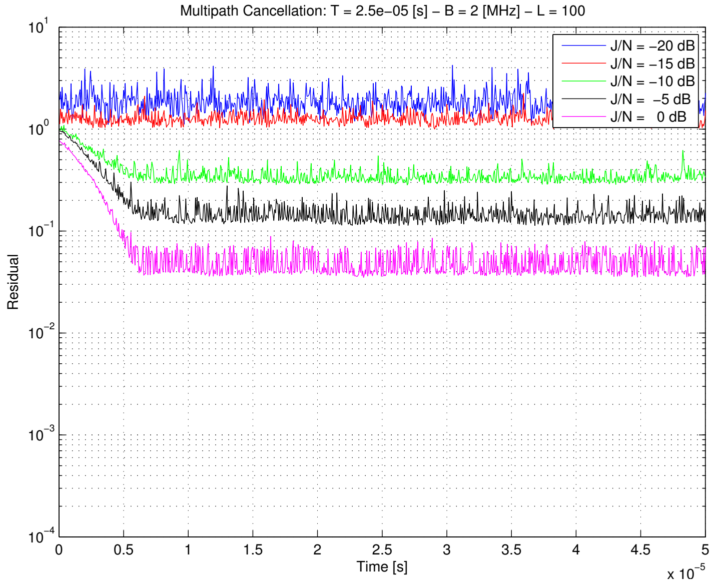


Figure 87: Residual power after cancellation: $T = 25\mu s$, $L = 100$

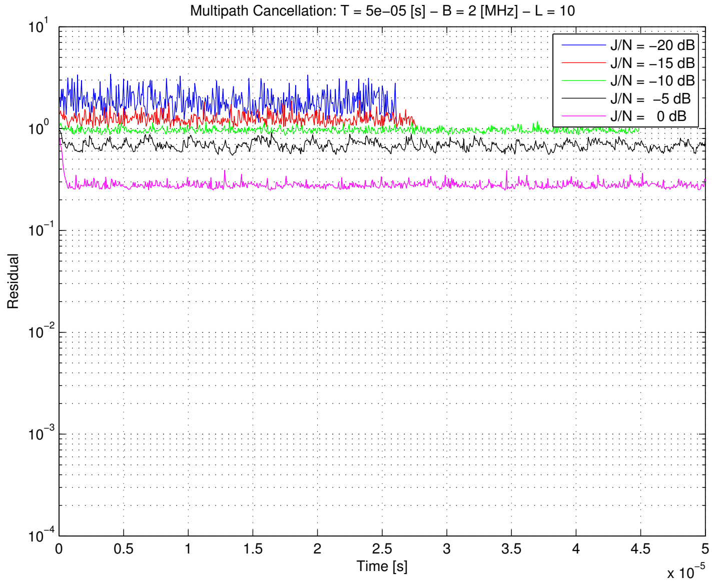


Figure 88: Residual power after cancellation: $T = 50\mu s$, $L = 10$

higher is the considered JNR more efficient are the estimation and cancellation results, as expected.

In Figure 93 and Figure 94 shown results have been obtained on variation of the memory tracking length L. It is worthwhile to notice that the waveform estimate (green line) is less noisy in case of $L = 100$ than with $L = 10$ because with a greater memory stack a more effective average can be performed, reducing the noise power.

In Figure 95 Figure 96 and Figure 97 a different analysis is given, accordingly to the variation of the jamming signal bandwidth. Decreasing the value F_s/f_M and thus increasing the bandwidth, the jamming spectrum becomes more spread and lower, as expected.

Furthermore, improved results have been carried out. In the following figures, the performance is still evaluated in terms of residual after cancellation, but now also the GNSS signal is considered, and it

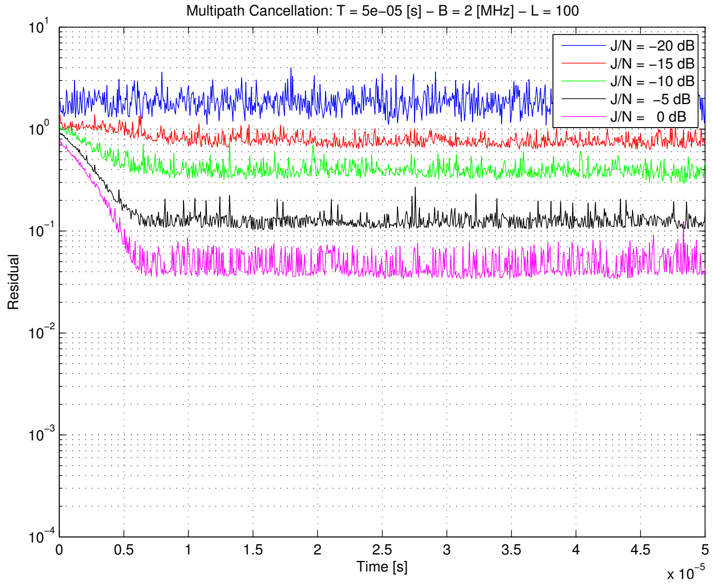


Figure 89: Residual power after cancellation: $T = 50\mu s$, $L = 100$

Type of Signal	Chirp Signal
Sampling frequency	$16MHz$
Min frequency	$0MHz$
F_s/f_M	$[10, 5, 2]MHz$
Max frequency	$[1.6, 3.2, 8]MHz$
Signal period	$[10, 25, 50]\mu s$
Number of paths	6
Path Delays	$[0, 310, 710, 1090, 1730, 2510]ns$
Path Power	$[0, -1, -9, -10, -15, -20]dB$
Mean Tracking Memory	$L = [10, 100]$

Table 11: Cancellation - Simulation Parameter

is added to the jamming signal. The considered GNSS signal is a Binary Offset Carrier (BOC) and in particular is a BOC(1,1), synthesized in MATLAB tool. It is worthwhile to underline that the GNSS signal is not affected by multipath propagation but it is assumed it is in LOS propagation.

In Figure 98, Figure 99 and Figure 100 cancellation results are shown. Now, the residual (red line) has the same envelope of the BOC spectrum. It is possible to notice that increasing the JNR from $-10[dB]$ to $10[dB]$ the residual decreases from 10^1 to 10^{-1}, as exspected. Moreover, with higher JNR the BOC spectrum more with the main lobes higly identifiable.

Also in this case, the estimation is better with a greater mean memory tracking L. In Figure 101 and Figure 102 results are shown, highlightening that the waveform estimate (green line) is still less noise with $L = 100$ than $L = 10$, as espected.

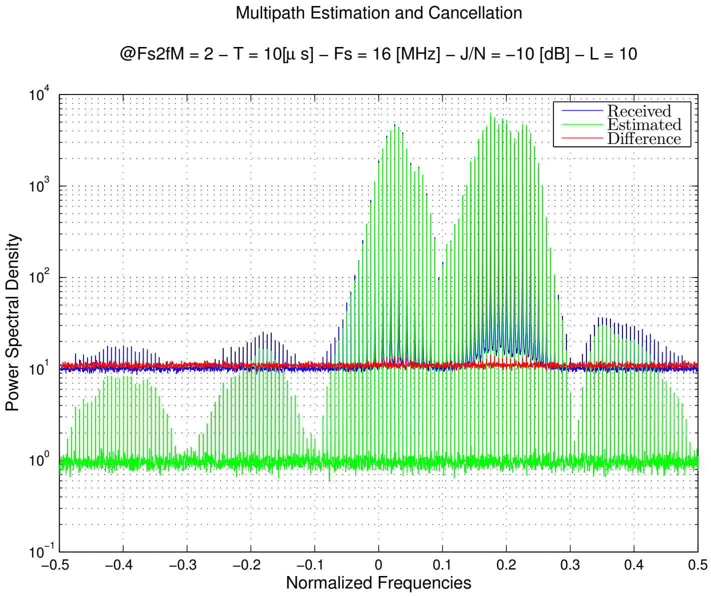


Figure 90: Multipath Cancellation Residual - JNR $= -10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

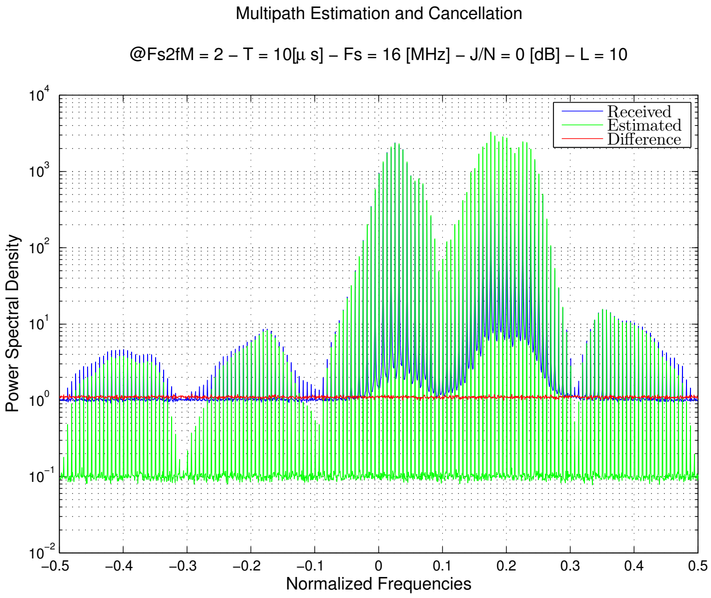


Figure 91: Multipath Cancellation Residual - JNR $= 0\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

In Figure 103, Figure 104 and Figure 105 cancellation performance is defined on the variation of the jamming bandwidth. As described for the previous case, decreasing the the value F_s/f_M interfering bandwidth increases. Even if a BOC signal is present, the cancellation is effective for all the considered values, with acceptable results also for worse case scenario JNR $= 0[\text{dB}]$.

In this section numerical results of the cancellation of a jamming signal affected by multipath have been showed. Results demonstrate that the ICC algorithm is still efficient in worse scenario, as urban canyon and high reflecting areas. Performance have been evaluated

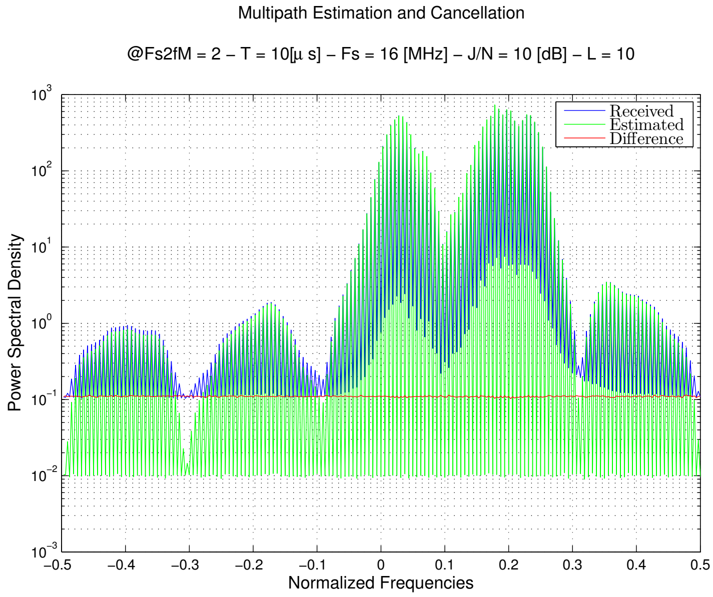


Figure 92: Multipath Cancellation Residual - $\text{JNR} = 10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

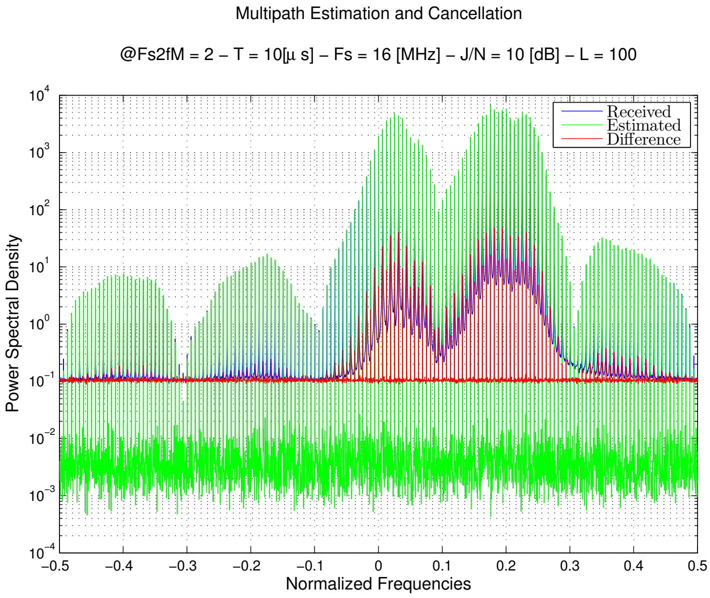


Figure 93: Multipath Cancellation Residual - $\text{JNR} = 10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 100$

also in presence of a BOC signal, in order to emulate as better as possible real scenarios. Also in this extra study-case the algorithm still works and it is able to perform jamming mitigation and thus to extract useful information.

2.5.5 *Complexity Evaluation*

As already done for the LOS case, it is necessary to estimate the computational complexity of the proposed algorithm in the study-case scenario. The algorithm is defined by four steps and for each of them a complexity evaluation has been already carried out in Sec-

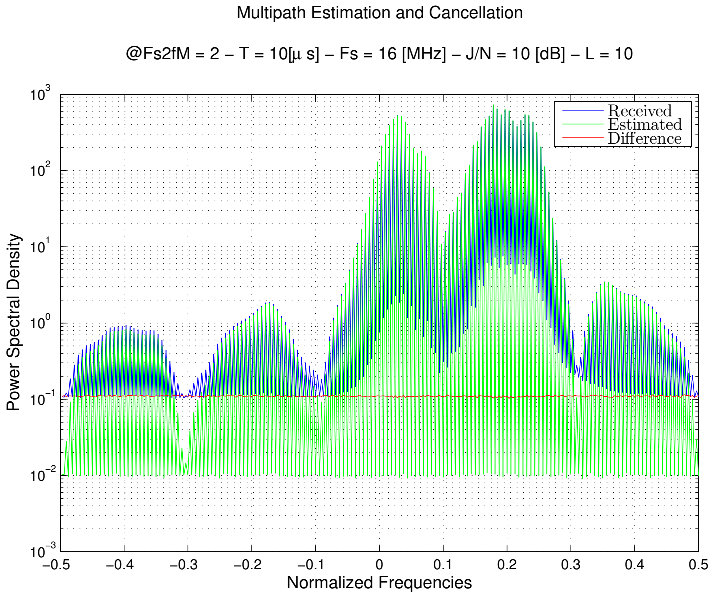


Figure 94: Multipath Cancellation Residual - JNR $= 10\text{dB} - F_s/f_M = 2 - T = 10\mu\text{s} - L = 10$

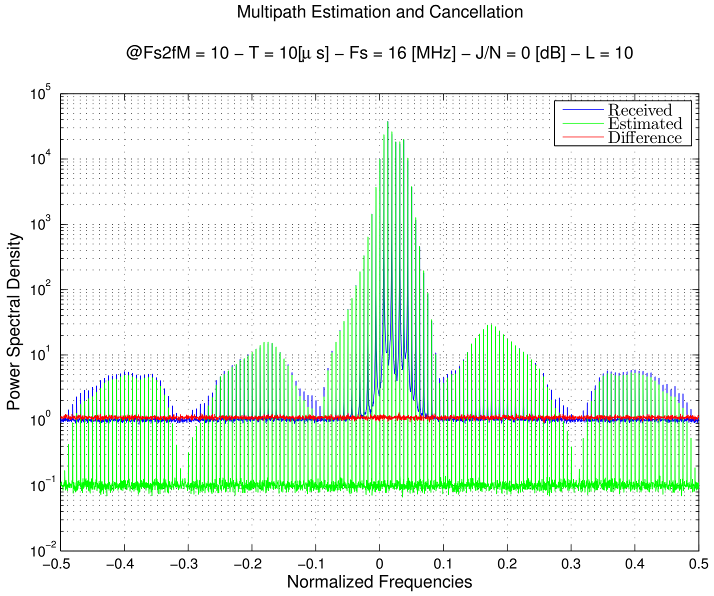


Figure 95: Multipath Cancellation Residual - JNR $= 0\text{dB} - F_s/f_M = 10 - T = 10\mu\text{s} - L = 10$

tion 2.3.5.1, Section 2.3.5.2,Section 2.3.5.3. It is worthwhile to notice that the application of the shown algorithm in *Multipath* scenario does not require any modification. It was supposed that the solution might consist in a simple replication in parallel of the ICC algorithm (described in [28],[29]) into a sufficient number of branches to match all the significant multipath components. Instead, the main idea of this approach comes from recognizing that propagation through a time-dispersive channel does not destroy, but rather transform, the AC structure of a waveform. By exploiting this characteristic, it is possible to preserve the ICC algorithm and to apply it in a non dis-

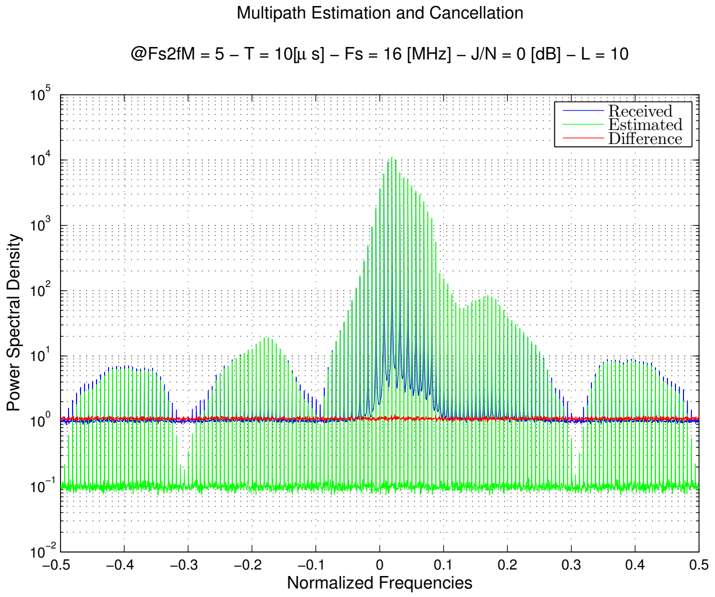


Figure 96: Multipath Cancellation Residual - $\text{JNR} = 0\text{dB} - F_s/f_M = 5 - T = 10\mu s - L = 10$

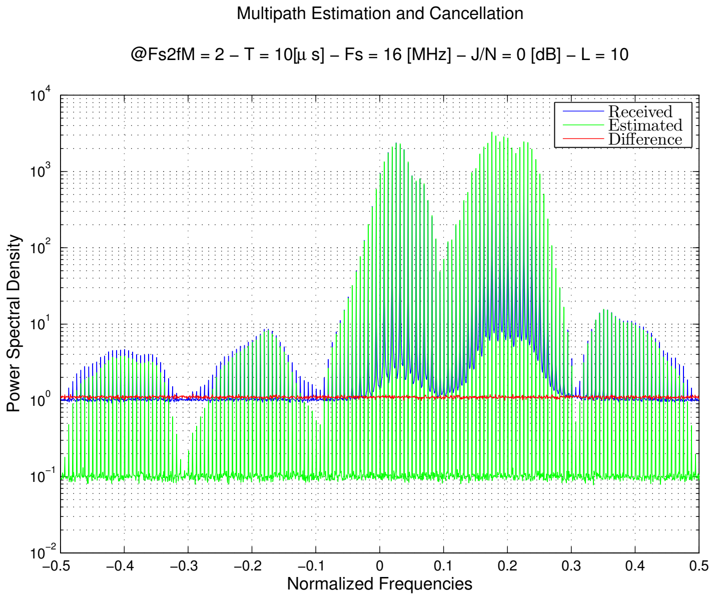


Figure 97: Multipath Cancellation Residual - $\text{JNR} = 0\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

persive channel, without increasing the complexity of the proposed approach.

2.6 CONCLUSIONS

In this chapter a solution for the management of jamming signal in a Multipath scenario was presented. The whole study was only focused on the interfering signal neglecting the useful one. First, a study of the jammer through the non dispersive channel was carried out. Starting from the results shown in [28], an analytical study was presented in order to expand the ICC algorithm already explained in [29]. In the

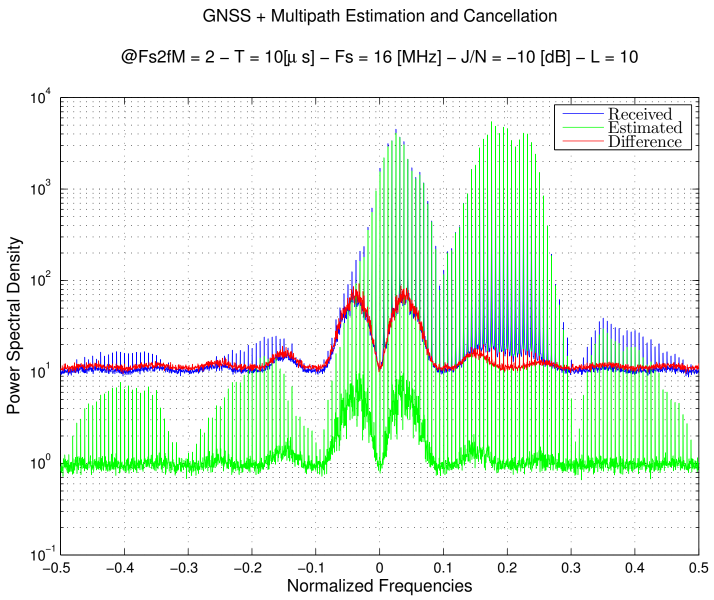


Figure 98: Multipath Cancellation: Residual & GNSS - JNR $= -10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

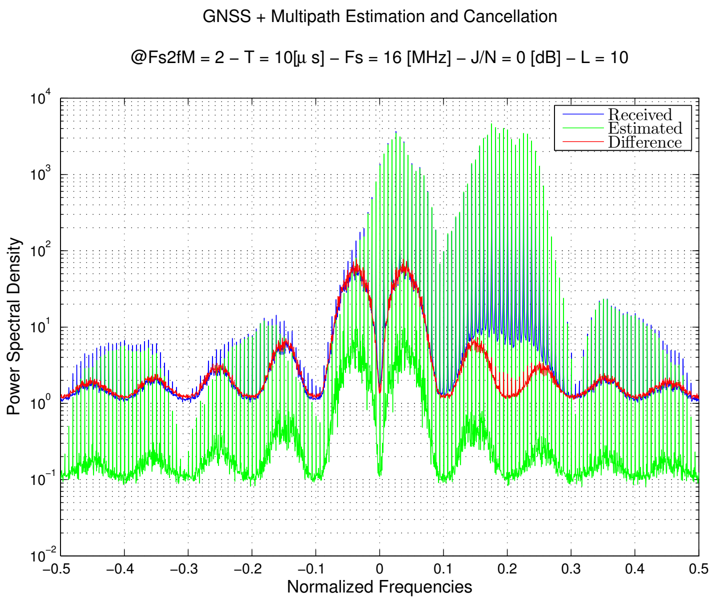


Figure 99: Multipath Cancellation: Residual & GNSS - JNR $= 0\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

first part of the chapter the attention was focused on the analytical study of the AC for a chirp signal. The analytical expression of the AC function was then used to design the matched detector in order to detect as well as possible the presence of the jamming signal. Numerical results showed that the performance by means of probability of detection was slightly better in case of an optimized detector, due to the higher energy of the detection test (in the same way as for a matched filter). Regarding the estimation and mitigation steps, simulation results were showed in [28] and [29].

In the second part of the Chapter, the attention was focused on the study of the jammer affected by multipath. The dispersive channel

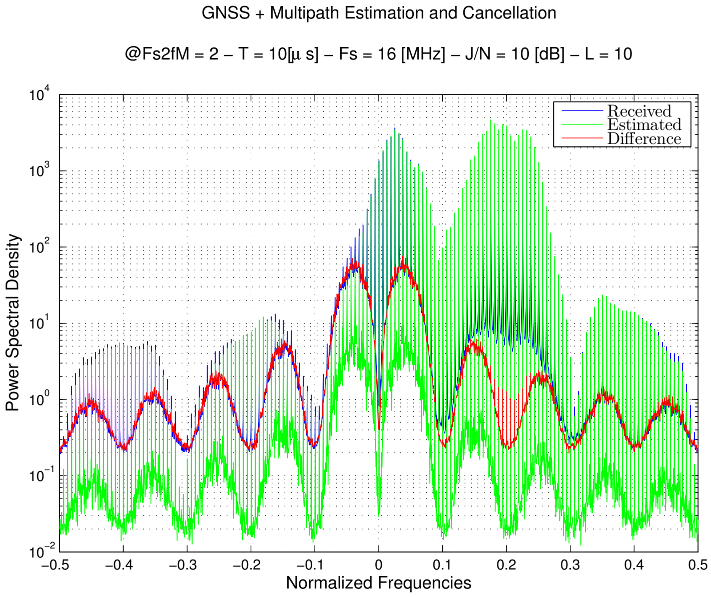


Figure 100: Multipath Cancellation: Residual & GNSS - JNR $= 10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

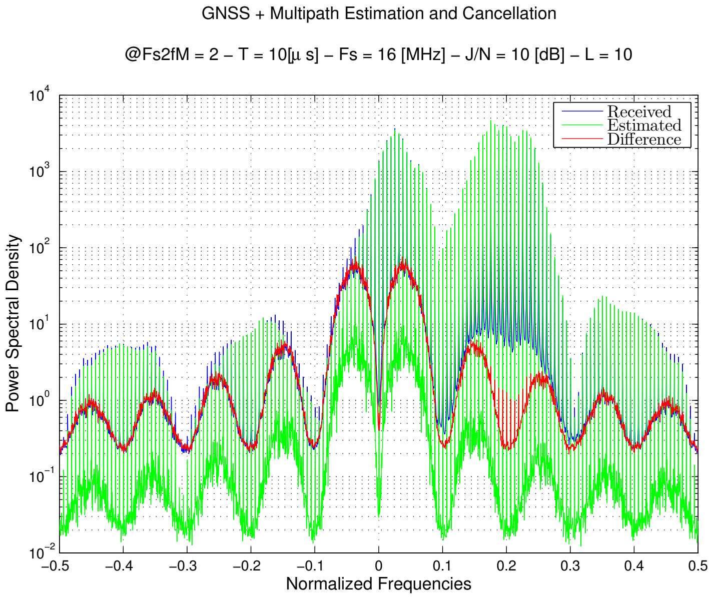


Figure 101: Multipath Cancellation: Residual & GNSS - JNR $= 10\text{dB} - F_s/f_M = 2 - T = 10\mu s - L = 10$

has been defined according to the *UMTS* standard [26]. In addition, the useful signal has been neglected in order to focus on the interfering event. The considered jamming signal was a chirp signal, with periodic envelope and structured characteristics of the AC function. Due to the dispersive propagation, the received signal was defined as the sum of all the delayed replicas, with different received power, different delays and phases at the receiver side. Then, as for the LOS case, an analytical study of the AC function with a multipath signal was proposed. Through this evaluation, it was possible to define the AC function as a linear combination of the delayed replicas weighted by the channel coefficients. Simulation results showed that

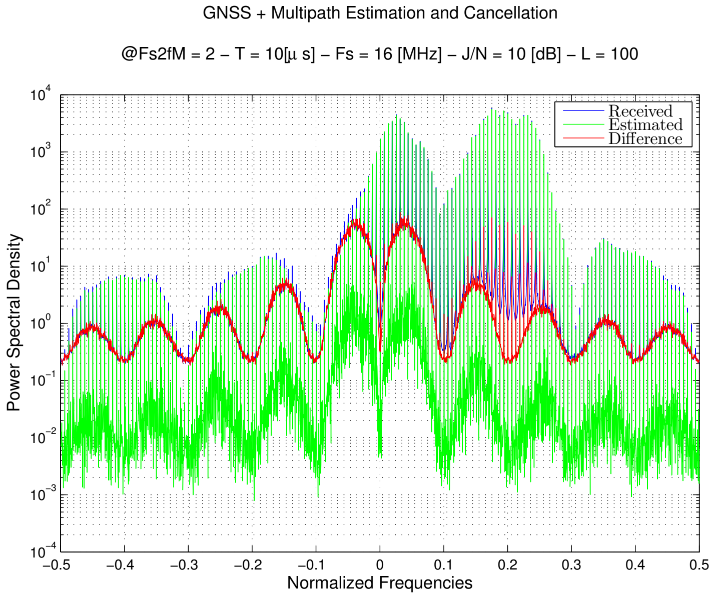


Figure 102: Multipath Cancellation: Residual & GNSS - JNR = 10dB − $F_s/f_M = 2 - T = 10\mu s - L = 100$

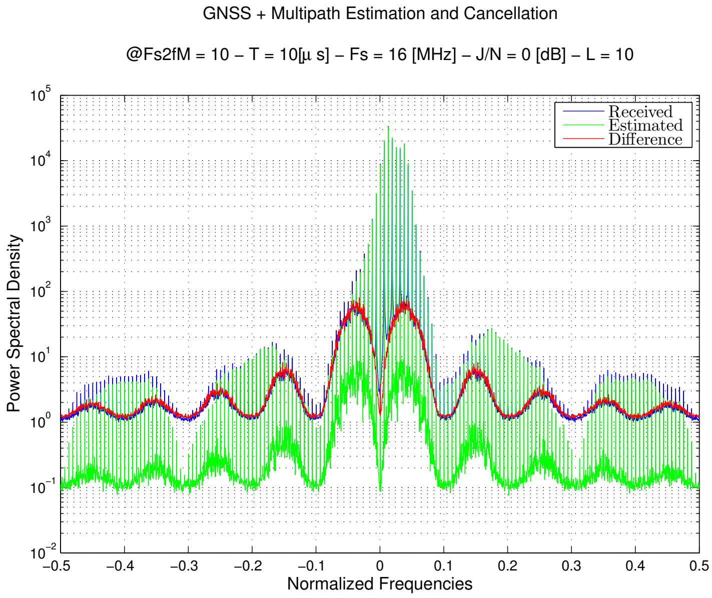


Figure 103: Multipath Cancellation: Residual & GNSS - JNR = 0dB − $F_s/f_M = 10 - T = 10\mu s - L = 10$

this mathematical expression is valid due to the fact that the AC function presents more than one secondary peaks, due to the overlapping of the delayed replicas. Successively, the detection of the interferer was carried out exploiting the properties of the AC function as for the non-dispersive channel. The performance of the detection step was determined through the evaluation of the probability of detection. Numerical results showed that in case of signal affected by multipath the detection is slightly better than the LOS case due to the presence of important secondary peaks that increases the probability of detection. In addition, the algorithm was tested also in terms of residual power cancellation. Results showed that even if the signal is composed by

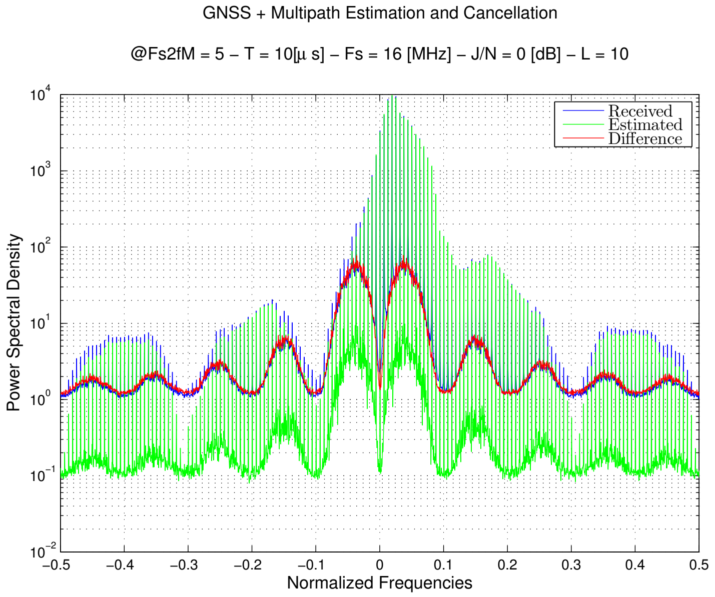


Figure 104: Multipath Cancellation: Residual & GNSS - JNR $= 0$dB $-$ $F_s/f_M = 5 - T = 10\mu s - L = 10$

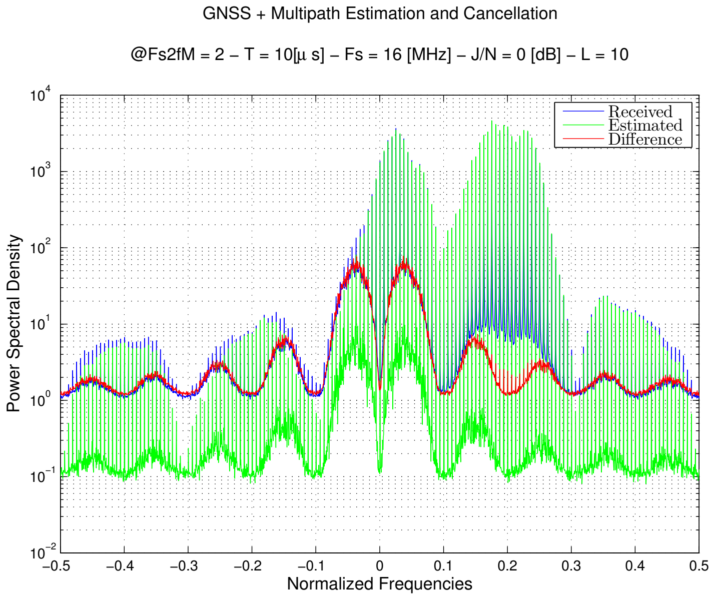


Figure 105: Multipath Cancellation: Residual & GNSS - JNR $= 0$dB $-$ $F_s/f_M = 2 - T = 10\mu s - L = 10$

delayed replicas, the algorithm is able to estimate and reconstruct the signal and then to subtract it from the received one. Thus, the mitigation step still works also for the dispersive channel scenario. Furthermore, the procedure is still effective also in presence of the GNSS signal. As matter of fact, in the estimation stage it is possible to reconstruct the jamming signal, which have higher energy than the useful one, and after mitigation the received spectrum is defined by only the useful signal. Consequently, the GNSS signal is not removed with the interfering signal but it is extracted from the received signal after the jamming cancelation. Even if the tested signal is a simulated signal, the results showed in this chapter demonstrate that the extension to the *Multipath* scenario is a valid solution to counteract jamming signal propagating in a urban scenario, and so to make more reliable the GNSS transmission also in complex environment. In addition, the extension of the algorithm to a dispersive channel scenario was performed without any modification to the main structure of the proposed procedure, thus without increasing the complexity of the algorithm and making the procedure implementable.

INTERFERENCE MANAGEMENT TECHNIQUES: FURTHER DEVELOPMENTS

It is well known that interference in GNSS is still an open challenge. In the previous chapters some approaches have been described. In the final chapter it has been shown that it is also possible to mitigate a jamming in worse scenario, introducing a possible research direction in the future developments.

Even if several literature works have been proposed and several techniques deeply investigated, improvements can be carried out. In this part I detection and mitigation techniques have been described. It has been shown that lower is the signal power, more difficult is the detection and consequently the mitigation, as expected. The whole study has been focused on the statistical characterization of the jamming event neglecting the useful GNSS signal. For this reason, the provided approach has been evaluated for lower power level of the interfering signal, even if the impact on the useful signal is not effective.

In addition, the mitigation step is still an open topic. In the second part of the second chapter it has been demonstrated that jamming signal can be mitigated also when affected by multipath propagation. The used method exploits the periodic characteristic of the interfering signal. The obtained results are an useful start for further developments in this direction. In particular, the attention will be focused on the increasing problem represented by the spoofing signal that is more complex than the previous jamming signals, considered in the described results.

Due to this, efficient anti-jamming and anti-spoofing techniques will be needed in order to counteract with more sophisticated disturbances and guarantee the reliability of the GNSS infrastructure.

Part II

SPOOFING THREAT

Spoofing is notoriously classified as the most dangerous threat of the GNSS infrastructure. Its main goal is to mislead the receiver tracking it and sending wrong information about its position. The receiver is not conscious of this attack, and it acquires the counterfeit signal and discards the authentic one. The rapid diffusion of GNSS location-based applications in a large set of human activities makes the navigation system infrastructure very vulnerable against malicious attacks which aim to disrupt the functionalities for illegal purposes. Taking into account this scenario, efficient and computationally efficient detection and mitigation techniques are required in order to counteract spoofing signals.

The aim of this part II is to present possible and simple approaches in the spoofing detection field. Scenarios affected by spoofing signals are considered and detection methods are described pointing out the principal steps and possible applications, without neglecting drawbacks.

3 SPOOFING IN GNSS

3.1 INTRODUCTION

The easy accessibility to the GNSS signal combined with a non security feature, as a cryptographic signature, in the signal modulation and data streams, makes civil infrastructures using open GNSS strongly vulnerable to jamming and spoofing attacks due to the predictability of open GNSS signals. RFI is considered as the most disruptive event for the GNSS system. As reported in [45][11], RFI affects the operation of the AGC and Low Noise Amplifier (LNA) in the RF front-end and it can also deny the correct functions of carrier an code tracking loops [14][10], causing deterioration and loss of lock in signal reception [36][76]. Thus, due to the high possibility of such attacks, the GNSS security is a very important topic and consequently intentional interfering attacks are a serious threat for the overall navigation system, considering the rife diffusion in the daily human life applications as emergency and safety-of-life ones [1]. In [74] and [78] an exhaustive evaluation of the spoofing threat in civil GPS infrastructure is provided. However, the attention is focused on the increasing risk of successful spoofing attacks due to the easy accessibility and cheap costs of the hardware and software equipment. Accordingly, it is possible to trick a receiver transmitting a counterfeit signal with false estimates of PVT solutions, without any awareness due to the intrinsic reliability on the receiver output. If an attack is successful the navigation solutions are not reliable and the consequences are obvious, as misleading the navigation receiver. The aforementioned problem is debated within the chapter analyzing the effects on the GPS L1 frequency signal, considerations that can be extended to other types of signals an navigation systems. Interference is a difficult threat for the GNSS infrastructure, and different type of jamming signal can be identified. Among them, the major issue is represented by the GNSS-like signals as meaconing and spoofing, as well. The former is the most simplistic way to generate a satellite navigation signal. In order to define a meaconing attack, it is necessary to have a passive antenna which receives the useful signal, then an amplifier and a transmission antenna which works at the same GPS frequency of the useful signal. All the receivers close to the jamming source detect the broadcast signal and decode the previous antenna position and not their own. It is possible to detect the presence of a meaconing attack if the rebroadcast signal has a higher power than the original signal. The latter instead is more sophisticated. It can be made by a GPS generator and then it is broadcast. In [36] a sophisticated case is provided. The spoofer was located close to the GPS receiver

[1] Described in: [36][74][67][68][69][79][46][38] [34][35][78]

in order to acquire the signal characteristics. Successively, the jammer was able to reproduce the signal and by slowly increasing its own transmitting power it captured the target receiver that tracked the counterfeit signal, thus decoding wrong PVT solutions. Authors showed that spoofing goes beyond the aim of denying the correct communications between transmitter and receiver, but its own aim is to mislead the target receiver sending incorrect position and time information. In this chapter possible approaches to counteract spoofing events are discussed. Taking into account all the results provided in [4], we proposed possible improvements exploiting AGC properties jointly to other metric measurements of the GPS receiver. The following sections will present a survey of the previous approaches and countermeasures in RFI and spoofing detection with particular attention on Signal Quality Monitoring (SQM) and AGC-based techniques. First, a brief introduction of the existing techniques is provided in Section 3.2. In Section 3.3 a well referred to SQM approaches review is reported. Successively, in Section 3.4 the concept of the AGC is described also in its application as a spoofer detection combined with the correlator and C/No measurements. Numerical results have been carried out studying and extracting information from collected data and they are showed in Section 3.5 in order to validate our approach. Finally, in Section 3.6 conclusions are provided with possible improvements.

3.2 LITERATURE SURVEY

At the beginning of GPS working system, several studies showed that the the recent systems could be susceptible to intentional jamming attacks. The countermeasure was to introduce a Y-code component to the military P-code signal in order to guarantee a reliable and effective transmission [37][75]. Apparently, these methods was recognized as a powerful technique in order to limit and avoid spoofing attacks. The drawback was that researchers did not take into account the possibility of spoofing attacks in civil infrastructure [60][57],[50]. This method assumed that the encrypted P(Y)-code is free of spoofing, and a reference receiver set at a safe location that is not subject to spoofing. The user receiver is the possible spoofing victim. Statistic of cross correlation between two receivers allows detecting the spoofing at a victim receiver. Although, it requires a secure communications link and a second receiver in order to exploit correlation properties it is still one of the more effective low computational methodologies proposed to date and it leverages the existing military signals.

Furthermore, it could be possible to design civil signal waveform which have intrinsic anti-spoofing capabilities. These have been investigated and candidates proposed [66]. In any case, the signal design cycle is extremely long and it requires modifications in GNSS infrastructure, so it is hard to implement these new waveforms in the near future.

A possible detection approach is defined by observing the behavior of the user's position or time estimates, usually for less sophisticated jamming attacks. If an unrealistic time-position jump occurs, as determined by the navigation Kalman filter, this could be used as flag of spoofing event. Several examples have been presented in [62][77].

Similarly, Receive Autonomous Integrity Monitoring (RAIM) techniques are able to detect malicious events. These techniques can be employed at position solution level and they are quite effective for the less sophisticated attacks. These methods are not computationally expensive though the single epoch mechanism for detection is quite sensitive to the jump magnitude-filter tuning. However, RAIM techniques work very well only if few spoofing events occur among several authentic solutions. On the other hand, if the majority of the signals are spoofed RAIM techniques discard the authentic signal, cause the main goal is to minimize the residual among received solutions.

In case of a single GPS antenna, detection can be performed leveraging a well-known technique based on adding inertial sensors and also cross checking the consistency of dynamics [82][47]. This method tests a residual between GPS spoofed measurements and inertial measurements, and monitors their discrepancies. Due to the availability and low cost of multi-axis MEMS accelerometers, the implementation of these techniques should be quite effective to consider and cross-compare reported movement, raising a confidence flag when they do not agree. However, the majority of common GPS receivers do not have such sensors. Furthermore, low cost inertial sensors are effective only in a short space of operating time under continuous spoofing environments, besides high-end sensors are more expensive than GPS receivers.

Spoofing detection and mitigation techniques could be defined modifying the pattern of the receiver's antenna. The GPS antenna is either omnidirectional (mobile devices) or hemispherical (fixed locations) and receives signals from all directions. A multi-antenna receiver can implement array techniques to steer beams toward the known direction of the satellites and nulls toward interfering power sources. Thus, the antenna array is one of the few methods that can both flag and attempt to mitigate a potential spoofing event when it occurs. Researchers have also proposed a synthetic array, applicable for a single antenna dynamic receiver, which is able to determine the presence of a spoofing source. It is functional but it has the drawback of increasing complexity and it is only applicable for a single stationary spoofing source [56][20].

The major limitation of spoofing is how it transmits the counterfeit GNSS signals. The fake signals are transmitted by the same wireless channel and they have the same propagation characteristics, regardless if the GNSS receiver is moving or not. A signal spatial correlation test was conducted to detect the spoofing [17]. The counterfeit signals are spatially correlated even if the GNSS antenna receiver is moving along an arbitrary trajectory. The detection technique was based on the monitoring of amplitude and Doppler correlation between all (fake and authentic) tracked signals. The presence of a spoofing attack is defined when a pairwise correlation is evaluated. However, it is worth to notice that this method was carried out in a scenario where multipath fading was absent and considering a fixed/stationary spoofing source.

Another possible technique consists in observing the channel components of the tracked signals. In [5] the described detection technique is based on the analysis of multipath components that affect GNSS signals propagation. A spoofing signal could be considered as a delayed replica of the authentic GNSS signal. The fundamental aspect is to observe the behavior in term of amplitude, delay and phase component of all the tracked paths. In case of a spoofing event these three parameters have different time envelope with respect to the multipath reflection. For example if the delay increases but the amplitude does not decrease as expected, according to the rules of multipath propagation, the presence of spoofing could be determined. A pre-despreading detection technique is presented in [42]. It consists in observing GNSS signal features in order to assess the presence of a spoofing signal before the de-spreading stage of the GNSS receiver. This technique operates on raw samples data looking at the abnormal behavior of the signal power content of the GPS spectrum. In this way a counterfeit event could be detected in the digital domain, exploiting the Delay and Multiply (DAM) property of the GPS code when the spoofing event has enough power to interrupt normal receiver's operation. In [44] a spoofing detection and protection technique is described. This method consists in statistical tests of Doppler, C/No and PVT solutions and relies on the information that the receiver obtained before the suspected spoofing attack. All these steps are performed by an independent module in the receiver operation chain that is able to keep memory of the GNSS signal's statistics. The proposed tests are based on monitoring the variance of Doppler offset and C/No which change with the presence of spoofing, defining distortion in the metrics. Once the spoofing is detected, the receiver uses stored information to start the correct acquisition procedure. However, this solution requires a complex processing unit inside the GNSS tracking chain with consequently computational costs. Moreover, several attempts for detection of GNSS spoofing events, even the most sophisticated ones, have been done in the signal processing domain. Most of them exploit correlation measurement and apply SQM techniques. The scope is to find, if present, additional correlation peaks that can show a possible spoofing attack [81][73][55]. Unfortunately, in order to have an updated correlator measurement, the computational complexity of the receiver has to be increase. Even if this could be possible, the next challenge is being able to discern between spoofing attack and multipath propagation effects.

An exhaustive review of the spoofing detection methods is provided in [43].

3.3 SPOOFING DETECTION: SIGNAL QUALITY MONITORING TECHNIQUES

Monitoring and detecting anomalies and disturbances on received signals are important steps to assess that receiver could be affected by a counterfeit signal. In order to have reliable positioning and navigation solutions, it is necessary to monitor the quality of the broadcast GPS signals. Several methods to detect anomalies by observing PVT solutions or processing received data have been investigated. Among these methods, SQM is the rising one. It is based on observing the behavior on time of the correlation shape by comparing outputs with a well-defined metric: the most common SQM tests are the Delta and Ratio tests, designed to identify asymmetric correlation peaks and to identify abnormal shape of the correlation peaks, respectively [59]. In previous literature, SQM techniques have been proposed as a method to monitor in time the envelope of the correlation function in multipath scenarios [27]. In the tracking stage the effects of a possible spoofing event are very similar to multipath ones: distortions of the correlation outputs due to the spoofing attack could be assessed as a strong multipath which is in-phase with the authentic signal. Thus, the SQM method has been extended for detection of spoofing attacks. In [19] authors have implemented the Ratio Test metric, proposed in [27], to detect any asymmetry and distortion in the correlation outputs due to an intermediate spoofing attack. They have observed both code and carrier tracking stages: the alignment of the fake signal in code-phase and carrier domains determines not suitable outputs from Delay Lock Loop (DLL) and Phase-Locked Loop (PLL). In [49] authors have analyzed two cases of intermediate spoofing attack. Firstly, the spoofer has to align its counterfeit signal to the authentic one, and possibly (once aligned) it has to increase the power on order to be tracked. This kind of spoofer is able to reach the code-phase alignment with the authentic GPS signal, that could be in constructive or not constructive interference. It was showed that the delta and ratio test are not able to detect the spoofing event if this is in constructive interference with the real signal. On the other hand, when the fake signal is out of phase with the authentic one Delta and Ratio test discriminators have different values from the nominal case, i.e. when the spoofer is not detected. However, it is necessary that the attack is not rapid in order to detect the presence of the spoofer. Thus, it could be assessed that SQM antispoofing techniques are valid methods to detect the counterfeit event with the assumption that the receiver already tracked the authentic signal. However, these methods could present some issues in a multipath propagation scenario because they could not distinguish between spoofing attack and a delayed reflection, so the detection flag will be raised if one of these occurs. For this reason, the implementation of a joint metric detection technique is needed. In [6] authors have proposed to use extra correlators jointly with the Ratio Test metric in order to overcome the ambiguity problem in detecting spoofer or multipath event. An important step is to define the setting of the correlator and extra-correlator, in order to detect vestigial signal presence. It is necessary that the two implemented metrics can be effective in the same portion of code delay. On the contrary, they will share only a small part and the detection results will be not reliable. In addition, it is possible that the effects of counterfeit signal could not be present in both metrics during the same time of observation. Thus, it is necessary to extend the observation time and a parallel check in both metrics is required: if both metrics present a high probability of detection, the receiver is able to distinguish between spoofer and multipath events. However, this joint detection techniques is not reliable with a high power spoofing signal. The strong counterfeit signal hides the real signal under the noise floor and the receiver is not able to understand that the tracked signal is the fake one: Ratio Test does not detect any distortion in the correlation function shape. Another joint detection technique has been proposed in [80]. The authors have described a non-cryptographic method for spoofing detection that consists in implementing jointly a correlation function distortion monitor and a total in-band power monitor. This technique relies on the incapability of a spoofer device to maintain for long time a low-power attack in order to not cause abnormal shape in the receiver correlator outputs. These two independent metrics consist in a symmetric difference between an early-late correlator pair (non-normalized Delta Test) and the measure of the total power in receiver bandwidth. The first metric aims to detect distortions in the correlation shape. The reliability of this result depends on the choice of the time-offset between the early and late local replica. The power monitor metric aims to measure the nominal value of the in-band power and to detect anomalies in increasing power when a spoofing event occurs.

In conclusion, many literature works state that SQM techniques are efficient spoofing detection solutions in a LOS scenario. However, with distorted propagation channel, i. e.the signal is affected by multipath and/or huge atmospheric interferences, the aforementioned techniques are not able to perfectly distinguish the presence or absence of the spoofing event.

3.4 PROPOSED ARCHITECTURE

In the previous sections, literature reviews for detection spoofing techniques and in particular for SQM approaches have been described. It is well known that the structure of the spoofing signal is GNSS-like, because it is generated in order to tick and mislead the target receiver. However, so that the attack to be effective, spoofing source has to reproduce and broadcast at least four Pseudorandom Noise (PRN) signals. And if an attack occurs, the detection is still difficult in particular before the de-spreading step. Some methods have been already presented, as the constant monitoring of the AGC response in order to measure unexpected values [4]. The provided method is very effective, but its main drawback consists in requiring enough information about the AGC component: it is not implementable in GNSS software receiver because it is not working with digital domain samples. Moving from these considerations, a method that consists in the joint observation of measurement outputs from different components of the GNSS receiver is proposed. The main goal is to provide a possible detection technique based on the observation of the AGC signal waveform aided with the information carried out from the correlation function and from the estimation of the C/No. For this purpose, firstly a description of the scenario is provided followed by the introduction to each metric used to detect the jamming threat.

3.4.1 *System model*

In [43] a simplistic expression of a spoofing signal is defined. As already said, the spoofing source generates many counterfeit PRNs that have quite the same power level of the authentic ones, a bit higher in order to attract the target to be spoofed. The spoofed received signal is written as [43]:

$$\begin{aligned} r(nT_s) &= \sum_{m=1}^{M} \sqrt{p_m^a} h_m^a \left(nT_s - \tau_m^a\right) c_m^a \left(nT_s - \tau_m^a\right) e^{j\phi_m^a + j2\pi f_m^a nT_s} \qquad (83) \\ &+ \sum_{q=1}^{N} \sqrt{p_q^s} h_q^s \left(nT_s - \tau_q^s\right) c_q^s \left(nT_s - \tau_q^s\right) e^{j\phi_q^s + j2\pi f_q^s nT_s} + \eta\left(nT_s\right) \end{aligned}$$

where T_s is the sampling interval, ϕ is the carrier phase, f is the Doppler frequency, p is the signal power and τ is the code delay; the subscripts m and q (and the upscripts a and s) correspond to authentic and spoofed PRN signal, respectively. The symbol $h(nT_s)$ represents the transmitted data the and $c(nT_s)$ is the PRN sequence, M is the total number of authentic and N of spoofed received signals; $\eta(nT_s)$ is the complex AWGN with zero-mean and variance equal to σ^2. According to the value of spoofed PRNs it is possible to differentiate the type of the spoofing attack. However, the spoofing source has to generate signal with a very similar power to the authentic ones, and consequently the received power level increases due to the jamming contributions [43].

3.4.2 *Automatic Gain Control*

The AGC adjusts the power level of the intermediate frequency signal at Analog-to-Digital Converter (ADC) input in order to minimize the quantization loss. The presence of the AGC is necessary to calibrate the gain in order to define a correct received input power. It is well know that the GNSS signal power at the Earth's surface is below the thermal noise floor, which is expressed as:

$$P_N = kT_A B_W \qquad (84)$$

where k is the Boltzmann's constant, T_A is the antenna temperature and B_W is the bandwidth. The thermal noise is then added to the noise of the front end components, defining the total noise power as the predominant value, written as:

$$P_{N,total} = k\left(T_A + T_R\right) B_W \tag{85}$$

where T_R is the equivalent receiver temperature derived from Friis formula. Taking into account that GNSS signals are below the thermal noise floor, the AGC is driven by the ambient noise or interference rather than the signal power. Consequently, it can be assessed that interfering signals are a main source that changes the AGC gain level. However, the presence of the AGC, even if the system seems to be driven by the thermal noise power, is necessary to calibrate the gain in order to define a correct received input power and also a possible RFI. In [11][51][41] the AGC level as an interference assessment tool has been investigated and the possible application of the AGC as an RFI detection solution is provided. AGC is sensitive to both wide band noise and continuous wave interferences. In [51][41][40] it has been shown that the AGC gain changes differently according to the type of interferers. Thus, if the incoming jammer is known and the AGC is previously calibrated against different types of attacks, it can be possible to estimate interfering power from the AGC level. In a pre-correlation method using AGC gain and adaptive lattice Infinite Impulse Response (IIR) filter parameters is provided. It can be used for detecting intentional interferences before the tracking stage. In addition, authors have carried out a classification method exploiting both AGC and IIR filter metrics. Therefore, the proposed algorithm is able to discern which kind of interfering occurs among single tone, swept signals and band limited white noise. As already said, due to the fact that the received signal is embedded in noise, the signal samples distribution is expected to be Gaussian. This is the reason why AGC component adjusts the gain in order to reach this type of distribution of the received samples. The more sensitive the AGC algorithm, the more accurate the detection of the RFI events [41].
In Figure 106 the AGC component is shown within the typical GPS receiver architecture. The function of the AGC is to optimize the gain of the front end to that of the analog-to-digital converter.

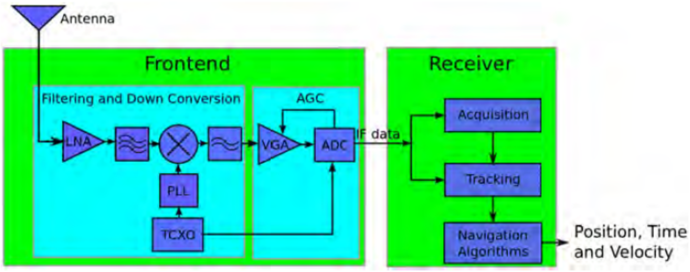


Figure 106: Typical GPS receiver with AGC shown

In [4] an interesting application of the AGC as a interfering detector is provided. The author describes the use of the AGC component response within the GPS L1 bandwidth as a simple way to detect potential spoofing signals. The noise-driven characteristic causes instability of the AGC output due to the continuous gain variation according to the received power. Taking into account this, a calibration of the AGC is necessary in order to define statistical properties in the nominal conditions, i. e.without spoofing events. The proposed results show that the presence of the spoofer, after an accurate calibration, adds energy in the useful band with a consequent drop of the AGC gain level. However, all the testing results have been carried out in a controlled scenario, neglecting how much jamming events can occur in real sites. Given that, an AGC-centric approach will not be reliable as it could arise false alarm flag too often. Consequently, the only AGC component cannot be considered as a stand-alone detector, but it can be considered as a complement to other approaches, providing an effective spoofer detection.

3.4.3 *Correlator*

In order to deny the correct GNSS acquisition and tracking procedures, spoofing signal make a fake correlation peaks being able to overlap the authentic one, leading the target receiver to a wrong tracking solution. The correlation output could be distorted by a spoofing attack, but the effect of the interaction with the authentic signal can be mistaken for multipath effects. Thus, some of the mitigation of multipath effect have been used to detect spoofing signals [59][19]. Firstly, the spoofer has to align its counterfeit signal to the authentic one, and possibly once aligned it has to increase the power in order to be tracked by the receiver tracking loop. In order to be aligned with the useful signal, spoofing has to perfectly know the position of the target receiver and thus estimate correctly necessary parameters. Instead, when the spoofer is not able to define in a correct manner the synchronization with the authentic signals, it the correlation window a strong correlation peak appear. This additional peak moves towards the authentic one trying to misdirect the tracking solution.

3.4.4 *C/No estimation*

As for the previous measurements, the carrier-to-noise ratio C/No estimation can be used to detect RFI events, but it is a noisy measurements. The environmental effects can strongly affect the C/No measurements, but unlike the AGC information the C/No measurements can be easily obtained from the receiver as it is an observable information. The C/No is a wide used metric in assessment of the quality of the tracking signals. This value is always evaluated in function of the elevation angle: greater the elevation angle, the higher the value of the C/No, due to the clear visibility of the satellites in orbits. When a RFI event occurs, consequently there is variation in the estimate C/No value. RFI raises the noise floor and thus the C/No presents a drop proportional to the interfering power that jams the target receiver. In presence of a spoofing signal the effects on the C/No estimate are similar to the RFI case. The spoofer can increase the noise floor of the target receiver with the aim to disrupt the acquisition and tracking of the authentic signals, but conversely to the RFI case the spoofer creates correlation peaks and thus C/No value commensurable to the authentic one. Thus, the detection is more difficult due to the capability of the spoofer source to generate counterfeit PRNs with a power equivalent to the expected one.

3.4.5 *AGC & Correlator & C/No : A combined Technique*

In the previous sections a brief description of the measurements provided by components inside the GNSS receiver is reported. The properties of the aforementioned approaches have been described, defining how them can be implemented as a jamming and spoofing detection techniques. The drawback is that all the methods proposed as a self-contained anti-jamming techniques, an thus considered independently, cannot be implemented due to their high probability of false alarm. As a matter of fact, for the AGC if a previous calibration is not made, the spoofing detection by means of the drops on the AGC level is not reliable, due to the fact that the components is driven by noise and thus any type of interference can be classified as a spoofing signal. The correlation distortion measurement can be lead astray by multipath components and the C/No estimates is highly sensitive to any type of events that increases the noise floor in the GNSS receiver. In [80] authors have proposed a non cryptographic GNSS anti-spoofing technique which exploits the difficulty of a spoofing source to generate a successful attack with both low PRNs power and minimizing the distortion in the correlation profile. The described method consists in monitoring simultaneously the received power and the distortion in the correlation shape. According to the authors, the combination of the two techniques permits to discern between multipath and spoofing effect and also to reduce the false-alarm probability with respect to the stand-alone approach.

Taking into account all these consideration and possible drawbacks of the aforementioned techniques, we propose a spoofing detection technique that relies on the combined observation and evaluation of the measurement carried out by the components of the GNSS receiver, i. e.AGC gain level, correlation shape and C/No envelope. As already stated, all the measurements are sensitive to the fluctuation due to the presence of the noise power and taken individually they are not reliable in detection spoofing effect. However, if a spoofer attack occurs, it determines contemporary distortions in all the processing measurement and thus it is possible to define a detection method by observing how and when these distortions are present. For example, if the AGC gain level has a very huge drop, the correlation distortion monitor presents a lack of the expected shape and the C/No value is very low even if the elevation angle is high, this could mean that a high power jamming event is occurring. Instead, if the AGC gain level has a fluctuation, the correlation distortion presents a variation without any lack of profile, and the C/No has a drop (at high elevation angle) but successively achieve again the expected value, it is very probable that a spoofing event is occurring. Thus, it can be possible to define a detection method by exploiting the combined measurements of AGC, correlation shape and C/No estimate.

3.5 NUMERICAL RESULTS

In order to confer effectiveness to the proposed approach, simulation results are shown in the following. These are carried out elaborating collected data both in controlled scenario and airport service area.

3.5.1 *Scenario*

The first simulation campaign is carried out elaborating data which have been collected from spoofing scenarios using the NovatelG3 receiver. From this data, both AGC and SQM messages are extracted in order to be monitored. Four different spoofer scenarios have been considered: the first one is the baseline scenario without spoofing signal; in the second, a spoofing signal with a very high power is considered (Ds2); in the third (Ds3) and fourth (Ds4) scenarios spoofer with a matched power with respect to the authentic signal is considered. The corresponding parameters are listed in table 12.

Scenario	Spoofing	Platform	Power
	Type	Mobility	Adv.(dB)
Baseline	No	-	-
Static Overpowered Time Push (Ds2)	Time	Static	10
Static Matched-Power Time Push (Ds3)	Time	Static	1.3
Static Matched-Power Pos. Push (Ds4)	Position	Static	0.4

Table 12: Spoofing Scenario Parameters

The second simulation campaign is carried out considering signals collected by airport stations placed in different locations in the world. These stations are equipped with *WAAS* receiver antennas. Also in this case, both AGC and SQM message are extracted to be elaborated.

3.5.2 *Simulation Results*

In this section simulation results of the previous measurements campaigns are shown. Firstly, we consider the data collected in the controlled spoofed scenarios, described in table 12. Subsequently, results from *WAAS* antenna in airport area are analyzed. A parsing code implemented in MATLAB platform has been used in order to parse this signal collected by the NovatelG3 receiver.

3.5.2.1 *Spoofed-controlled test*

In Figure 107 the AGC gain envelope in the aforementioned four scenarios is shown. It is possible to notice that in the baseline case, the figure in the top left, the envelope of the AGC level it is quite constant, due to the absent of any kind of disturbance. In the Ds2 case, the figure in the top right, the AGC gain decrease rapidly defining a huge variation due to the fact that there is a spoofing input power that bury the authentic signal. In the Ds3, the figure in the lower-left, the AGC drop is decisively lesser than the previous case, but at the same time it defines the presence of some extra input power, due to the presence of a matched-power spoofing signal. In the last Ds4 case, the figure in the lower right, the AGC gain level is lesser than the previous case due to the presence of a spoofing signal even in this case with a matched-power to the authentic one.

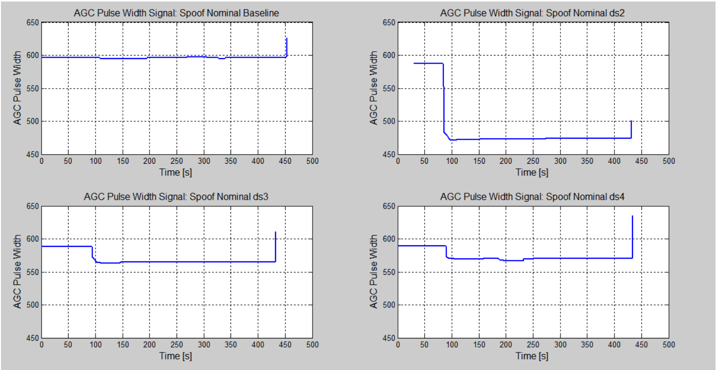


Figure 107: AGC gain for the baseline and three spoofed scenarios

In Figure 108 the correlator measurement in the four scenarios is evaluated in function of the chip offset and time. As for the previous case, it is possible to notice the effects of the presence of the spoofing signal, in particular for the matched-power cases. In the baseline case no alteration are visible, as expected due to the absence of the spoofing signal. Also in the Ds2 case any variation is detected, but conversely to the previous case, now the correlation shape is uniform because the victim receiver has tracked the spoofed signal that has a very high power. Instead, in case Ds3 and Ds4 evident variations in the correlation profile are present. In Ds3 case the fluctuations occur for both negative and positive offset chip. The case of variations located in negative offsets, i. e.they occur in advance with respect the 0 offset, has an important meaning. They cannot be produced by the presence of multipath effects because it is always appears later with respect to the synchronized replica. Thus, the presence of correlation peak in negative offset represents a spoofing attack that is incoming in the tracking loop. In the Ds4 case, the correlation shape variation occurs in the positive offset. In this case, and in general for all the positive offset peak location, it could be interpreted as the tracking circuit tracks the spoofed signal and rejects the authentic one.

In order to better define the quality of the tracking operation, different correlation metrics are used. These metrics are defined as a set of weight-coefficients through which a linear combination with the

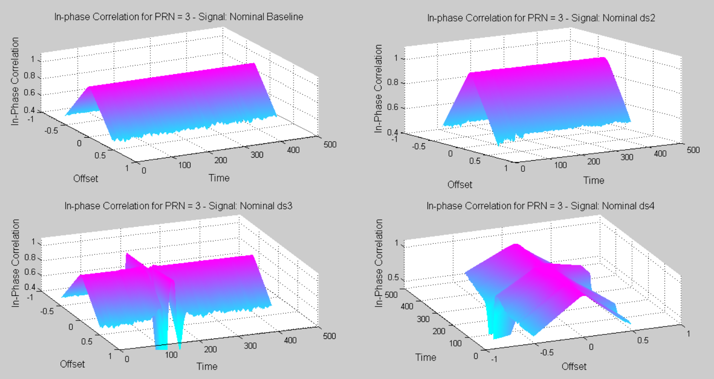


Figure 108: Correlation profile for the baseline and three spoofed scenarios

correlator bins is evaluated. In our approach three metrics are implemented:

- Metric 1: $[0, -1, -1, -1, -1, -1, 0, +1, -1, -1, +1, 0, +1]$;
- Metric 2: $[0, 0, -1, -1, -1, -1, 0, +1, +1, +1, +1, 0, 0]$;
- Metric 3: $[-0.0953, 0.3813, -0.5935, 0.3972, -0.8725, 0.9582,$ $-0.8680, 0.7322, 0.1232, -0.3189, 0.2056, 0.7654, -0.8118]$.

The coefficients are 13 as the correlator bins considered. The 7- element represents the offset 0 and consequently the other coefficients regard to the previous and to the successive bins, respectively. As mentioned previously, the linear combination of the correlation shape is used to evaluate the reliability of the tracking process. In Figure 109, Figure 110, Figure 111 results of the implementation of metric 1, metric 2 and metric 3 are shown. For all the three sets of coefficients, the adopted linear combinations define evident variations only for the spoofing signals with matched-power. In the baseline case no variation is detected, because no spoofing signal is present. In Ds2 the result is the same as before, but in this case due to the very high power of the spoofer, the correlation shape does not have any variations and consequently there is any alteration on the metric. Instead, for the matched-power case Ds3 and Ds4 due to the fact that correlation measurement is not uniform, also the metric result shows evident fluctuations for different received PRNs and consequently the quality of the tracking operation is not reliable.

From the simulation results, it is possible to deduce that the AGC works well in presence of strong spoofers detecting a high input power. In case of matched-power spoofers AGC is not reliable because huge drops are not present in the gain level envelope. Small drops cas be associated to a noise fluctuation. On the other hand, the SQM approach, by exploiting the correlation metric, is effective for matched-power spoofers because the linear combinations present irregular behavior. Conversely, SQM is not reliable in case of strong spoofers due to the fact that correlation function does not present any distortion, thus the metric test does not show any irregular event.

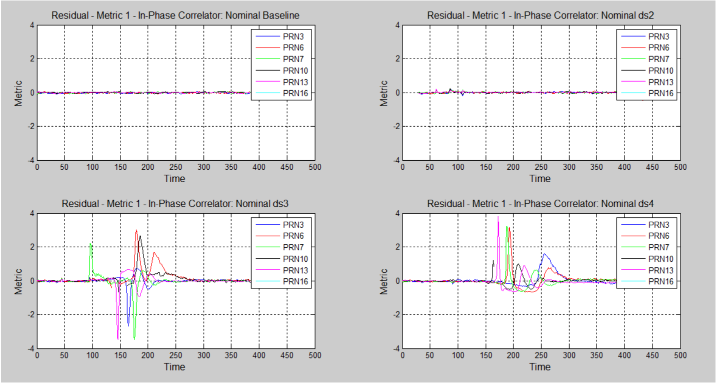


Figure 109: Correlation metric 1 in baseline and three spoofed scenarios

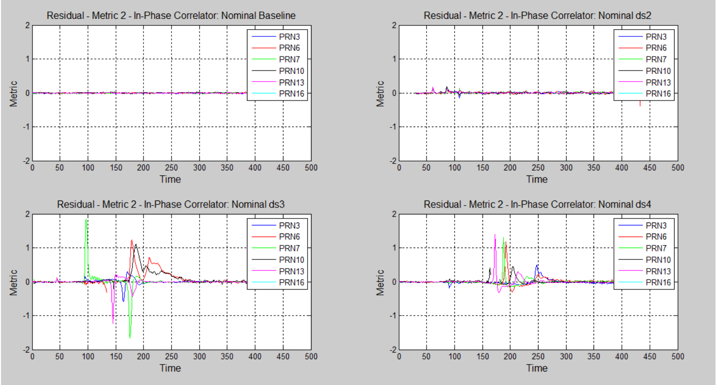


Figure 110: Correlation metric 2 in baseline and three spoofed scenarios

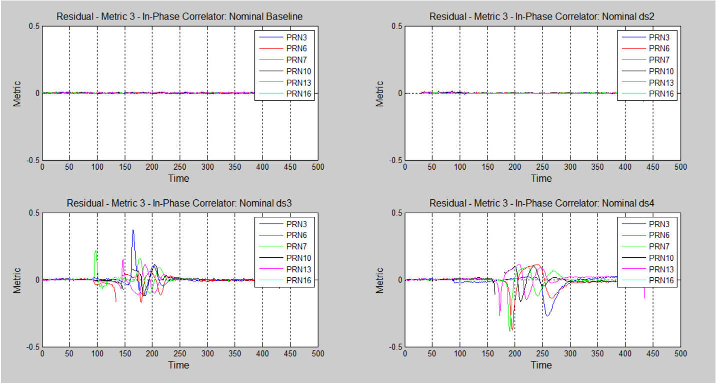


Figure 111: Correlation metric 3 in baseline and three spoofed scenarios

3.5.2.2 *Aiport test*

In the following, results of the second measurement campaign are reported. The evaluated data has been collected in real scenario, and not controlled as in the previous case, by a *WAAS* antennas located in an airport area. From these data, messages of AGC and C/No have been extracted and evaluated, writing and implementing a parser code in MATLAB. In particular, among the stations evaluated only two reference stations are considered, FAI and ZMA-A stations.

In Figure 112 and Figure 113 the AGC gain envelope in time is shown for FAI and ZMA-A stations, respectively. First of all, the timeaxis is expressed in seconds from the conversion of the time-stamp information embedded in the GPS message. The value Time of Week (TOW) represents the number of the week in which the signal is received at which the seconds are added.

It is possible to notice that the in the FAI station AGC level presents a fluctuation in the range from $[612 - 627]$ around the mean value 620.61. This variation is due to the only noise power showing that any RFI event or spoofing event occurs in the considered time-window. Instead, in the ZMA-A station AGC level is affected by several and deep drops for the entire considered time-window. These variations show that several interfering events are present causing also very huge drop of the AGC gain proving that high powers are injected in the target receiver.

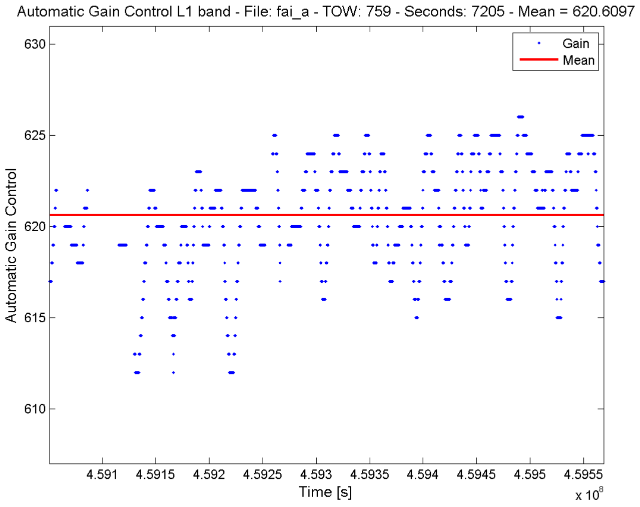


Figure 112: Automatic Gain Control of a free RFI station

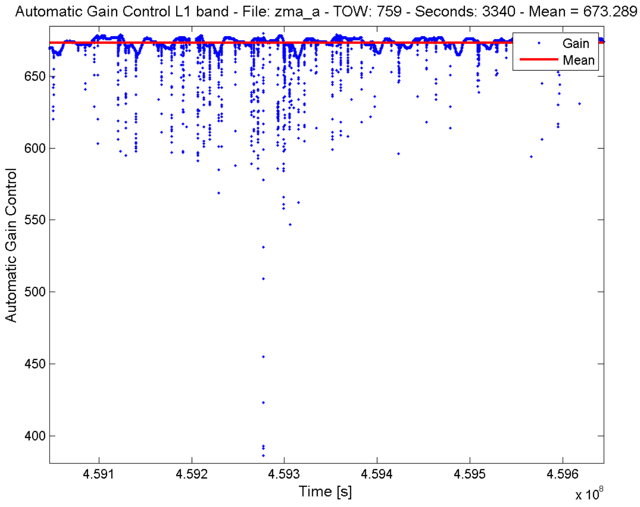


Figure 113: Automatic Gain Control of a RFI station

In Figure 114 a quality comparison between the two stations is provided. In this case a better time-information translation is defined, showing the week period in which the signals have been collected.

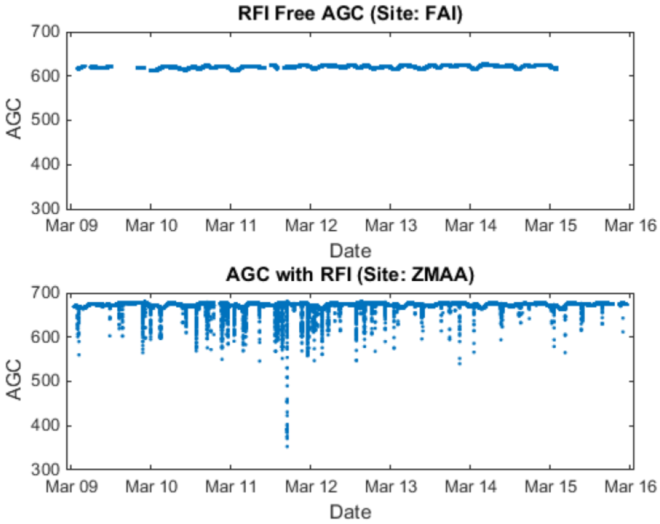


Figure 114: AGC: comparison between FAI and ZMA-A stations

In Figure 115 and Figure 116 AGC and histogram of the signal are showed for both stations. It is worthwhile to notice that the free-RFI present a distribution characterized by a mean value equal to 620.65 and a standard deviation equal to 3.05; for the interfered station the mean value is equal to 673.29 and a standard deviation equal to 4.76. Usually, in order to define statistic parameter necessary for a statistical study, the reference case is the free-RFI case, due to the fact that the principal aim is to detect malicious event. According to the shown results, possible detection threshold can be defined by the statistical value of the FAI station.

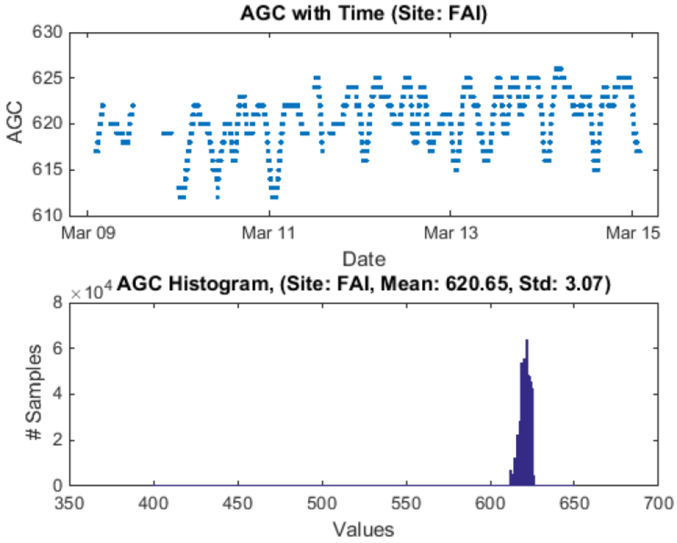


Figure 115: FAI station: AGC gain level and histogram

However, all the considerations above are not sufficient to define a detection method only by exploiting AGC gain envelope and its sta-

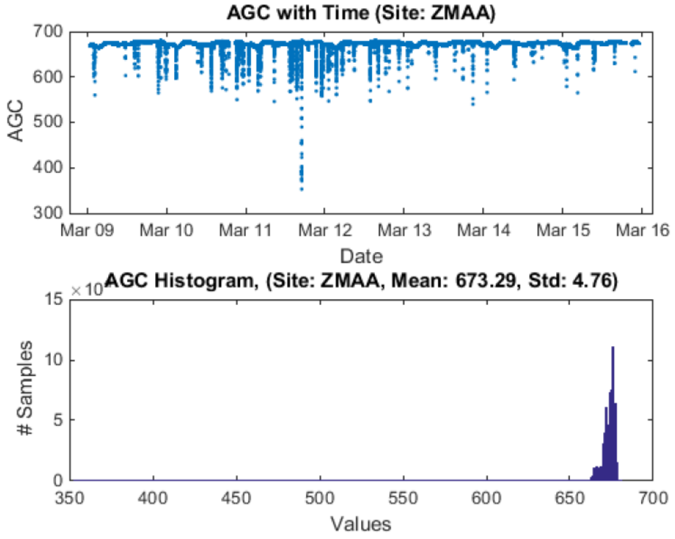


Figure 116: ZMA-A station: AGC gain level and histogram

tistical characteristics. The AGC stand-alone approach is not reliable because very sensitive to any noise variations without the capability of distinguish which kind of disturbance is occurring. For this scope, the C/No measurement is monitored. From the collected data, the message containing power information is extracted and evaluated. As previously, measurements from FAI and ZMA-A stations are considered.

In Figure 117 the AGC level and the C/No value for the PRN 14 are shown for the FAI station. It is possible to notice that both AGC gain and C/No envelope do not present any significant variation, confirming that any jamming or spoofing event is occurring.

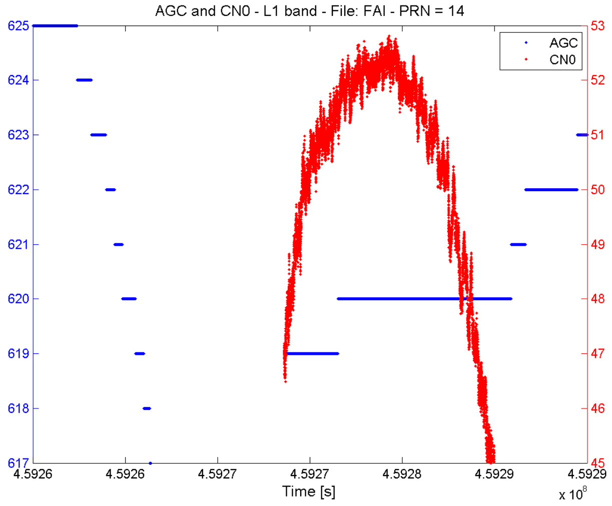


Figure 117: FAI station: AGC gain level and C/No PRN 14

In Figure 118, Figure 119, Figure 120, Figure 121 and Figure 122 the AGC level and the C/No value for the PRN 14, PRN 18, PRN 21, PRN 22, PRN 24 are shown for the ZMA-A station, respectively. In all the figures the drops in both envelopes occur at the same time-instant. In particular, the AGC considered drop are longer not more than 10 seconds. Thus, from the figures, it is possible to understand that when an AGC change occurs a change in the C/No estimate value occurs too. Furthermore the main drops in the C/No envelope, those one that are bigger than 5[dBHz], occur in correspondence to high elevation angle, i. e.in that range of visibility angle in which the received power has to be the maximum expected one, as for example the case of the PRN 18. In addition, after the drop the value of the C/No comes back to the expected value. Taking into account all the previous considerations, this aspect can be exploited to define if a jamming event is occurring and in particular if a spoofing signal is tricking or not the target receiver. It is well known that the spoofer has to generate PRNs with power equal to the authentic one; thus, in this cases possible spoofing event can be present due to the fact that after the short time-drop the C/No is at the expected value, as if the victim receiver tracks the counterfeit signal without any awareness of the presence of the counterfeit signal.

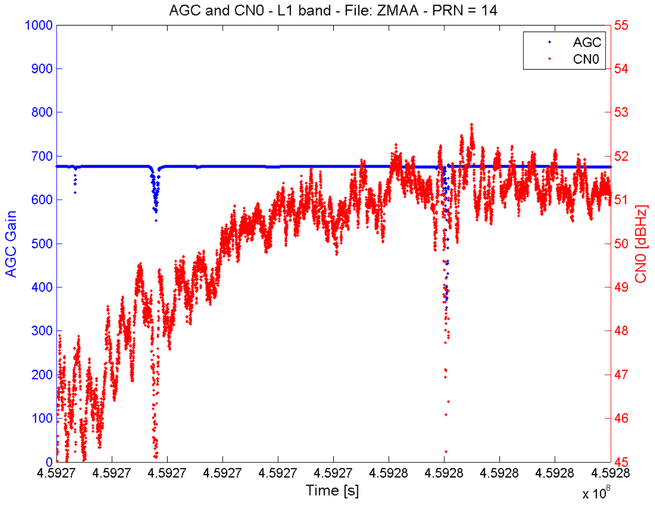


Figure 118: ZMA-A station: AGC gain level and C/No PRN 14

In Figure 123 and Figure 124 the C/No envelope on time for the PRN14 of FAI station and the corresponding SQM Metric 1 are shown, respectively. It is possible to observe that the C/No does not present any particular variation and this is also shown in the relative metric. The shape of the metric is proportional to the C/No estimate: the higher the C/No value, the thinner the metric residual. In Figure 125 and Figure 126 the zoom on one C/No repetition and its corresponding metric are reported in order to show better the correlation between the two measurements.

In Figure 125 and Figure 126 the zoom on the C/No for the PRN 14 for the FAI station and the corresponding metric are shown, respectively. It is possible to notice that any huge drop does not occur in the C/No estimate and consequently there is not any fluctuation in the metric results that is very close to the 0 value.

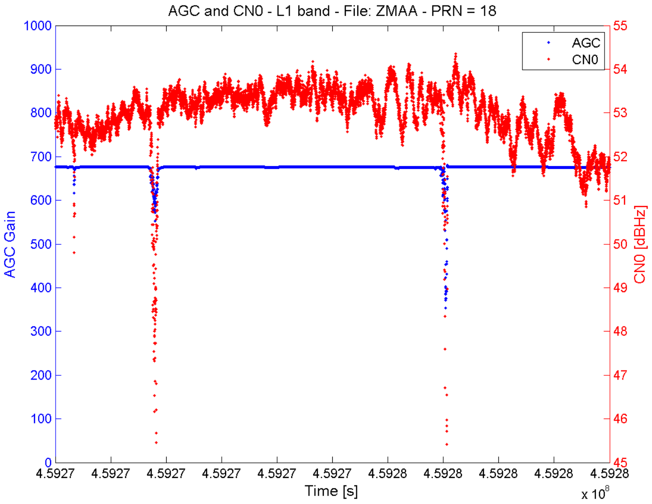


Figure 119: ZMA-A station: AGC gain level and C/No PRN 18

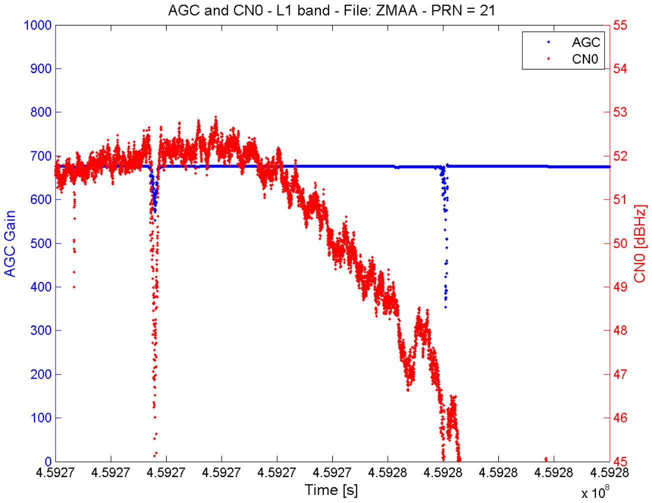


Figure 120: ZMA-A station: AGC gain level and C/No PRN 21

In Figure 127 and Figure 128 the zoom on the C/No for the PRN 14 for the ZMA-A station and the corresponding metric are shown, respectively. First of all, it is important to underline that the metric result is evaluated only for C/No greater than 35[dBHz], and thus the time-start is different. However, this is not a critical aspects for our considerations. The first lobe on the left it is characterized by five drops in the interval in which the C/No is high and then a lack of signals, going towards lower C/No values. The SQM metric value presents several fluctuations corresponding to the drops in the C/No envelope, and also in the metric result the lack of signal is obviously detected. The second lobe on the right presents a huge drop always in the interval in which the C/No is high and in the metric residual there is a fluctuation, as to arise a possible presence of a malicious disturb. Anyway, taking into account all these considerations, the most important aspect to be underlined is that comparing the metric results in Figure 126 and 128 the metric residual is quite higher in the latter one.

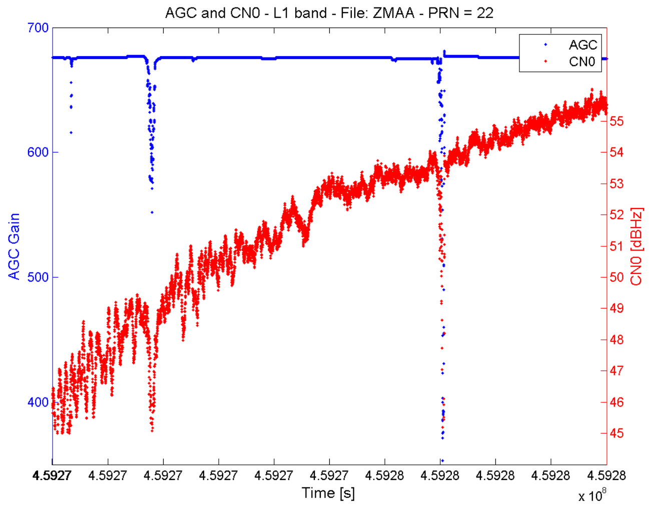


Figure 121: ZMA-A station: AGC gain level and C/N0 PRN 22

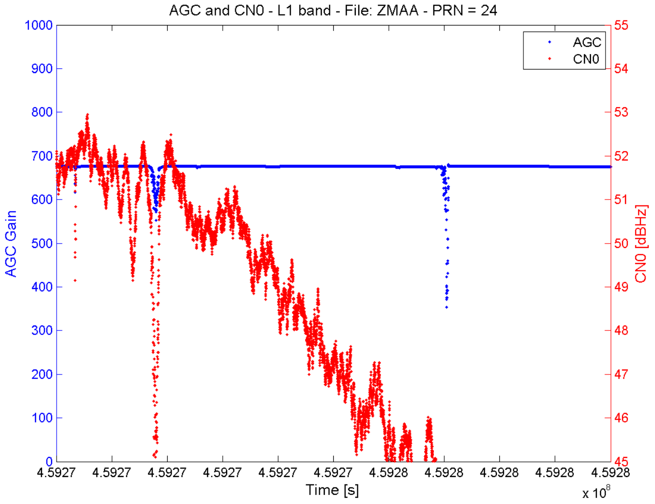


Figure 122: ZMA-A station: AGC gain level and C/N0 PRN 24

Considering that the receiver antenna are GPS antennas and that the expected C/N0 is defined by the communication standard, the mean value of the metric should be equal in both cases, but the interfering events in the ZMA-A case increase the value of the metric residual, showing that a malicious attack occurs.

The same considerations can be carried out for the other cases. In Figure 129 and Figure 130 the PRN 18 for the ZMA-A station is shown. Also in this case, C/N0 envelope presents drops and the corresponding metric is higher than the free interference case, presenting evident fluctuations in the thinner interval. The same is for PRN 21 and PRN 22 for the ZMA-A station reported in Figure 131 and Figure 132, in Figure 133 and Figure 134, respectively.

An interesting case is the one represented in Figure 135 and Figure 136, showing the PRN 24 measurements for the ZMA-A station. The C/N0 envelope presents two close lobes for each repetition. The relative metric presents values similar to the previous case, but the

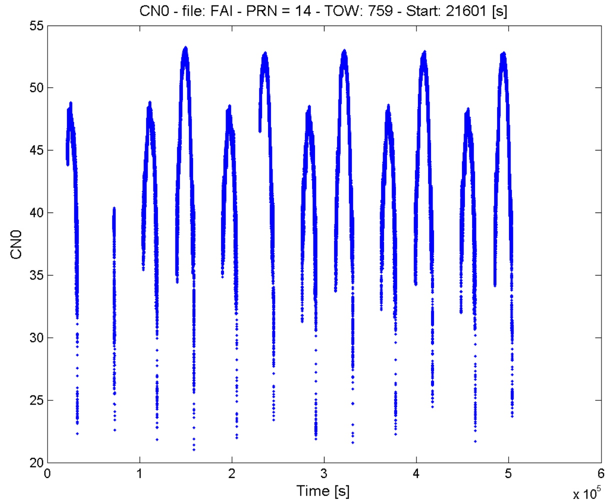


Figure 123: FAI station: C/No PRN 14 envelope

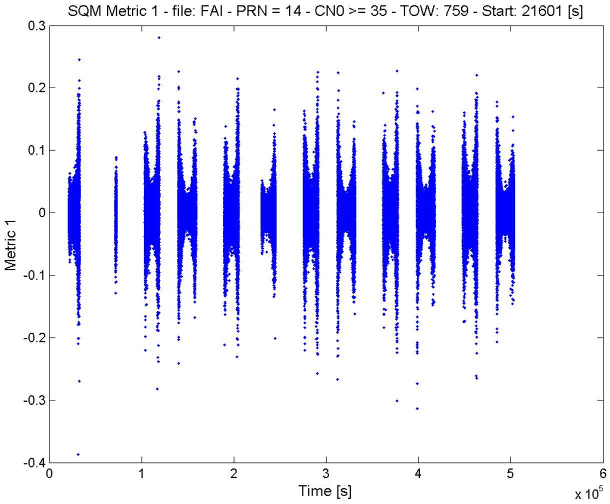


Figure 124: FAI station: Metric 1 residual for the PRN 14

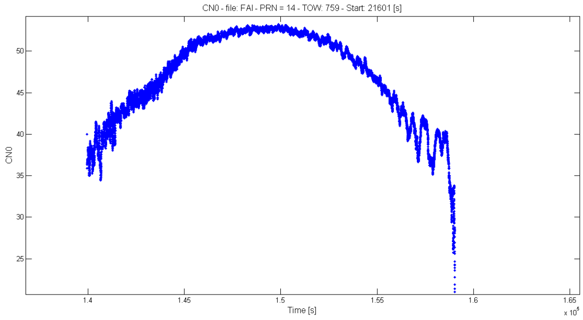


Figure 125: FAI station: Zoom on C/No PRN 14 envelope

most interesting results is the presence of the first metric burst. This smaller C/No estimate cannot be associated to a delayed replica due to the fact that it occurs in advance respect the bigger one. Thus it can be associated to the presence of a spoofer or a strange repetition of the PRN 24.

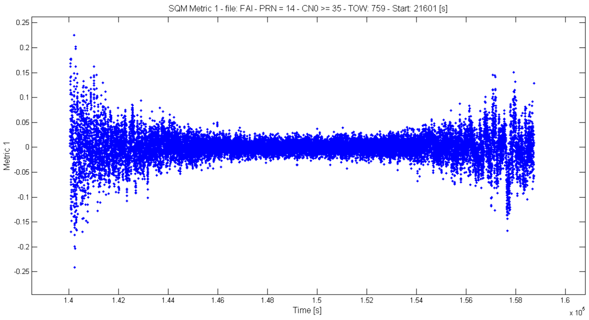


Figure 126: FAI station: Zoom Metric 1 residual for the PRN 14

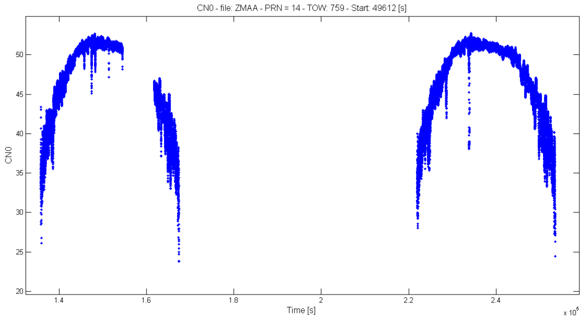


Figure 127: ZMA-A station: Zoom C/No PRN 14 envelope

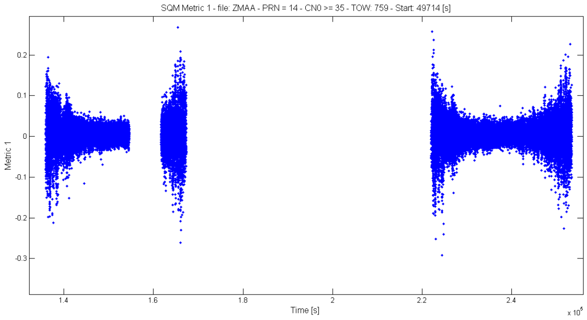


Figure 128: ZMA-A station: Zoom Metric 1 residual for the PRN 14

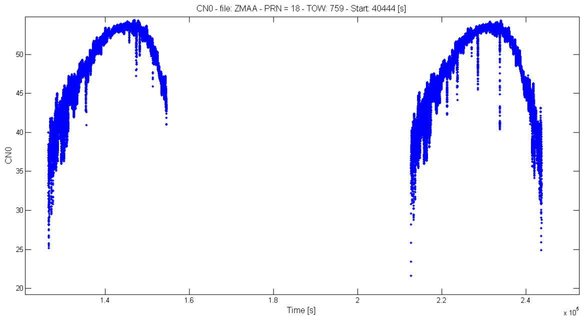


Figure 129: ZMA-A station: Zoom C/No PRN 18 envelope

In conclusion, these results have shown that a possible combined technique can be exploited for a jamming detection technique and above all for a starting point for the spoofing detection, that has to be further investigated and improved.

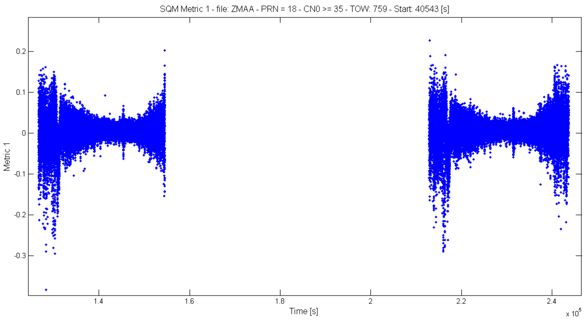


Figure 130: ZMA-A station: Zoom Metric 1 residual for the PRN 18

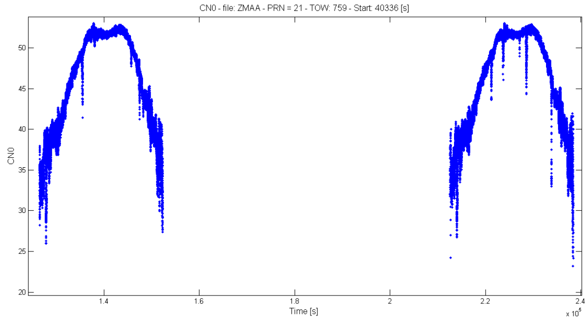


Figure 131: ZMA-A station: Zoom C/No PRN 21 envelope

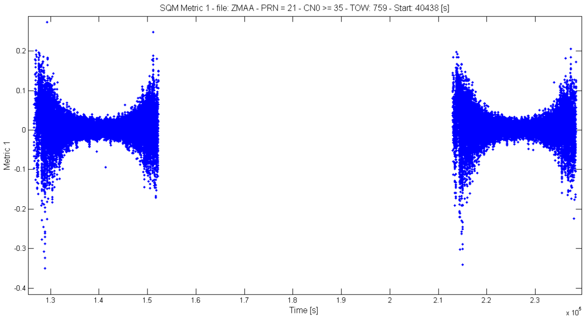


Figure 132: ZMA-A station: Zoom Metric 1 residual for the PRN 21

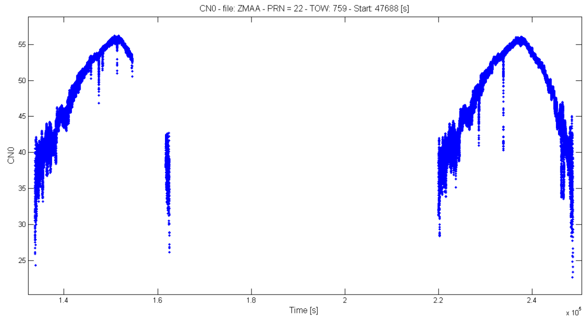


Figure 133: ZMA-A station: Zoom C/No PRN 22 envelope

3.6 conclusions

In this chapter an approach for the jamming and spoofing detection is proposed. The described method consists in the combined evalua-

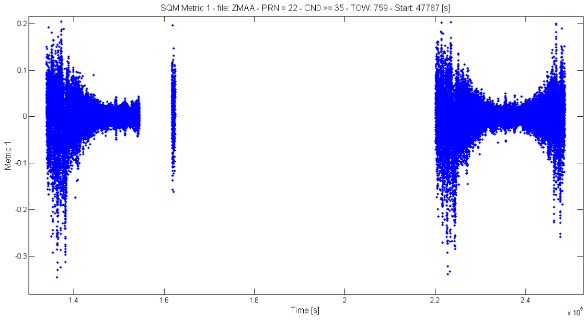


Figure 134: ZMA-A station: Zoom Metric 1 residual for the PRN 22

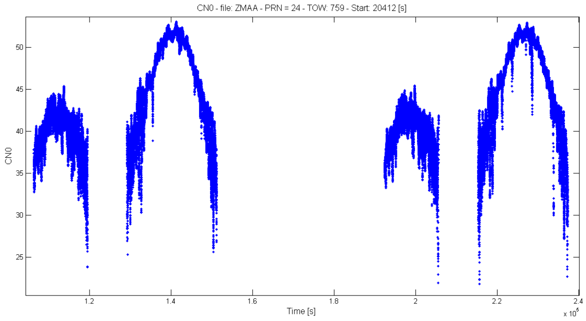


Figure 135: ZMA-A station: Zoom C/No PRN 24 envelope

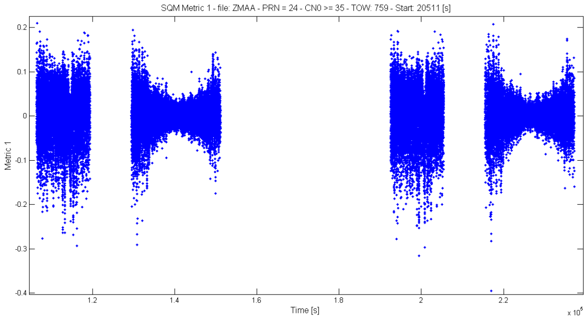


Figure 136: ZMA-A station: Zoom Metric 1 residual for the PRN 24

tion of the AGC, correlator profile and C/No estimate measurements intrinsically generated by the GNSS receiver. Simulation results have substantiated the effectiveness of our approach. Results have been carried out using data collected in different scenarios with different conditions. From the analysis of the spoofed data, it was possible to deduce that the AGC approach works well in case of strong spoofers, but it is not effective with the weak ones. Conversely, the SQM approach is not reliable for strong spoofer, but it works well for matched-power cases. In addition, from analysis of the airport data, it is evident that in real scenario AGC is strongly affected by RFI events, thus aiding techniques has to be added. Accordingly, AGC, correlation and C/No measurement have been shown highlighting which can be the effects of a spoofing attack, and they have been processed in order to define the presence or not of the malicious event. However, the combined evaluation of these metrics improves the possibility of detection of counterfeit signals affecting the receiver, decreasing the false alarm rate that could be higher if a single metric is used as a stand-alone approach.

AKNOWLEDGEMENTS A significant thanks is given to the researchers of the GPS Laboratory at Stanford University and Zeta for providing us the tested signal used during our simulations. The study on the spoofing detection problem will be submitted as a journal paper in collaboration with Professor Dennis M. Akos et al.

SPOOFING DETECTION TECHNIQUES: FURTHER DEVELOPMENTS

The research of efficient and simple spoofing detection and mitigation techniques will continue to be the main scope in GNSS research field. Considering all the analysis described in the previous chapter, GNSS conventional receiver are strongly subjected to jamming and spoofing attacks. In particular, if the receiver can detect the presence of a jamming signal because its power is above the useful signal, in case of spoofing signal the receiver is not consciousness of the occurring attack because the signal power is matched with the authentic one. Thus, in order to avoid that counterfeit signals trick the target receiver, efficient detection techniques need to be designed.
In this work it has been show that a possible combined observation of receiver measurements can be applied as jamming and spoofing detection technique for a stand-alone GPS receiver, which does not benefit of any additional measurement provided by aiding systems. Observing AGC, correlator shape and C/No measurements it is possible to define a detecting method. With particular assumptions, it is also possible to detect spoofing signals. We expect that the complexity increases, but all these metric are provided by the GNSS receiver and thus no any modification in the hardware and software architecture has to be made. Two different main scenarios have been proposed: the controlled and the airport one. It has been shown that the combined solution can be effective in the detection of spoofing signal too, with a possibility to reduce the receiver vulnerability.
However, it is obvious that update end efficient techniques have to be designed in order to counteract the increasing and fast diffusion of spoofing equipments. Spoofing constitutes the main threat for a navigation system receiver, and research on this matter will continue to appear and to be a challenge, every time that new scenarios or more complex systems will be taken into consideration. Thus, further developments are required. In the real-world scenario GNSS receivers are subjected to the multipath propagation effects due to the several reflections generated by the surrounding scenario. Consequently, it is necessary to take into account also the possible effect that the multipath propagation can generate. The scope is to efficiently discern added peaks generated by multipath and peaks generated by the presence of the spoofing signal. In this direction, it could be possible to define statistical properties for both multipath and spoofing and then to develop a countermeasure technique. On the other hand, a possible approach could be the observation of the correlation shape. If a peak is located in the negative offset of the AC function, i. e.it is in advance with respect to the zero-offset, thus this peak can only represent the presence of a spoofing attack (because a spoofer is able to move the peak "to the left"). It cannot be confused as a multipath effect, because in this case the peak has to be located later than the align

time-instant due to the nature of the multipath propagation. Other solutions are represented by the improvement of the techniques based on the observation of the C/No estimation in function of the elevation angle and in comparison with contemporary drops in the AGC gain level (as defined in Chapter 3). In addition, possible solution is represented by the implementation of spare searching correlators that can "look for" energy outside the main peak and thus signals that have a wider bandwidth with respect to the receiver. This technique can be efficient but with a higher complexity because more correlators are required. Conversely, the SQM techniques are more probable due to the fact that measurements are provided by the GNSS receiver.

In conclusion, new challenges are defined by different communication complex systems. Due to the increasing diffusion of civil infrastructure relying on GNSS, these new challenges will need to be solved trying to not modify the system architecture and preserving the technical knowledge of the current positioning systems.

CONCLUDING REMARKS

In this dissertation, techniques for possible enhancement of the performance in satellite navigation systems have been studied and designed. The common topic between the two presented part is the interfering threat in GNSS.

In the first part the attention has been focused on the study of possible detection and mitigation techniques for structured interfering signals. In particular, a jamming detection method performed in the frequency domain has been provided. The mathematical tool of WT has been exploited in order to detect discontinuities in interfering PSD envelope. The same techniques has been applied in time-domain in order to define the duty-cycle of an interfering waveform. Thus, it is possible to define the activity in time of the jamming source. Successively, an improvement of an existing technique has been described. An analytical study of the chirp signal has been evaluated and analytical AC function has been expressed in a closed form. Additional results in terms of cancellation performance have been showed in order to improve proposed algorithm (in [P4]). Moving from these results, the aforementioned algorithm has been applied in a different and harsh scenario. In this case, the interfering signal has been considered affected by multipath propagation (UMTS channel), then resulting from the contribution of the delayed replicas. The described algorithm has been tested also for this particular case. Numerical results have shown that the provided method still works properly detecting and canceling multipath jamming signal, also in presence of the useful GNSS signal. Thus, its effectiveness has been demonstrated by means of computer simulations and emulations, showing its capabilities.

In the second part of this dissertation, the attention has been focused on the most sophisticated interfering waveform, the spoofing signal. Since spoofing signal has become a very important topic, several literature works have been presented in order to provide valid solutions of different kinds. After a deep review of existing works, a possible solution in spoofing detection has been presented. Our approach has been based on the jointly observation of different measurement outputs from three main blocks inside the GNSS receiver. The study has been centered on the analysis of the output signal of the AGC, the correlator and the estimation of the C/No. Exploiting these envelopes in a jointly way, a possible detection approach has been defined, by the evaluation of data collected in controlled scenario and airport area.

BIBLIOGRAPHY

[1] A novel multipath interference cancellation scheme for rake channel estimation. In *Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd*, 2001.

[2] Evaluation of multipath effects on interference cancellation in gnss using space-time based array processing. In *Electromagnetic Noise and Interference Control Session, Ursi General Assembly*, 08/2008 2008.

[3] A multipath mitigation algorithm in global navigation satellite systems arrays using independent component analysis. In *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*, 06/2010 2010.

[4] D.M. Akos. Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc). In *Journal of the Institute of Navigation, Navigation*, volume 59, 2012.

[5] K. Ali, Xin Chen, and F. Dovis. On the use of multipath estimating architecture for spoofer detection. In *Localization and GNSS (ICL-GNSS), 2012 International Conference on*, pages 1–6, June 2012.

[6] K. Ali, E.G. Manfredini, and F. Dovis. Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics. In *Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION*, pages 1240–1247, May 2014.

[7] Asghar Tabatabaei Balaei and Dennis Akos Andrew G. Dempster. Quantization degradation of gnss signal quality in the presence of cw rfi. In *IEEE International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'08), In Proceedings*, pages 42–47, 2008.

[8] Asghar Tabatabaei Balaei, Jinghui Wu, and Andrew G. Dempster. Comparison between gps and galileo satellite availability in the presence of cw interference. In *International Symposium on GPS/GNSS (IGNSS), In Proceedings*, 2007.

[9] A.T. Balaei, B. Motella, and Dempster A.G. Gps interference detected in sydney-austalia. In *International Global Navigation Satellite Systems Society IGNSS Symposium 2007, Proceedings of*, 2007.

[10] A.T. Balalei, J. Barnes, and A.G. Dempster. Characterization of interference effects on gps signal carrier phase error. In *SSC (2005)*, 2005.

[11] F. Bastide, D. Akos, C. Macabieu, and B. Roturier. Automatic gain control (agc) as an interference assessment tool. In *ION*

GNSS 16th. International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003), Proceedings of, pages 2042–2053, September 2003.

[12] R. Bauernfeind, I. Kramer, H. Beckmann, B. Eissfeller, and V. Vierroth. In-car jammer interference detection in automotive gnss receivers and localization by means of vehicular communication. In *Integrated and Sustainable Transportation System (FISTS), 2011 IEEE Forum on*, pages 376–381, 2011.

[13] J.W. Betz. Effect of narrowband interference on gps code tracking accuracy. In *National Technical Meeting of the Institute of Navigation ION-NTM 2000, Proceedings of*, pages 16–27, 2000.

[14] J.W. Betz. Effect of partial-band interference on receiver estimation of c/no: Theory. In *National Technical Meeting of the Institute of Navigation ION-NTM 2001, Proceedings of*, pages 16–27, 2001.

[15] D. Borio, S. Savasta, and L. LoPresti. On the dvb-t coexistence with galileo and gps systems. In *3rd ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC 2006), Proceedings of*, 2006.

[16] R Boucher and Joseph C. Hassab. Analysis of discrete implementation of generalized cross correlator. *Acoustic, Speech and Signal Processing, IEEE Transaction on*, 29(3):609–611, Jun 1981.

[17] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle. Gnss spoofing detection in handheld receivers based on signal spatial correlation. In *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*, April 2012.

[18] A. Brown, D Reynolds, D. Roberts, and S. Serie. Interference localisation trials using adaptive antennas array. In *The Institute of Navigation of ION GPS 1999, Proceedings of*, pages 137–142, 1999.

[19] A. Cavaleri, B. Motella, M. Pini, and M. Fantino. Detection of spoofed gps signals at code and carrier tracking level. In *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, pages 1–6, Dec 2010.

[20] Saeed Daneshmand, Ali Jafarnia-Jahromi, Ali Broumandon, and Gérard Lachapelle. Gps spoofing detection using raim with ins coupling. In *the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012),Proceedings of*, pages 1233–1243, September 2012.

[21] I. Daubechies. The wavelet transform, time-frequency localization and signal analysis. *Information Theory, IEEE Transactions on*, 36(5):961–1005, 1990.

[22] P.G.M. de Jong, T. Arts, A.P.G. Hoeks, and R.S. Reneman. Determination of tissue motion velocity by correlation interpolation

of pulsed ultrasonic echo signals. *Ultrasonic Imaging*, 12(2):84–98, Apr. 1990.

[23] P.G.M. de Jong, T. Arts, A.P.G. Hoeks, and R.S. Reneman. Experimental evaluation of the correlation interpolation technique to measure regional tissue velocity. *Ultrasonic Imaging*, 13(2):145–161, Apr. 1991.

[24] GPS Directorate. *Systems engineering and integration Interface Specification IS-GPS-200G*.

[25] F. Dovis and L. Musumeci. Use of wavelet transforms for interference mitigation. In *Localization and GNSS (ICL-GNSS), 2011 International Conference on*, pages 116–121, June 2012.

[26] ETSI. Universal mobile telecommunications system. Technical report, ETSI TR 101 112 v3.2.0, 1998.

[27] M. Fantino, A. Molino, P. Mulassano, M. Nicola, and M. Rao. Signal quality monitoring: Correlation mask based on ratio test metrics for multipath detection. In *IGNSS 2009*, Gold Coast, Australia, 12/2009 2009.

[28] G. Gabelli. *Code Synchronization and Interference Management Techniques for Satellite Navigation and Communications*. PhD thesis, University of Bologna, 2014.

[29] G. Gabelli, R. Casile, A. Guidotti, and G.E. Corazza. Gnss jamming interference: Characterization and cancellation. In *2013 International Technical Meeting of The Institute of Navigation, Proceedings of*, pages 828–834, 2013.

[30] J.C. Grabowski. Field observations of personal privacy devices. In *International Technical Meeting of The Institute of Navigation, Procedings of, Newport Beach, CA, January 2012*, pages 689–741, 2012.

[31] Joseph C. Grabowski. Personal privacy jammers. In *GPS World*, 2012.

[32] K. Gromov, D. Akos, D. Pullen, and P. Enge. Gidl: Generalized interference detection and localization system. In *13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000), Proceedings of*, pages 447–457, 2000.

[33] D Hambling. Gps chaos: How a 30$ box can jam your life. Technical report, New Scientist, 2011.

[34] Guenter Hein, Felix Kneissl, Jose-Angel Avila-Rodriguez, and Stefan Wallner. Authenticating gnss: Proofs against spoofs, part 1. July/August 2007.

[35] Guenter Hein, Felix Kneissl, Jose-Angel Avila-Rodriguez, and Stefan Wallner. Authenticating gnss: Proofs against spoofs, part 2. *INSIDE GNSS*, September/October 2007:71–78, 2007.

[36] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M Jr Kintner. Assessing the spoofing threat: development of a portable gps civilian spoofer. In *ION GNSS 21st. International Technical Meeting of the Satellite Division, Proceedings of*, 2008.

[37] Global Positioning System Wing Systems Engineering & Integration. Navstar gps space segment/navigation user interfaces interface specification - is-gps-200 revision e. Technical report, GPSW, June, 8 2010.

[38] Usman Muhammad Iqbal and Samsung Lim. Legal and ethical implications of gps vulnerabilities. In *Journal of International Commercial Law & Technology*, volume 3, July 2008.

[39] O. Isoz and D. Akos. Development of a deployable low cost interference detection and localization system for the gnss l1/e1 band. In *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, pages 1–4, 2010.

[40] O. Isoz, A.T. Balalei, and D. Akos. Interference detection and localization in gps l1 band. In *Proceedings of ION NTM 2010, San Diego, CA*, 2010.

[41] O. Isoz, D. Akos, T. Lindgren, C.C. Sun, and S.S. Jan. Assessment of gps l1/galileo e1 interference monitoring system for the airport environment. In *ION GNSS 24th. International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2011), Proceedings of*, pages 1920–1930, September 2011.

[42] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. Pre-despreading authenticity verification for gps l1 ca signals. *Navigation*, 61(1).

[43] Ali Jafarnia Jahromi. *GNSS Signal Authenticity Verification in the Presence of Structural Interference*. PhD thesis, University of Calgary, 2013.

[44] A. Jovanovic, C. Botteron, and P.-A. Farine. Multi-test detection and protection algorithm against spoofing attacks on gnss receivers. In *Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION*, pages 1258–1271, May 2014.

[45] E.D. Kaplan and C.J. Hegarty. *Understanding GPS: Principles and Applications*. Artech House mobile communications series. Artech House, 2005.

[46] A.J. Kerns, D.P. Shepard, J.A. Bhatti, and T.E. Humphreys. Unmanned aircraft capture and control via gps spoofing. In *National Workshop on the New Clockwork for Time-Critical Cyber-Physical Systems*, volume 31, 2014.

[47] S. Khanafseh, N. Roshan, S. Langel, Fang-Cheng Chan, M. Joerger, and B. Pervan. Gps spoofing detection using raim with ins coupling. In *Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION*, pages 1232–1239, May 2014.

[48] T. Kraus, R. Bauernfeind, and B. Eissfeller. Survey of in-car jammers-analysis and modeling of the rf signals and if samples (suitable for active signal cancellation). In *24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Proceedings of*, pages 430–435, 2011.

[49] Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Issac Miller. An in-line anti-spoofing device for legacy civil gps receivers. In *the 2010 International Technical Meeting of The Institute of Navigation, Proceedings of*, pages 698–712, January 2010.

[50] S. Lo, David De Lorenzo, Per Enge, D. Akos, and P. Bradley. Signal authentication: A secure civil gnss for today. *Inside GNSS*, 2009.

[51] M. Luo, G. Xie, D. Akos, and S. Pullen. Radio frequency interference validation testing for laas using the standford integrity monitor testbed. In *Proceedings of ION NTM 2003, Anaheim, CA*, 2003.

[52] R.G. Lyons. *Understanding digital signal processing*. 3rd edn. Prentice Hall Signal PIR. Upper Saddle River, 2010.

[53] L. Musumeci and F. Dovis. A comparison of transformed-domain techniques for pulsed interference removal on gnss signals. In *Localization and GNSS (ICL-GNSS), 2012 International Conference on*, pages 1–6, June 2012.

[54] L. Musumeci and F. Dovis. Performance assessment of wavelet based techniques in mitigatin narrow-band interference. In *Localization and GNSS (ICL-GNSS), 2013 International Conference on*, pages 1–6, June 2013.

[55] A. Ndili and P. Enge. Gps receiver autonomous interference detection. In *Position Location and Navigation Symposium, IEEE 1998*, pages 123–130, Apr 1998.

[56] John Nielsen, Ali Broumandan, and Gérard Lachapelle. Gnss spoofing detection for single antenna handheld receivers. *Navigation*, 58(4).

[57] Brady W. O'Hanlon, Mark L. Psiaki, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. Real-time gps spoofing detection via correlation of encrypted signals. In *Journal of The Institute of Navigation,NAVIGATION*, pages 267–278, September 2013.

[58] I. G. Petrovski. *GPS, GLONASS, Galileo, BeiDou for Mobile Devices*. United Kingdom: Cambrige University Press. Cambrige University Press, 2014.

[59] R.E. Phelts. *Multicorrelator techniques for robust mitigation of threats to GPS signal quality*. PhD thesis, Stanford University, October 2001.

[60] Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. Civilian gps spoofing detection based on dual-receiver correlation of military signals. In *24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),Proceedings of*, pages 2619–2645, September 2011.

[61] RAE. The royal academy of engineering, global navigation space systems: Reliance and vulnerabilities. Technical report, 2011.

[62] K. Deergha Rao, M.N.S. Swamy, and E.I. Plotkin. Anti-spoofing filter for accurate gps navigation. In *the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000),Proceedings of*, pages 1536–1541, September 2000.

[63] F. Reed, P. Feintuch, and N. Bershad. Time delay estimation using the lms adaptive filter - static behaviour. *IEEE Trans Acoust Speech Signal Process.*

[64] M. Sahmoudi and M.G. Amin. Fast iterative maximum-likelihood algorithm (fimla) for multipath mitigation in the next generation of gnss receivers. *Wireless Communications, IEEE Transactions on*, 7(11):4362–4374, 2008.

[65] J. Sanz Subirana, J.M. Juan Zornoza, and Hernandéz-Pajares. *GNSS Data Processing (Vol. I.: Fundamentals and Algorithms)*. Esa. Esa, 2013.

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

[67] D. Shepard and Todd E. Humphreys. Characterization of receiver response to a spoofing attack. In *the ION GNSS Meeting, Proceedings of*, 2011.

[68] Daniel P. Shepard, Jahshan A. Bhatti, Todd E. Humphreys, and Aaron A. Fansler. Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks. In *the ION GNSS Meeting, Proceedings of*, 2012.

[69] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. Evaluation of the vulnerability of phasor measurement units to {GPS} spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4):146–153, 2012.

[70] K. Sheridan, Y. Ying, and T. Whitworth. Pre- and post- correlation interference detection within software defined radio. In *25th*

International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Proceedings of, pages 3542–3548, 2012.

[71] M. Trinkle and D.A. Gray. Interference localisation trials using adaptive antennas array. In *The Institute of Navigation of ION GPS 2002, Proceedings of*, pages 613–619, 2002.

[72] European Union. *European GNSS (Galileo) open service signal in space interface control document*.

[73] A.J. Van Dierendonck. *GPS Receivers*. Global Positioning System: Theory and Application. Parkinson, B. and Spilker, J.J, JR., Ed ., 1996.

[74] John A. Volpe. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. Technical report, National Transportation Systems Center, 2001.

[75] Phillip Ward. Monograph on gps antispoofing. In *8th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1995),Proceedings of*, pages 1563–1571, September 1999.

[76] Jon S. Warner and Roger G. Johnston. *A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing*. Journal of Security Administration.

[77] Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, and John Fagan. Countermeasures for gps signal spoofing. In *the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005),Proceedings of*, pages 1285–1290, September 2005.

[78] K. Wesson, D. Shepard, and T.E. Humphreys. Straight talk on anti-spoofing: Securing the future of pnt. In *GPS World*, 2012.

[79] K.D. Wesson, T.E. Humphreys, and B.L. Evans. Position paper: Secure time transfer for cps. In *National Workshop on the New Clockwork for Time-Critical Cyber-Physical Systems*, 2012.

[80] K.D. Wesson, B.L. Evans, and T.E. Humphreys. A combined symmetric difference and power monitoring gnss anti-spoofing technique. In *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, pages 217–220, December 2013.

[81] Shepard Daniel P. Bhatti Jahshan A. Humphreys Todd E. Wesson, Kyle D. An evaluation of the vestigial signal defense for civil gps anti-spoofing. In *the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),Proceedings of*, pages 2646–2656, September 2011.

[82] Nathan A. White, Peter S. Maybeck, and Stewart L. DeVilbiss. Mmae detection of interference/jamming and spoofing in a dgps-aided inertial system. In *the 11th International Technical*

Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998),Proceedings of, September 1998.

[83] M. Wildemeersch, E. Cano Pons, A. Rabbachin, and J. Fortuny Guasch. Impact study of unintentional interference on gnss receivers. Technical Report EUR 24742 EN, EC Joint Research Centre, 2010.

[84] J. Yi, Z. Shu-fang, S. Xiao-wen, Z. Jing-bo, and H. Qing. A new rake-based multipath estimation algorithm in gnss receivers. In *Image and Signal Processing (CISP), 2010 3rd International Congress on*, volume 9, pages 4313–4317, 10/2010 2010.

[85] Lei Zhang and Xiaolin Wu. On the application of cross correlation function to subsample discrete time delay estimation. *Digital Signal Processing*, 16(6):682–694, Nov. 2006.

ACKNOWLEDGMENTS

Con questa tesi porto a termine il mio Dottorato, percorso durato tre anni durante i quali ho potuto mettere alla prova ed arricchire la mia personalità. Quest'esperienza mi ha concesso di lavorare, vivere e condividere gran parte del mio tempo con tante persone, ciascuna delle quali mi ha lasciato qualcosa. Per questo vorrei ringraziare tutte loro per avermi concesso il loro tempo, i loro sorrisi e il loro appoggio nei momenti un po' più bui. I loro consigli e le loro attenzioni ed il loro modo di comunicare con me hanno contribuito in buona parte a ciò che sono oggi. La prima persona che ringrazio è Giovanni, che è stato una guida durante questo mio percorso, e che mi ha trasmesso professionalità e dedizione. La sua accoglienza nel gruppo di ricerca mi ha trasmesso fiducia, coraggio e interesse, e donato l'opportunità di affrontare un percorso tortuoso ma soddisfacente. Ringrazio tutti i miei colleghi del gruppo Digicomm che ho conosciuto nel corso dei tre anni. Ho condiviso con loro momenti faticosi e difficili ma anche tante soddisfazioni. Ognuno di loro mi ha donato qualcosa e sebbene abbiano intrapreso strade diverse è comunque per me importante dedicare loro un pensiero per ringraziarli dell'affetto mostratomi. Quindi un caloroso grazie va a Giulio, Daniele, Alberto, Francesco, Lina, Stefano, Vahid, Alessandro e Sergio, ed anche alle nuovissime leve che ho conosciuto alla fine del mio percorso. Un grazie è rivolto anche ad Alessandro Vanelli Coralli che pur non essendo il mio supervisore ha contribuito alla mia crescita umana e professionale.

A special thanks is given to Prof. Dennis Akos and to his research group, who hosted me at the University of Colorado, Boulder. It has been really an honor to work with them, and it has been a wonderful opportunity of growth.

Vorrei ringraziare tutti coloro che mi hanno sempre affiancato in tutto ciò che ho fatto e che faccio ogni giorno dandomi la forza di continuare a crescere e migliorare. Quelle persone con cui ho condiviso tanto e che mi hanno reso la persona che sono oggi. Ringrazio tutti gli amici quelli di vecchia data e quelli più recenti, per avermi sostenuto nei momenti difficili ed esaltato in quelli più felici. Un grazie incommensurabile va a Stefano, una persona veramente speciale per me. Lo ringrazio per l'esserci sempre stato, disponibile, premuroso e paziente ma al tempo giusto anche severo. Lo ringrazio per la sua voglia di farmi sentire all'altezza e di vedermi realizzata e per l'infinita dolcezza e pazienza avuta anche nei momenti meno felici. Infine, devo ringraziare la mia famiglia. Mio padre, mia madre ed i miei due fratelli sono sempre stati i miei primi sostenitori. Hanno sempre creduto in me. Senza nessuna esitazione hanno accolto ogni mia decisione con felicità ed entusiasmo. Li ringrazio per tutto ciò che mi hanno trasmesso ed insegnato, e per l'immenso affetto donatomi ogni giorno.

Semplicemente, grazie a tutti ...