Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

DEPARTMENT OF INFORMATION ENGINEERING
UNIVERSITY OF PADOVA

Corso di Laurea in Ingegneria delle Telecomunicazioni

GNSS Spatial Spoofing with Ground Antenna Array

Marco Ceccato

Relatore Prof. Stefano Tomasin
Dipartimento di Ingegneria dell'Informazione
Università degli Studi di Padova

Supervisore Francesco Formaggio

14 Ottobre, 2019

Anno Accademico 2019/2020

Contents

Acronyms

ADC analog-to-digital converter 4

AGC automatic gain control 4

AWGN additive white Gaussian noise 13

BOC binary offset carrier 4

BPSK binary phase-shift keying 4, 40

CNR carrier to noise ratio 35

COTS commercial off-the-shelf 5

DGNSS differential GNSS positioning 18

DoA direction of arrival 5

DS-CDMA direct-sequence code-division multiple access 4

DSP digital signal processing 2

FDMA frequency-division multiple access 3

FIR finite impulse response 11, 27

GNSS global navigation satellite system ix, 1–7, 10, 18, 19, 32, 33, 39, 45

GPS global positioning system 1, 3, 5, 32

INS inertial navigation system 1, 6

LNA low-noise amplifier 4

LoS line-of-sight 12

LRC local replica correlation 39, 40

LS least squares ix, 2, 29, 37, 39, 45

MA multiple access 3, 4

MEO medium earth orbit 32

MIMO multiple-input and multiple-output 12–14

MSE mean squared error ix, 22, 26, 27, 30, 33, 39, 45

PDF probability density function 40

PPS precise positioning service 18

PRN pseudo-random noise 4, 10, 11, 24, 33

PVT position, velocity and precise time 5

RF radio frequency 3, 4

SER signal to error ratio 31, 32

SNR signal to noise ratio 32, 35

SPS standard positioning service 18, 39

UAV unmanned aerial vehicle ix, 1, 3, 5, 6, 45, 46

List of Figures

Abstract

The rapid growth of drone swarm technology offers incredible chances in many fields, and in turn, presents new challenges never faced before. Safety and reliability are crucial for the tasks unmanned aerial vehicles (UAVs) will cover in the future. Research on security schemes concerning the collaboration within a group of drones is still missing. In this work, we propose a novel global navigation satellite system (GNSS) spoofing approach for drone swarms. The attack relies on a powerful ground antenna array which aims at spoofing an entire region in the sky. Two signal processing schemes to perform spoofing are presented. The first one, optimum in terms of mean squared error (MSE), is based on the multidimensional extension of the Wiener filter. The latter proposal is a sub-optimal method which uses an iterative least squares (LS) strategy and requires less computational effort. Finally, spoofing performance will be evaluated according to different metrics and parameters.

Chapter 1

Introduction

In recent years the use of UAVs, is catching on in many fields. Swarms of drones are emerging as a disruptive technology to solve real-world problems for both civilian and military applications. The communication and cooperation among elements of a swarm enable to build intelligent autonomous systems where the role of a human operator can be reduced.

Usually, drones adopt sensor fusion schemes to enrich the information provided by their inertial navigation system (INS) [2]. GNSSs provide a powerful localization solution, and the fusion between GNSS data and INS enable robust real-time navigation even in challenging conditions.
The impact and the fundamental roles which drones will cover in the near future, compel the research community to focus on security aspects about drones. On December 5, 2011, an American military UAV was captured by Iranian forces exploiting a spoofing attack against the global positioning system (GPS) receiver of the drone, showing that serious vulnerabilities exist [3]. Albeit GNSS anti-spoofing research has come a long way since then, security keeps on being a crucial aspect for GNSS receivers embedded in drones. On the other hand, the recent drone incident at Gatwick Airport [4] highlighted that some defense mechanisms are required to ensure public safety in cases where a swarm of drones is under the control of malicious actors.
The purpose of this thesis is to lay the groundwork for a novel spoofing approach, which strikes several UAVs at the same time. The idea behind the *spatial spoofing attack* is to emulate onto a predefined region the desired GNSS signals dominating the one coming from real satellites by using a powerful antenna array on the ground. In contrast to the most common target-oriented attacks, the strength of the proposed spatial approach is to deceive numerous small drones with the same effort, without caring about the location tracking of each UAV. In this work, we develop models capable of

describing the scenario, we propose methods to achieve the attack efficiently, and finally, we conduct a feasibility analysis to clarify requirements. More specifically,

- in Chapter 2, a brief overview of the GNSS systems will be provided. Then key elements about GNSS signals and receivers will be outlined, whereas in the last part we will have a look at spoofing techniques and related works;
- in Chapter 3 all the models needed to describe the spatial spoofing will be presented. We will start from the geometrical model of the scenario, continuing with the channels model for both the ground and the space channel;
- in Chapter 4, the attack will be described more in details. Two digital signal processing (DSP) schemes specifically designed for the antenna array will be proposed. The first one follows the Wiener approach to produce the target signal while the second one is based on iterative LS method;
- in Chapter 5, the performance of our proposed solutions will be evaluated according to several parameters. The effect of spatial spoofing on positioning will be considered, and finally, attack schemes that use map deformations will be treated;
- in Chapter 6, conclusion and final remarks will be drawn. Requirements and assumption will be highlighted as well as consideration of computational complexity. In the end, future works and extensions will be described.

Chapter 2

GNSS Overview and Related Works

In this chapter, a short introduction of the GNSS systems will be presented. In the end, some related works regarding spoofing attacks and state-of-the-art for the UAVs security will be outlined.

2.1 GNSS Systems

A GNSS is a geolocation system composed of a network of artificial satellites in orbit and ground-based pseudolites. The GNSS systems provide accurate timing, position and navigation to electronic receivers using radio frequency (RF) signals transmitted in broadcast along the atmosphere by satellites. The operational GNSSs which today supply services around the world are the American GPS, the European Galileo, the Russian GLONASS, and the Chinese BeiDou, whereas the Indian NAVIC and the Japanese QZSS have regional coverage.
The original motivations for satellite navigation were military applications, however, GNSS positioning services have become a de facto standard for the widest range of industrial and civilian applications.

2.1.1 GNSS Signals

Today's GNSS all make use of the frequency band between 1 and 2 GHz, which is termed L-band that offers reduced attenuation and impact of atmospheric effects [1]. In Fig. 2.1 an overview of spectrum allocation is depicted. Since satellites need to share the transmission medium, GNSSs use multiple access (MA) techniques. GLONASS is based on frequency-division

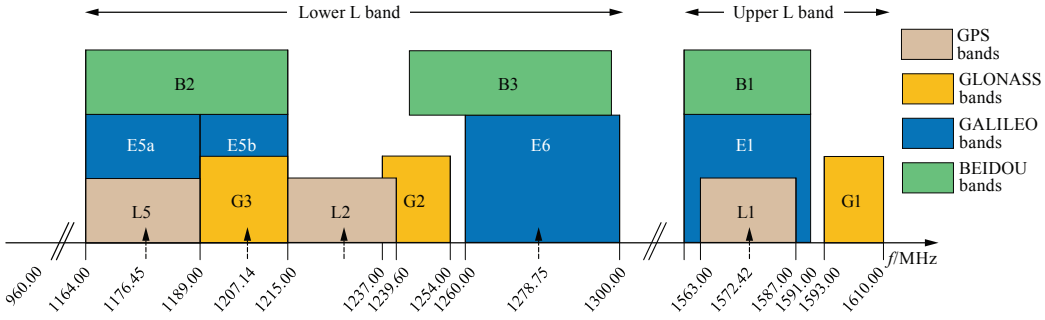


Figure 2.1: Frequency bands used by global satellite navigation systems. From [1].

multiple access (FDMA) whereas the others make use direct-sequence code-division multiple access (DS-CDMA), where each satellite has its code and their signals overlap both in time and in frequency. In the GNSS field, the codes are commonly called pseudo-random noise (PRN) binary sequences. In order to reduce the MA interference, these codes are designed to present cross-correlation orthogonality among different satellites. Codes' bandwidth is deliberately spread in the frequency domain, in order to make signals more robust to natural interference and noise.
The modulation schemes adopted in GNSS are the binary phase-shift keying (BPSK) and the binary offset carrier (BOC). In spite of their simplicity, those modulation schemes are chosen due to their autocorrelation properties that make it easy for receivers to synchronize and decode data.

2.1.2 GNSS Receivers

The structure of GNSS receivers can be separated into three main blocks:

RF Block has the purpose of listening to the medium and producing a digital signal. It is composed of L-band antenna and RF front-end including low-noise amplifier (LNA), the oscillator, down converter and mixers, and the bandpass filters. Finally, there is the analog-to-digital converter (ADC) and, optionally, an automatic gain control (AGC).

Signal-processing Block aims at de-spreading the received signals and producing the so-called pseudoranges. Local replicas of reference signals for each satellite are generated and then by performing cross-correlation functions each satellite's signal is separated from the other satellite signals. Once acquired, the Doppler shift and the code phase of each signal are estimated by tracking loops which exploit feedback

structures to refine the estimations over time. The output of this block is thus the set of pseudoranges and the decoded data message.

Navigation Block processes the data messages and pseudoranges in order to obtain the position, velocity and precise time (PVT). It performs positioning algorithms that are based on the triangulation process, and exploit all the available data/corrections to improve the final accuracy.

Nowadays, multifrequency and multi-constellation receivers (including GPS, Galileo, GLONASS, BeiDou) are on the market and their accuracy keeps growing. Moreover, regional augmentation systems provide additional corrections to increase their performance.

2.2 Spoofing and Detection Schemes

Spoofing of GNSS is the transmission of fake signals with the intent that the victim receiver will deem them as authentic signals. Increased concern about GNSS spoofing is being caused by recent news reports about GNSS attacks [3, 4, 5] and by the availability of inexpensive programmable signal simulators that can be used to mount an attack with commercial off-the-shelf (COTS) hardware [6]. Anti-spoofing research has evolved in the last years to face these aspects, proposing spoofing detection techniques to monitor the integrity of received signals. However, most of the general-purpose receivers available on the market do not develop advanced anti-spoofing tools and thus cannot be considered secure against the state-of-the-art attacks. On the upside, advanced authentication schemes on both data and signals level are paving the way for future GNSS systems [7, 8, 9] , nevertheless, the road is still long, and current GNSS receivers are still carefully exposed making GNSS-driven systems prone to unpredictable incidents.
In [6] cutting-edge attacks and defense schemes are reviewed. The use of multiple antennas introduces new possibilities for both attack and defense side. Consistency among received signals on different antennas and the estimation of the direction of arrival (DoA) [10, 11] can be used as defense mechanisms. Multiantenna receivers can furthermore improve the positing performance against jamming and other interferences by using signal processing techniques [12].

2.2.1 Drone Swarms Security

The rise of UAV and drone swarms presents new challenges to ensure security both for data communication with ground stations and for providing robust

navigation algorithms which prevent malicious attacks. We will focus on GNSS related issues with special attention on security for groups of drones which is a new field of research, whereas [13] offers a literature review on spoofing against a single UAV target.
Jamming is surely the rudest technique, however, can still be effective toward commercial GNSS receivers [14]. Jamming is powerful to strike several targets at the same time, however, since it can be easily detected, jamming can be circumvented by drone swarms switching into INS navigation until the attack is evaded. Multi-agent inertial navigation can indeed be reliable for short periods without the need for GNSS support. To avoid attack detection, more sophisticated techniques are thus required, especially for swarms of drones where UAVs can exchange data among them to collaborate and verify the consistency of the received GNSS signals [15]. In order to spoof several targets, the consistency must be maintained, and precise estimations for the UAVs' locations may be required to adopt beamforming techniques and get individual channels. However, when the number of drones is large, the obtaining of their precise locations may become tricky. Moreover, assuring consistency of spoofed positions can turn stringent in cases where drones have additional information on their positional relations by the use of other geolocation methods. In [16] the spoofing of a group of drones is investigated and calculation for attacker's antennas placement are stated, under the assumption that the locations of UAVs are fixed and known.
This thesis proposes a new approach not present in the literature. Spoofing an entire region instead of a set of targets implies a change of perspective. First of all, it automatically solves the problem of keeping consistency among spoofed signals, then it also makes less stringent the requirements about knowledge of UAVs' locations. As we will see, nothing comes for free, and spatial spoofing would require more resources, despite this, the novel approach could produce interesting advances at the intersection of drone swarms and GNSS security.

Chapter 3

System Models

As mentioned in Chapter 1, the concept of the attack is to replicate a target GNSS signal over a map by using a set of ground antennas to deceive the drones' receiver. The purpose of this chapter is to outline details about the attack setting and simplifying assumptions, and create useful models allowing a mathematical description of the scenario.

3.1 Geometric Model of the Scenario

The entities involved in the attack are the emulated orbiting satellites, the malicious antennas array, the GNSS receivers embedded in drones and finally the region where the swarm is supposed to fly over. A representation of the system is depicted in Fig. 3.1, where the reader can get a visual representation of the entities and their placement. The considered area of interest over which the attacker aims to spoof the signal is assumed to be a 2D rectangular region. The extension to 3D regions is feasible, however, since most of the swarm flying formations place drones at the same height [17], the lower-dimensional case seems to be more appealing. We fix an orthonormal coordinate system with unit vectors $\hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}, \hat{\boldsymbol{z}}$ and an origin point O. For simplicity, we could set O_z to be placed at the sea level. We refer to this system as the reference coordinate system.
Let $\mathcal{M}$ be the plane over which we aim to produce the target/fake signal:

$$\mathcal{M} = \{(x, y, z) \in \mathbb{R}^3 : x \in [x_a, x_b], y \in [y_a, y_b], z = h\}, \tag{3.1}$$

where h is the height of the region from the ground. Let N_s be the number of satellites involved. The i-th satellite is denoted as $\mathcal{S}_i$ and its location is:

$$\boldsymbol{p}_i^{(\mathcal{S})} = \left(x_i^{(\mathcal{S})}, y_i^{(\mathcal{S})}, z_i^{(\mathcal{S})}\right) \qquad i = 0, 1, \ldots, N_s - 1. \tag{3.2}$$

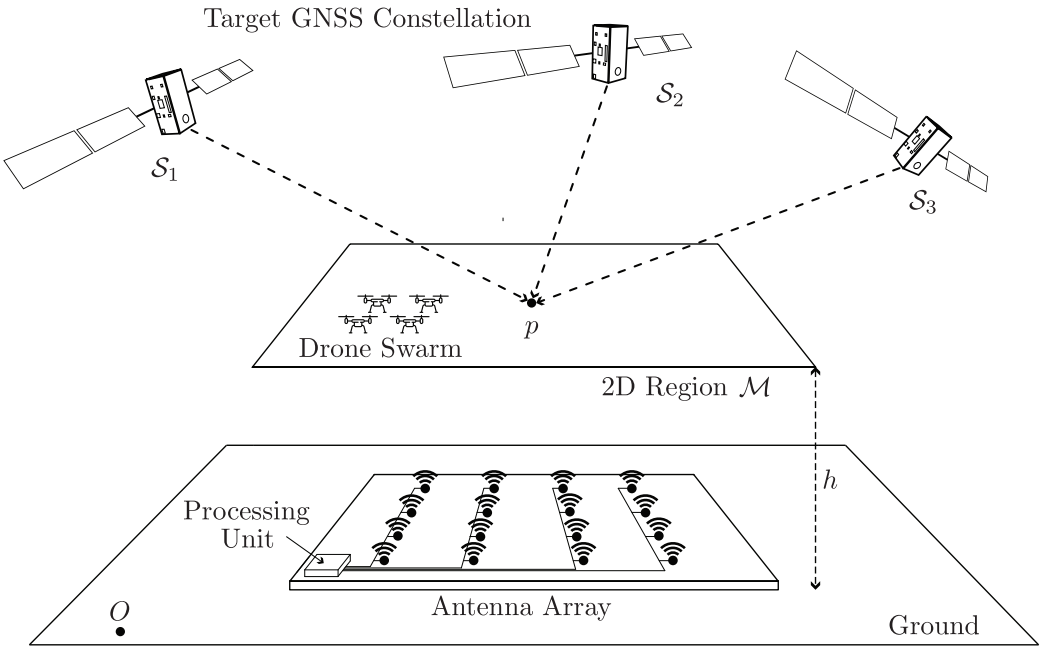


Figure 3.1: Scenario overview with $N_s = 3$ satellites and $N_p = 16$ antennas.

The distance between the generic point $\boldsymbol{p} = (x, y, h) \in \mathcal{M}$ and the i-th satellite is:

$$\rho_i^{(\mathcal{S})}(x, y) = \sqrt{\left(x - x_i^{(\mathcal{S})}\right)^2 + \left(y - y_i^{(\mathcal{S})}\right)^2 + \left(h - z_i^{(\mathcal{S})}\right)^2}. \tag{3.3}$$

In the considered scenario all the N_a antennas are placed at the sea level over a square region whose size, in general, may be different from that of $\mathcal{M}$. A few words about the placement policy will be carried out later on. The same reasoning about distances between points of $\mathcal{M}$ and the i-th antenna can be done, obtaining the antennas-map ranges $\rho_i^{(\mathcal{A})}(x, y)$. Let c denote the speed of light in vacuum, thus the overall signal propagation delay between the map and the antennas/satellites can be approximated with:

$$\tau_i^{(\mathcal{S})}(x, y) = \frac{\rho_i^{(\mathcal{S})}(x, y)}{c} \qquad \tau_k^{(\mathcal{A})}(x, y) = \frac{\rho_k^{(\mathcal{A})}(x, y)}{c}. \tag{3.4}$$

Antennas and satellites are assumed to stand still, thus the time evolution does not affect the geometrical models used in this work. However, the quick movement of satellites underlines the need for refreshing over a long observation period.

3.1.1 Grid representation of the Map

Albeit the above model is consistent and flexible to describe region $\mathcal{M}$, a discrete representation of the system is needed to obtain a numerically treatable model. The region $\mathcal{M}$ is therefore represented as a finite set of points $\mathcal{P} \subset \mathcal{M}$ located on a grid layout with step-size δ on both axis. In Fig. 3.2 a representation of the grid is shown. The grid is composed by P points on

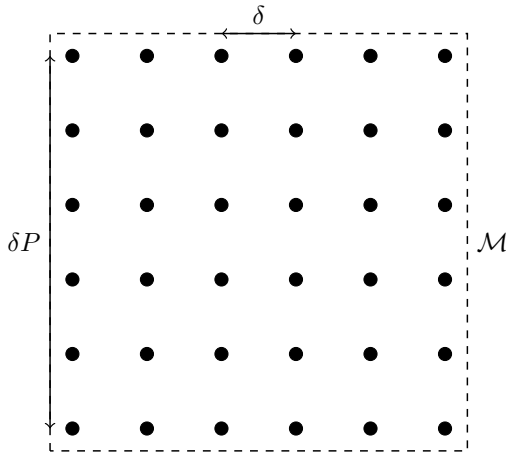


Figure 3.2: Grid representation of the Map by using $N_p = 36$ points.

the x-axis and P points on the y-axis for a total of $N_p = P^2$ points. The grid elements are described by index $j = (q-1)P + p$, where $p \in \{1, 2 \ldots, P\}$ denotes the index on x-axis and $q \in \{1, 2, \ldots, P\}$ denotes the index on y-axis. The location of the j-th point is denoted as:

$$\boldsymbol{p}_j^{(\mathcal{P})} = \left(x_j^{(\mathcal{P})}, y_j^{(\mathcal{P})}, h\right) = \left((p-1)\delta, (q-1)\delta, h\right). \tag{3.5}$$

The notation used for the ranges on the map, previously defined as a function of x and y, can now be simplified by expressing the ranges for the j-th point as:

$$\tau_{i,j}^{(\mathcal{S})} = \tau_i^{(\mathcal{S})}\left(x_j^{(\mathcal{P})}, y_j^{(\mathcal{P})}\right) \qquad \tau_{k,j}^{(\mathcal{A})} = \tau_k^{(\mathcal{A})}\left(x_j^{(\mathcal{P})}, y_j^{(\mathcal{P})}\right). \tag{3.6}$$

More consideration about the grid and its parameters will be drawn in the Chapter 5.

3.1.2 Antenna Array

The attacker is supposed to have under his control an antenna array, namely a set of multiple connected antennas which work together as a single antenna.

Albeit it is not ensured to be the best layout for the aimed task, the N_a antennas are placed at sea level following a 2D grid shape similar to the one of the map. The k-th antenna is denoted as $\mathcal{A}_k$ and its location as:

$$\boldsymbol{p}_k^{(\mathcal{A})} = \left(x_k^{(\mathcal{A})}, y_k^{(\mathcal{A})}, 0\right). \tag{3.7}$$

Since the power of the signal to spoof is extremely low, is it expected that very-low power antennas are needed, leading to several feasible L-band array implementations that use a significant number of small dipoles, such as large microstrip antenna.

3.2 Signal Model

The model used to represent the transmitted baseband GNSS signal is the following:

$$s_i(t) = \sum_{\ell=-\infty}^{+\infty} \sum_{k=0}^{Q-1} d_\ell^{(i)} c_k^{(i)} h_{T_x}\left(t - (k + \ell Q)T_c\right), \tag{3.8}$$

where:

- $c_k^{(i)} \in \{-1, 1\}$ is the periodic *spreading code* or PRN sequence associated with the i-th satellite. We denote with N_c its period;
- $d_\ell^{(i)} \in \{-1, 1\}$ is the navigation data transmitted by the i-th satellite;
- Q is the number of chip between the change of data, usually is a multiple of the code length N_c. The ratio $\frac{1}{QT_c}$ is the navigation data frequency;
- $h_{T_x}(t)$ is the real-valued pulse that represents the chip and has finite-energy E_h;
- T_c is the chip period.

However, since the navigation data are not considered because they don't affect the behavior of the signal we would like to replicate, we impose $d_\ell^{(i)} = 1$, $\forall i, \ell$. The assumption translates into the following simplified model:

$$s_i(t) = \sum_{k=-\infty}^{+\infty} c_k^{(i)} h_{T_x}\left(t - kT_c\right), \tag{3.9}$$

and the corresponding passband signal is:

$$s_i^{(pb)}(t) = \Re\left[e^{\mathrm{i}\,2\pi f_c t + \mathrm{i}\,\phi_{i,0}} s_i^{(bb)}(t)\right], \tag{3.10}$$

where f_c is the carrier frequency of the GNSS system and $\phi_{i,0}$ is the initial phase offset for the carrier and i is the imaginary unit. Unless made explicit, we will refer to baseband signals in the following.

3.2.1 Discrete Time Model

We consider that the satellites are synchronized and they share a common time reference. Using the continuous-signal model defined in Section 3.2, the satellites' signal is obtained directly from the spreading code and then transmitted by using the transmission filter h_{Tx}. The equivalent discrete-time representation is obtained as follows. The PRN codes for all the satellites are represented by the vector $\boldsymbol{c}_k$:

$$\boldsymbol{c}_k = \left[c_k^{(0)}, c_k^{(1)}, \ldots, c_k^{(N_s-1)}\right]^T \in \{-1, 1\}^{N_s \times 1}, \tag{3.11}$$

whose components are periodic in k with period N_c. In this work the signals are represented with a sample time larger than the chip time T_c. Let κ be the chip oversampling factor. We define the sampling time according to the following relationship:

$$T_s = \frac{T_c}{\kappa} \qquad \kappa \in \mathbb{N} \setminus \{0\}, \tag{3.12}$$

thus we obtain κ samples per chip. Since $\boldsymbol{c}_k$ has sample time T_c and the signal we aim to model, namely $\boldsymbol{s}_\ell$, has different sampling frequency we used a multi-rate system approach [18] to address the problem. The signal $\boldsymbol{c}_k$ is firstly upsampled by a factor κ:

$$\boldsymbol{z}_\ell = \begin{cases} \kappa \boldsymbol{c}_k & kT_c = \ell T_s \Leftrightarrow k\kappa = \ell, \\ 0 & \text{otherwise}, \end{cases} \tag{3.13}$$

and then it is filtered by the finite impulse response (FIR) filter h_{Tx}:

$$s_\ell^{(i)} = z^{(i)} * h_{Tx}\,[\ell] \qquad i = 0, 1, \ldots, N_s - 1, \tag{3.14}$$

where $x * y[n]$ is the convolution between signals x and y, computed at time n. In Fig. 3.3 the process is summarized. Note that the filter h_{Tx} plays two roles:

1. The role of interpolation filter to remove replicas in the frequency domain;
2. The role of transmission filter that shapes the spectrum according to the designed modulation scheme.

In this work the chosen pulse shape is the raised cosine with the roll-off factor β.

3.3 Channel Models

In the aforementioned scenario there are two different channels, the former between the antennas, and the grid and the latter between satellites and the target map. For both channels it is assumed line-of-sight (LoS) propagation and the absence of *fast-fading* and *multi-path* phenomena. The Doppler shift is to be considered perfectly counterbalanced by the tracking process. The considered effects of the channels on the transmitted signals are only two:

- Delays $\tau^{(\mathcal{S})}$ and $\tau^{(\mathcal{A})}$ that play a fundamental role for the positioning estimation;
- Attenuation that follows the *free-space path loss* propagation principle.

As we will see, each point of the grid can be seen as a receive antenna providing a multiple-input and multiple-output (MIMO) scheme.

3.3.1 Ground Channel

This section will focus on modeling the channel for the ground antenna array. The previously mentioned channel's effects between the k-th antenna and the j-th point of the map-grid can be described by the following transfer function:

$$h_{k,j}(t) = \sqrt{A_{k,j}^{(\mathcal{A})}}\delta\left(t - \tau_{k,j}^{(\mathcal{A})}\right), \tag{3.15}$$

where $A_{k,j}^{(\mathcal{A})}$ is the free-space attenuation term:

$$A_{k,j}^{(\mathcal{A})} = \left(\frac{c}{4\pi f_c \rho_{k,j}^{(\mathcal{A})}}\right)^2 \qquad \rho_{k,j}^{(\mathcal{A})} = \left\|\boldsymbol{p}_k^{(\mathcal{A})} - \boldsymbol{p}_j^{(\mathcal{P})}\right\|. \tag{3.16}$$

The sampling time of the entire discrete-time system is T_s. The sample transmitted at time ℓ from the k-th antenna is denoted as $x_\ell^{(k)}$.
Using the above assumptions, we can represent the discrete-time channel by a discrete-time complex filter with a single tap at delay $\tau_{k,j}^{(\mathcal{A})}$. It is possible

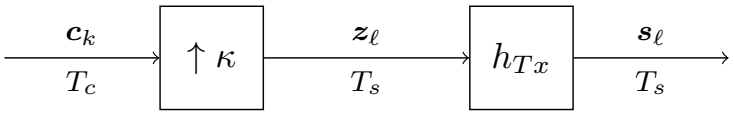


Figure 3.3: Discrete time processing of the satellites' signals.

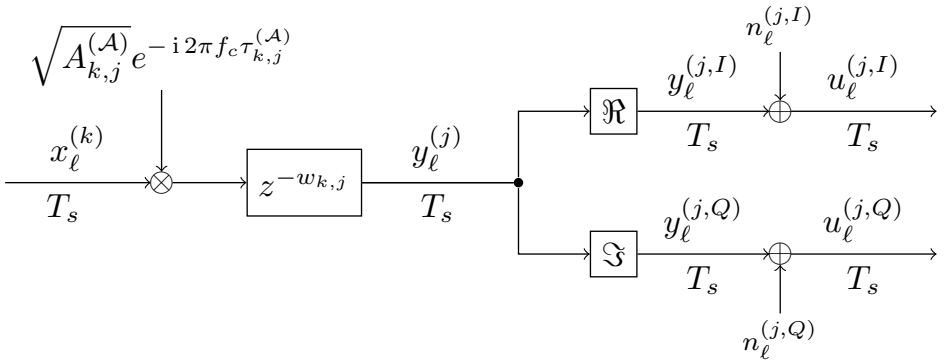


Figure 3.4: Representation of the point-to-point baseband channel between the k-th ground antenna and the j-th point of the grid.

to decompose the delay term as:

$$\begin{aligned} \tau_{k,j}^{(\mathcal{A})} &= w_{k,j} T_s + r_{k,j} \\ w_{k,j} = \left\lfloor \frac{\tau_{k,j}^{(\mathcal{A})}}{T_s} \right\rfloor \in \mathbb{Z}^+ \qquad & r_{k,j} = \mathrm{mod}\left(\tau_{k,j}^{(\mathcal{A})}, T_s\right) \in [0, T_s), \end{aligned} \tag{3.17}$$

where $w_{k,j}$ represents the delay (in number of symbol periods) of the received signal , whereas $r_{k,j}$ is the reminder that affects only the phase. If all the terms $w_{i,j}$ were equal on the grid, we would neglect that decomposition by considering the classic MIMO model, neglecting the group delay of $w_{i,j}$ samples, however, in our case most of them are not equal. We assume all the antennas (and the satellites) to be perfectly synchronized, thus we only add the residual carrier phase term, namely $e^{-\mathrm{i}\,2\pi f_c \tau_{k,j}^{(\mathcal{A})}}$, arising from the baseband down-conversion. The point-to-point baseband channel is then summarized in Fig. 3.4, where the in-phase and quadrature components of $y_\ell^{(j)}$ are considered, and where $n_\ell^{(j)}$ is the additive white Gaussian noise (AWGN) term. The aim of this section is to create a model that takes into consideration all the points of the grid and manage all the ground antennas as a single transmitter. The set containing all the antennas' samples at time ℓ is represented as the following vector:

$$\boldsymbol{x}_\ell = \left[x_\ell^{(0)}, x_\ell^{(1)}, \ldots, x_\ell^{(N_a-1)}\right]^T \in \mathbb{C}^{N_a \times 1}, \tag{3.18}$$

and using the same notation, the received signal in all the points of the map as:

$$\boldsymbol{y}_\ell = \left[y_\ell^{(0)}, y_\ell^{(1)}, \ldots, y_\ell^{(N_p-1)}\right]^T \in \mathbb{C}^{N_p \times 1}. \tag{3.19}$$

We define the following quantities:

$$\begin{aligned} h_{\min} &= \min_{k,j} w_{k,j} \\ h_{\max} &= \max_{k,j} w_{k,j} \\ L_h &= h_{\max} - h_{\min} + 1. \end{aligned} \tag{3.20}$$

The idea is to extend the classical MIMO channel model [19] by considering its temporal evolution, represented by L_h filter taps. Hence the model for the input-output relation is:

$$\boldsymbol{y}_\ell = \sum_{h=h_{min}}^{h_{max}} \hat{\boldsymbol{H}}_h \boldsymbol{x}_{\ell-h} \qquad \hat{\boldsymbol{H}}_h \in \mathbb{C}^{N_p \times N_a}, \tag{3.21}$$

where for each time h, the entries of matrix $\hat{\boldsymbol{H}}_h$ are defined as:

$$h_{j,k}^{(h)} = \begin{cases} \sqrt{A_{k,j}^{(\mathcal{A})}} e^{-\mathrm{i}\, 2\pi f_c \tau_{k,j}^{(\mathcal{A})}} & \text{if} \quad h = w_{k,j}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.22}$$

Notice that the larger is κ, the longer is the temporal-length of the filter. Other factors that contribute to determine L_c are: the size of the map, the antenna disposition and the height of grid.
Note that the peculiarity of the described scenario is that, even by assuming a flat fading channel represented by one single tap, we end up with a *memory effect* on the map that must be taken into account. In fact, the signal received at time ℓ is written as a function of several past samples $\boldsymbol{x}_{\ell-h}, h = h_{\min}, \ldots, h_{\max}$.

Special case of memory less channel

When $h_{\max} = h_{\min} = \bar{h}$ the previously defined model becomes the well-known MIMO channel model with a group delay of $\bar{h}$ samples:

$$\boldsymbol{y}_\ell = \hat{\boldsymbol{H}} \boldsymbol{x}_{\ell-\bar{h}}. \tag{3.23}$$

As we will se later on, in this case there are some implications can simplify the attacker task.

3.3.2 Space Channel

Using a similar formulation of the ground channel, it is possible to define the model for the channel between the satellites and the drones (space channel).

The first assumption is that the satellites are considered to be synchronized and transmit their symbols at the same time. The point-to-point channel between the i-th satellite and the j-th point of the grid has the same model of (3.15) and it is denoted as:

$$g_{i,j}(t) = \sqrt{A_{i,j}^{(\mathcal{S})}}\delta\left(t - \tau_{i,j}^{(\mathcal{S})}\right). \tag{3.24}$$

In the space channel the delay $\tau_{i,j}^{(\mathcal{S})}$ can be decomposed in several parts. The understanding of all its contribution is crucial to properly model the target signal in such a way the behavior of the GNSS signals is ensured whereas other aspects that do not affect the attack analysis are ignored. The total propagation delay between the i-th satelite to the j-th grid point can be decomposed as:

$$\tau_{i,j}^{(\mathcal{S})} = q_{i,j}QT_c + f_{i,j}T_c + b_{i,j}T_s + \xi_{i,j}, \tag{3.25}$$

where:

- $q_{i,j}$ is the delay (in data symbols) to propagation. This quantity is not important to express the target signal, because we neglect the data $d_\ell^{(i)}$. Therefore this delay can be considered as a group delay;

$$q_{i,j} = \left\lfloor \frac{\tau_{i,j}^{(\mathcal{S})}}{QT_c} \right\rfloor \in \mathbb{Z}^+ \tag{3.26}$$

- $f_{i,j}$ describes the remaining delay as the circular shift of the PRN code on its period, it is fundamental to estimate the pseudo-range;

$$f_{i,j} = \left\lfloor \frac{\tau_{i,j}^{(\mathcal{S})}}{T_c} \right\rfloor - q_{i,j}Q \quad \in \{0, 1, \ldots, N_c - 1\} \tag{3.27}$$

- $b_{i,j}$ is the remaining delay (in number of samples). This quantity is fundamental for the sample-level synchronization with the local replica, to achieve cross-correlation with a temporal resolution of T_s;

$$b_{i,j} = \left\lfloor \frac{\tau_{i,j}^{(\mathcal{S})}}{T_s} \right\rfloor - \kappa\left(q_{i,j}Q + f_{i,j}\right) \quad \in \{0, 1, \ldots, \kappa - 1\} \tag{3.28}$$

- $\xi_{i,j}$ is the reminder, that we do not consider. This contribution can be estimated by using the carrier phase estimation.

$$\xi_{i,j} = \mod\left(\tau_{i,j}^{(\mathcal{S})}, T_s\right) \quad \in [0, T_s) \tag{3.29}$$

Once obtained the above quantities, we can follow the same approach used for the ground channel to build the space channel model. First of all, in order to determine the length of the filter, the following quantities are defined:

$$\begin{aligned} \hat{g}_{\min} &= \min_{i,j} \left(\kappa f_{i,j} + b_{i,j}\right) \\ \hat{g}_{\max} &= \max_{i,j} \left(\kappa f_{i,j} + b_{i,j}\right) \\ L_{\hat{g}} &= \hat{g}_{\max} - \hat{g}_{\min} + 1. \end{aligned} \tag{3.30}$$

The space channel use as input the signal $\boldsymbol{s}_\ell$ defined in Section 3.2.1, and produce as output the signal $\boldsymbol{r}_\ell \in \mathbb{C}^{N_p \times 1}$, with the following input-output relation:

$$\boldsymbol{r}_\ell = \sum_{h=\hat{g}_{\min}}^{\hat{g}_{\max}} \hat{\boldsymbol{G}}_h \boldsymbol{s}_{\ell-h} \qquad \hat{\boldsymbol{G}}_h \in \mathbb{C}^{N_p \times N_s}, \tag{3.31}$$

where the the entries of the h-th tap of $\hat{\boldsymbol{G}}_h$ are obtained as for the ground channel:

$$\hat{g}_{j,i}^{(h)} = \begin{cases} \sqrt{A_{i,j}^{(\mathcal{S})}} e^{-\mathrm{i}\, 2\pi f_c \tau_{i,j}^{(\mathcal{S})}} & \text{if} \quad h = \kappa f_{i,j} + b_{i,j}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.32}$$

We finally define as the target signal, or desired signal:

$$\boldsymbol{d}_\ell = \alpha \boldsymbol{r}_\ell \qquad \alpha \in \mathbb{R}^+, \tag{3.33}$$

albeit $\boldsymbol{r}_\ell$ holds all the features to be the target GNSS signal, the attacker may additionally decide to alter the power of the spoofed signal or to change dynamically α to make the attack more effective.

3.4 Receiver Architecture

In this section we describe the simplified architecture of the hypothetic receivers under attack, underlying some observation regarding our aimed target signal $\boldsymbol{d}_\ell$, the actual spoofed signal $\boldsymbol{y}_\ell$ and the position estimation process. In our model, the receiver is supposed to know all the propagation details, making possible to down-convert the passband signal directly to baseband without any residual frequency and considering the time frame of reference to be synchronized between satellites and receivers. The sampling time of the received signal is assumed to be T_s. The receiver, placed in the j-th point of the grid obtains the baseband signal, processes M samples of the

received signal $y_\ell^{(j)}$ and, for each of the constellation satellites, performs a cross-correlation with a local replica $\tilde{c}_\ell^{(i)}$ as a function of m, i.e.,

$$R_m^{(i,j)} = \sum_{\ell=0}^{M-1} y_\ell^{(j)} \tilde{c}_{\ell-m}^{(i)}. \tag{3.34}$$

The acquisition process aims at finding the optimum value of m which maximizes the correlation, i.e.,

$$m_{i,j}^* = \underset{m\in\{0,\dots,\kappa N_c-1\}}{\operatorname{argmax}} R_m^{(i,j)}. \tag{3.35}$$

Note that using this approach, for a higher sampling rate the correlation is more precise, since we increase the temporal resolution to track accurately the delay. Usually $M = \kappa N_c$ or a multiple of that quantity, but in general M can take any value. After the acquisition process, the delay $\tau_{i,j}^{(S)}$ (neglecting $q_{i,j}$ contribution) is approximated as:

$$\left(\kappa f_{i,j} + b_{i,j}\right) T_s + \xi_{i,j} = m_{i,j}^* T_s + \epsilon \quad \epsilon \in [0, T_s]. \tag{3.36}$$

We assume ϵ to be uniformly distributed in the interval $[0, T_s]$, namely $\epsilon \sim \mathcal{U}(0, T_s)$. Hence the estimate average for the partial delay is:

$$\mathbb{E}\left[\left(\kappa f_{i,j} + b_{i,j}\right) T_s + \xi_{i,j}\right] = m_{i,j}^* T_s + \frac{T_s}{2}. \tag{3.37}$$

In order to compute the final pseudorange we require the value of $q_{i,j}$. Usually, receivers resolve this integer ambiguity and here $q_{i,j}$ is supposed to be known. The estimation of the pseudorange between the i-th satellite and the receiver is therefore:

$$\hat{\rho}_{i,j} = c\left(q_{i,j} Q N_c T_c + m_{i,j}^* T_s + \frac{T_s}{2}\right). \tag{3.38}$$

The propagation of the error, due to the unknown ϵ, on the pseudorange is:

$$\rho_{i,j} = \hat{\rho}_{i,j} + c\left(\epsilon - \frac{T_s}{2}\right). \tag{3.39}$$

Hence the true distance $\rho_{i,j}$ between the i-th satellite and the receiver is bounded by:

$$\hat{\rho}_{i,j} - \frac{cT_c}{2\kappa} \leq \rho_{i,j} \leq \hat{\rho}_{i,j} + \frac{cT_c}{2\kappa}, \tag{3.40}$$

from where we can note that, in our model, the accuracy of the pseudorange estimation depends on the oversampling factor κ. As already mentioned, this estimation can be improved by looking at the phase $\phi_{i,j}^{(\mathcal{S})}$ of the received signal, however for now this is not taken into account.

3.4.1 Position Estimation Algorithm

Once the baseband signal processing component computes the measurements, the next step is to use the pseudoranges to estimate the location of the receiver. Several positioning schemes are available in the literature: a) Code Based Positioning, or standard positioning service (SPS), b) Code and Carrier Based Positioning, or precise positioning service (PPS), c) differential GNSS positioning (DGNSS).

- The receiver does not introduces further time offsets. The spoofing attack starts after the receiver is tracking the true GNSS signals, then it is already synchronized with the satellite system time. This assumption considerably simplifies our problem by removing the uncertainty of the time synchronization. Moreover the minimum number of satellites required to compute an estimate drops to 3 instead of 4.

- The carrier phase is not tracked. Albeit PPS positioning is extremely accurate phase tracking is a difficult task, especially for a moving receiver such as those embedded in drones.

- The exact location of the satellites is known. Using the navigation data, the GNSS systems provide the location of the satellites.

In order to implement the SPS, we use an iterative solution by linearizing the problem with respect to successive approximations of the receiver location and use the *Least-Square method* when more than 3 satellites are in view. See Appendix A for the details.

Chapter 4

Spatial Spoofing Attack

In the previous Chapter 3 we established the scenario where the attack takes place and we built some related models. In this chapter the attack and our proposed solutions to make the spoofing effective will be described.

4.1 Attack Scheme

As already mention in Chapter 1, the attacker aims to replicate a counterfeit 2D map of a given location A at a height h in region $\mathcal{M}$ at location B. The grid defined in Section 3.1.1 and the antenna array shall be placed in the site B. The fake map to be spoofed in the grid and the setting needed before proceeding with the actual attack are generated according to the following procedure:

1. The attacker designs the grid with N_p points where the drone swarm is hovering or where it is supposed fly over. The ground channel is computed following the model presented in Section 3.3.1;

2. The attacker designs an equivalent grid that represent the sky of site A by using the same number of point N_p of the other grid. The satellites channel is carried out using model defined in Section 3.3.2.

Each point of the grid placed in A matches one point of the grid located in B. For simplicity, in the description of the geometrical model the two grids are the same and overlaps. Note that the two grids can have different heights, inclinations and sizes thereby enabling the attacker to produce deformation effect on the map that might be useful to manipulate the swarm formation and deceive their GNSS receivers. Albeit we do not cover this aspect, it is not mandatory for the points representing the maps to be placed following a

grid scheme, allowing other possible disposition accurately designed by the attacker. Once the channel for both the target map and the actual region under attack are determined, we can summarize the models used to represent the target signal $\boldsymbol{d}_\ell$, and the received signal $\boldsymbol{y}_\ell$ as:

$$\begin{cases} \boldsymbol{y}_\ell = \sum_{h=h_{min}}^{h_{max}} \hat{\boldsymbol{H}}_h \boldsymbol{x}_{\ell-h} & \text{for the ground channel,} \\ \boldsymbol{d}_\ell = \alpha \sum_{h=\hat{g}_{\min}}^{\hat{g}_{\max}} \hat{\boldsymbol{G}}_h \boldsymbol{s}_{\ell-h} & \text{for the space channel.} \end{cases} \tag{4.1}$$

The purpose of the spatial spoofing attack is thus, for a given signal $\boldsymbol{d}_\ell$, to replicate it through using $\boldsymbol{y}_\ell$ by transmitting an appropriate signal $\boldsymbol{x}_\ell$. Let $\boldsymbol{e}_\ell$ be the error between the desired sample vector $\boldsymbol{d}_\ell$ and the obtained spoofed sample vector $\boldsymbol{y}_\ell$, at the ℓ-th sample, i.e.,

$$\boldsymbol{e}_\ell = \boldsymbol{y}_\ell - \boldsymbol{d}_\ell. \tag{4.2}$$

In the following we will focus on signal processing schemes to obtain efficiently $\boldsymbol{x}_\ell$ that replicates as closely as possible the target signal, minimizing the required resource and the reconstruction error $\boldsymbol{e}_\ell$ for given interval of time. Writing the problem in mathematical terms, we aim to solve the following optimization problem:

$$\{\boldsymbol{x}_\ell\}_{opt} = \arg\min_{\{\boldsymbol{x}_\ell\}} \mathbb{E}\left[\boldsymbol{e}_\ell^H \boldsymbol{e}_\ell\right], \tag{4.3}$$

for a given time interval, by using N_a ground antennas and all the models presented so far.

4.2 Multidimensional Wiener Scheme

The first proposed solution for the above problem is based on the well-known Wiener filter [20] extended to the multidimensional case. The main assumption behind this approach is that in order to replicate $\boldsymbol{d}_\ell$ on the grid, the signal $\boldsymbol{x}_\ell$ to be transmitted by the N_a ground antennas should be written as the linear combination of the satellites' codes $\boldsymbol{c}_k$, for a sufficiently large set of samples.
The idea is hence to filter the up-sampled signal $\boldsymbol{z}_k$ with the multidimensional filter $\boldsymbol{C}$ to obtain the antennas' signals. In Figure 4.1 an overview of the system is depicted. The filter $\boldsymbol{C}$ has several implicit constraints needed for the spoofing of the target signal:

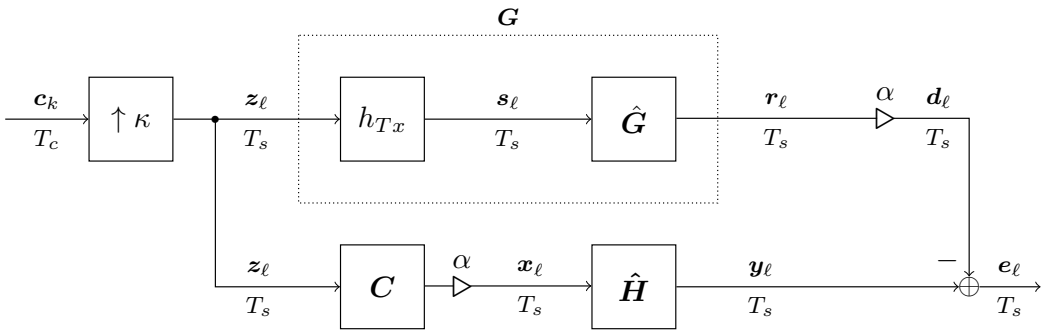


Figure 4.1: The multidimensional Wiener scheme.

- Interpolate the signal $\boldsymbol{z}_\ell$ to remove the frequency repetitions arising from upsampling;
- Perform the proper pulse shaping to make the output signal $\boldsymbol{x}_\ell$ ready for transmission;
- Operate as channel equalizer to compensate for effects introduced by the ground channel $\hat{\boldsymbol{H}}$.

Let us consider $\boldsymbol{G}$ as the cascade of h_{Tx} and the satellite channel $\hat{\boldsymbol{G}}$, then, using the notation of the satellite channel, we can write the desired signal as:

$$\boldsymbol{d}_\ell = \alpha \sum_{p=g_{min}}^{g_{max}} \boldsymbol{G}_{\ell-p}\boldsymbol{z}_p \qquad \boldsymbol{G}_p \in \mathbb{C}^{N_p \times N_s} \quad \boldsymbol{z}_\ell \in \mathbb{Z}^{N_s \times 1}, \tag{4.4}$$

where g_{min} and g_{max} determine the length of the filter $\boldsymbol{G}$, i.e.,

$$\boldsymbol{G}_\ell \neq \boldsymbol{0} \qquad \text{for:} \quad g_{min} \leq \ell \leq g_{max}. \tag{4.5}$$

Let $L_c = c_{max} - c_{min} + 1$ be a design parameter for the filter. Therefore, by filtering the signal $\boldsymbol{z}_\ell$ with $\boldsymbol{C}$, we obtain the signal

$$\boldsymbol{x}_\ell = \alpha \sum_{p=\ell-c_{max}}^{\ell-c_{min}} \boldsymbol{C}_{\ell-p}\boldsymbol{z}_p \qquad \boldsymbol{C}_\ell \in \mathbb{C}^{N_a \times N_s}. \tag{4.6}$$

Then the received signal $\boldsymbol{y}_\ell$ can be written as a function of transmitted $\boldsymbol{x}_\ell$ by using a slightly different version of (3.21), namely

$$\boldsymbol{y}_\ell = \sum_{q=\ell-h_{max}}^{\ell-h_{min}} \hat{\boldsymbol{H}}_{\ell-q}\boldsymbol{x}_q \qquad \boldsymbol{x}_q \in \mathbb{C}^{N_a \times 1}. \tag{4.7}$$

Using the above notation the received signal can hence be written as the double filtering of $\boldsymbol{z}_\ell$:

$$\boldsymbol{y}_\ell = \alpha \sum_{q=\ell-h_{max}}^{\ell-h_{min}} \sum_{p=q-c_{max}}^{q-c_{min}} \hat{\boldsymbol{H}}_{\ell-q} \boldsymbol{C}_{q-p} \boldsymbol{z}_p. \tag{4.8}$$

The aim of this section is to find the best coefficients for the filter $\boldsymbol{C}$:

$$\boldsymbol{C}_\ell = \begin{bmatrix} \hat{c}_{0,0}^{(\ell)} & \hat{c}_{0,1}^{(\ell)} & \cdots & \hat{c}_{0,N_s-1}^{(\ell)} \\ \hat{c}_{1,0}^{(\ell)} & \hat{c}_{1,1}^{(\ell)} & \cdots & \hat{c}_{1,N_s-1}^{(\ell)} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{c}_{N_a-1,0}^{(\ell)} & \hat{c}_{N_a-1,1}^{(\ell)} & \cdots & \hat{c}_{N_a-1,N_s-1}^{(\ell)} \end{bmatrix} \qquad \ell = c_{min}, \ldots, c_{max}, \tag{4.9}$$

namely,

$$\boldsymbol{C}_{opt} = \underset{\left\{\hat{\boldsymbol{c}}_{n,m}^{(\ell)}\right\}}{\arg\min}\, \mathbb{E}\left[\boldsymbol{e}_\ell^H \boldsymbol{e}_\ell\right], \tag{4.10}$$

which corresponds to the problem stated in (4.3) under the assumption that $\{\boldsymbol{x}_\ell\}_{opt}$ can be written as a linear combination of the signal $\{\boldsymbol{z}_\ell\}$.

4.2.1 Computation of the Square Error

In order to express the MSE as a function the filter $\boldsymbol{C}$ coefficients, the first step is to calculate the square of the error signal $\boldsymbol{e}_\ell$. Using the its definition (4.2) we obtain the squared signal

$$\boldsymbol{e}_\ell^H \boldsymbol{e}_\ell = \boldsymbol{y}_\ell^H \boldsymbol{y}_\ell - \boldsymbol{y}_\ell^H \boldsymbol{d}_\ell - \boldsymbol{d}_\ell^H \boldsymbol{y}_\ell + \boldsymbol{d}_\ell^H \boldsymbol{d}_\ell. \tag{4.11}$$

We now expand each term separately. For first term we get:

$$\begin{aligned} \boldsymbol{y}_\ell^H \boldsymbol{y}_\ell &= \left(\alpha \sum_{\ell_1} \sum_{p_1} \boldsymbol{z}_{p_1}^H \boldsymbol{C}_{\ell_1-p_1}^H \hat{\boldsymbol{H}}_{\ell-\ell_1}^H\right) \left(\alpha \sum_{\ell_2} \sum_{p_2} \hat{\boldsymbol{H}}_{\ell-\ell_2} \boldsymbol{C}_{\ell_2-p_2} \boldsymbol{z}_{p_2}\right) \\ &= \alpha^2 \sum_{p_1} \sum_{p_2} \boldsymbol{z}_{p_1}^H \sum_{\ell_1} \sum_{\ell_2} \boldsymbol{C}_{\ell_1-p_1}^H \hat{\boldsymbol{H}}_{\ell-\ell_1}^H \hat{\boldsymbol{H}}_{\ell-\ell_2} \boldsymbol{C}_{\ell_2-p_2} \\ &= \alpha^2 \sum_{p_1} \sum_{p_2} \boldsymbol{z}_{p_1}^H \underbrace{\sum_{q_1} \sum_{q_2} \boldsymbol{C}_{\ell-p_1-q_1}^H \hat{\boldsymbol{H}}_{q_1}^H \hat{\boldsymbol{H}}_{q_2} \boldsymbol{C}_{\ell-p_2-q_2}}_{\boldsymbol{B}^{(\ell-p_1,\ell-p_2)}} \boldsymbol{z}_{p_2}, \end{aligned} \tag{4.12}$$

note that in the last passage the indices of the summations have been changed, $q_1 = \ell - \ell_1$ and $q_2 = \ell - \ell_2$. On the second term we obtain:

$$\begin{aligned} \boldsymbol{y}_k^H \boldsymbol{d}_k &= \left(\alpha \sum_{\ell} \sum_{p} \boldsymbol{z}_p^H \boldsymbol{C}_{\ell-p}^H \hat{\boldsymbol{H}}_{k-\ell}^H \right) \left(\alpha \sum_{h} \boldsymbol{G}_{k-h} \boldsymbol{z}_h \right) \\ &= \alpha^2 \sum_{p} \sum_{h} \boldsymbol{z}_p^H \sum_{\ell} \boldsymbol{C}_{\ell-p}^H \hat{\boldsymbol{H}}_{k-\ell}^H \boldsymbol{G}_{k-h} \\ &= \alpha^2 \sum_{p} \sum_{h} \boldsymbol{z}_p^H \underbrace{\sum_{q} \boldsymbol{C}_{k-p-q}^H \hat{\boldsymbol{H}}_q^H \boldsymbol{G}_{k-h}}_{\boldsymbol{D}^{(k-p,k-h)}} \boldsymbol{z}_h, \end{aligned} \tag{4.13}$$

where $q = k - \ell$ ($\ell = k - q$). Similarly, for the third one:

$$\begin{aligned} \boldsymbol{d}_k^H \boldsymbol{y}_k &= \left(\alpha \sum_{h} \boldsymbol{z}_h^H \boldsymbol{G}_{k-h}^H \right) \left(\alpha \sum_{\ell} \sum_{p} \hat{\boldsymbol{H}}_{k-\ell} \boldsymbol{C}_{\ell-p} \boldsymbol{z}_p \right) \\ &= \alpha^2 \sum_{h} \sum_{p} \boldsymbol{z}_h^H \sum_{\ell} \boldsymbol{G}_{k-h}^H \hat{\boldsymbol{H}}_{k-\ell} \boldsymbol{C}_{\ell-p} \\ &= \alpha^2 \sum_{h} \sum_{p} \boldsymbol{z}_h^H \underbrace{\sum_{q} \boldsymbol{G}_{k-h}^H \hat{\boldsymbol{H}}_q \boldsymbol{C}_{k-p-q}}_{\boldsymbol{E}^{(k-h,k-p)}} \boldsymbol{z}_p. \end{aligned} \tag{4.14}$$

Notice by inspection that $\boldsymbol{E}^{(a,b)} = \boldsymbol{D}^{(a,b)H}$. For the last term we get:

$$\begin{aligned} \boldsymbol{d}_k^H \boldsymbol{d}_k &= \left(\alpha \sum_{h_1} \boldsymbol{z}_{h_1}^H \boldsymbol{G}_{k-h_1}^H \right) \left(\alpha \sum_{h_2} \boldsymbol{G}_{k-h_2} \boldsymbol{z}_{h_2} \right) \\ &= \alpha^2 \sum_{h_1} \sum_{h_2} \boldsymbol{z}_{h_1}^H \underbrace{\boldsymbol{G}_{k-h_1}^H \boldsymbol{G}_{k-h_2}}_{\boldsymbol{F}^{(k-h_1,k-h_2)}} \boldsymbol{z}_{h_2}, \end{aligned} \tag{4.15}$$

and therefore by summing all the terms, we obtain the following simplified expression:

$$\begin{aligned} \frac{\boldsymbol{e}_k^H \boldsymbol{e}_k}{\alpha^2} &= \sum_{p_1} \sum_{p_2} \boldsymbol{z}_{p_1}^H \boldsymbol{B}^{(k-p_1,k-p_2)} \boldsymbol{z}_{p_2} - \sum_{p} \sum_{h} \boldsymbol{z}_p^H \boldsymbol{D}^{(k-p,k-h)} \boldsymbol{z}_h \\ &- \sum_{p} \sum_{h} \boldsymbol{z}_h^H \boldsymbol{D}^{(k-p,k-h)H} \boldsymbol{z}_p + \sum_{h_1}^{k-g_{min}} \sum_{h_2} \boldsymbol{z}_{h_1}^H \boldsymbol{F}^{(k-h_1,k-h_2)} \boldsymbol{z}_{h_2}. \end{aligned} \tag{4.16}$$

4.2.2 Properties of the Satellites' Signal

In order to calculate the expectation of the previously computed squared error, we need to consider some important properties of the signal $\boldsymbol{z}_\ell$ that simplify the calculation. We have that:

- as described in (3.13) $\boldsymbol{z}_\ell = \mathbf{0}$ for $\ell \neq k\kappa$, whereas on other samples they are equal $\boldsymbol{z}_\ell = \kappa \boldsymbol{c}_k$ unless for a multiplicative factor

$$\mathbb{E}\left[\boldsymbol{z}_\ell\right] = \mathbb{E}\left[\boldsymbol{c}_k\right] = \mathbf{0}; \tag{4.17}$$

- row elements that compose $\boldsymbol{c}_k$ are orthogonal for two different satellites:

$$\mathbb{E}\left[c^*_{k,p} c_{k,q}\right] = \begin{cases} 1 & p = q, \\ 0 & p \neq q \end{cases} \quad \Rightarrow \quad \mathbb{E}\left[z^*_{\ell,p} z_{\ell,q}\right] = \begin{cases} \kappa^2 & p = q, \\ 0 & p \neq q; \end{cases} \tag{4.18}$$

- there is no temporal correlation on the PRN codes:

$$\begin{aligned} \mathbb{E}\left[\boldsymbol{c}^H_{k_1} \boldsymbol{c}_{k_2}\right] &= \begin{cases} N_s & k_1 = k_2, \\ 0 & k_1 \neq k_2 \end{cases} \\ \Rightarrow \quad \mathbb{E}\left[\boldsymbol{z}^H_{\ell_1} \boldsymbol{z}_{\ell_2}\right] &= \begin{cases} \kappa^2 N_s & \ell_1 = \kappa k = \ell_2, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{4.19}$$

  Notice that the above writings are not so rigorous, in fact the PRN codes are periodic, thus the above properties are correct for $|\ell_2 - \ell_1| < N_c$.

Let us define the following scalar quantity with respect to the generic matrix $\boldsymbol{Q}^{(\ell_1,\ell_2)}$ that depends on ℓ_1 and ℓ_2:

$$q\left(\boldsymbol{z}_{\ell_1}, \boldsymbol{z}_{\ell_2}, \ell_1, \ell_2\right) = \boldsymbol{z}^H_{\ell_1} \boldsymbol{Q}^{(\ell_1,\ell_2)} \boldsymbol{z}_{\ell_2} = \sum_{i=0}^{N_s-1} \sum_{j=0}^{N_s-1} q^{(\ell_1,\ell_2)}_{ij} z^*_{\ell_1,i} z_{\ell_2,j}. \tag{4.20}$$

Then if we calculate the expected value of that quantity, by using the previous properties we obtain:

$$\begin{aligned} \mathbb{E}\left[\boldsymbol{z}^H_{\ell_1} \boldsymbol{Q}^{(\ell_1,\ell_2)} \boldsymbol{z}_{\ell_2}\right] &= \sum_{i=0}^{N_s-1} \sum_{j=0}^{N_s-1} q^{(\ell_1,\ell_2)}_{ij} \mathbb{E}\left[z^*_{\ell_1,i} z_{\ell_2,j}\right] = \\ &= \kappa^2 \sum_{i=0}^{N_s-1} q^{(\ell_1,\ell_2)}_{ii} \delta_{\ell_1-\ell_2} = \begin{cases} \kappa^2 \operatorname{tr}(\boldsymbol{Q}) & \ell_1 = \ell_2, \\ 0 & \ell_1 \neq \ell_2. \end{cases} \end{aligned} \tag{4.21}$$

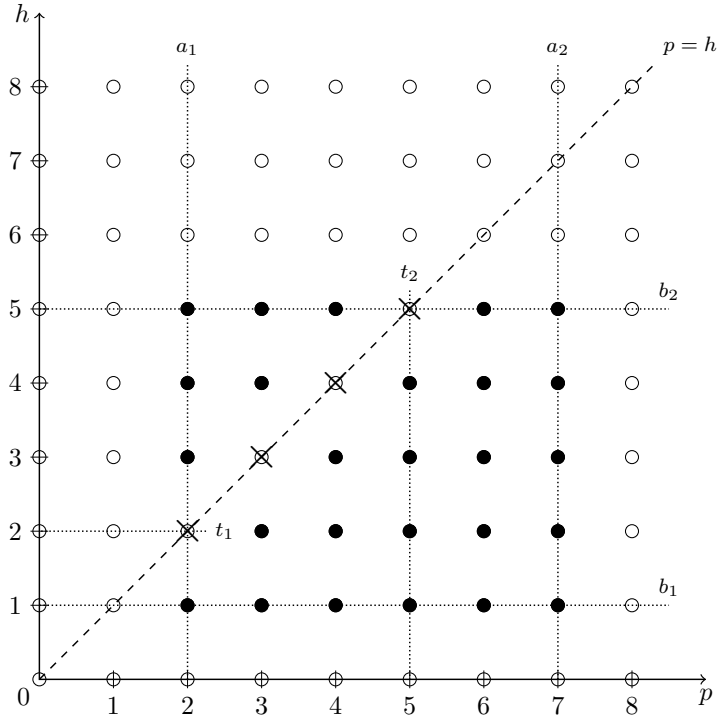


Figure 4.2: Example of map grid and the effect of periodic PRN on the received signal.

Consider the following a double summation of the expectation terms, we get the following:

$$\sum_{p=a_1}^{a_2} \sum_{h=b_1}^{b_2} \mathbb{E}\left[\boldsymbol{z}_p^H \boldsymbol{Q}^{(p,h)} \boldsymbol{z}_h\right] = \kappa^2 \sum_{p=t_1}^{t_2} \mathrm{tr}\left(\boldsymbol{Q}^{(p,p)}\right). \tag{4.22}$$

In order to clarify (4.22), let us represent the left side summation terms as the grid depicted in Fig. 4.2. The points represent all the possible terms for a double summation whereas the filled ones are the terms which are inside the summation boundaries $a_1 \leq p \leq a_2$ and $b_1 \leq h \leq b_2$. Among the terms contained in the resulting rectangle, only the ones which lie in the dashed line (namely $p = h$) are non-null. The remaining terms to be summed (cross markers), can thus be represented as a single summation with index $t_1 \leq p \leq t_2$. Note that, in general, the intersection between the rectangle and the dashed line might be empty. Therefore, by using (4.21) and the above reasoning, we obtain the right side of (4.22).

4.2.3 Mean Square Error

If we exploit the properties obtained in the previous Section rhe computation of for the expectation of (4.16) become easier. The first step is to perform a substitution of the summation indices moving the variable ℓ to the signal $\boldsymbol{z}$:

$$\begin{aligned}\frac{\boldsymbol{e}_k^H \boldsymbol{e}_k}{\alpha^2} = &\sum_{p_1}\sum_{p_2} \boldsymbol{z}_{k-p_1}^H \boldsymbol{B}^{(p_1,p_2)} \boldsymbol{z}_{k-p_2} - \sum_{p}\sum_{h} \boldsymbol{z}_{k-p}^H \boldsymbol{D}^{(p,h)} \boldsymbol{z}_{k-h} \\ &- \sum_{p}\sum_{h} \boldsymbol{z}_{k-h}^H \boldsymbol{D}^{(p,h)H} \boldsymbol{z}_{k-p} + \sum_{h_1}^{k-g_{min}} \sum_{h_2} \boldsymbol{z}_{k-h_1}^H \boldsymbol{F}^{(h_1,h_2)} \boldsymbol{z}_{k-h_2}.\end{aligned} \tag{4.23}$$

If we calculate the expected value for the quantity $\boldsymbol{e}_k^H \boldsymbol{e}_k$ we get:

$$\begin{aligned}\frac{1}{\alpha^2}\mathbb{E}\left[\boldsymbol{e}_k^H \boldsymbol{e}_k\right] &= \sum_{p_1}\sum_{p_2} \mathbb{E}\left[\boldsymbol{z}_{k-p_1}^H \boldsymbol{B}^{(p_1,p_2)} \boldsymbol{z}_{k-p_2}\right] + \sum_{h_1}\sum_{h_2} \mathbb{E}\left[\boldsymbol{z}_{k-h_1}^H \boldsymbol{F}^{(h_1,h_2)} \boldsymbol{z}_{k-h_2}\right] \\ &- \sum_{p}\sum_{h} \left(\mathbb{E}\left[\boldsymbol{z}_{k-p}^H \boldsymbol{D}^{(p,h)} \boldsymbol{z}_{k-h}\right] + \mathbb{E}\left[\boldsymbol{z}_{k-h}^H \boldsymbol{D}^{(p,h)H} \boldsymbol{z}_{k-p}\right]\right) \\ &= \kappa^2 \sum_{p} \mathrm{tr}\left(\boldsymbol{B}^{(p,p)}\right) + \kappa^2 \sum_{h} \mathrm{tr}\left(\boldsymbol{F}^{(h,h)}\right) \\ &- \kappa^2 \sum_{p} \left(\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right) + \mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)\right).\end{aligned} \tag{4.24}$$

Expanding the traces expressions we can exploit the linearity of the trace operator:

$$\begin{aligned}\mathrm{tr}\left(\boldsymbol{B}^{(p,p)}\right) &= \sum_{q_1}\sum_{q_2} \mathrm{tr}\left(\boldsymbol{C}_{p-q_1}^H \hat{\boldsymbol{H}}_{q_1}^H \hat{\boldsymbol{H}}_{q_2} \boldsymbol{C}_{p-q_2}\right) \\ \mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right) &= \sum_{q} \mathrm{tr}\left(\boldsymbol{C}_{p-q}^H \hat{\boldsymbol{H}}_{q}^H \boldsymbol{G}_p\right) \\ \mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right) &= \sum_{q} \mathrm{tr}\left(\boldsymbol{G}_p^H \hat{\boldsymbol{H}}_{q} \boldsymbol{C}_{p-q}\right) \\ \mathrm{tr}\left(\boldsymbol{F}^{(h,h)}\right) &= \mathrm{tr}\left(\boldsymbol{G}_h^H \boldsymbol{G}_h\right).\end{aligned} \tag{4.25}$$

The final expression for the MSE functional is written as a function of the filter $\boldsymbol{C}$.

4.2.4 Minimization of the MSE Functional

We now compute the minimum of (4.24) with respect to $\boldsymbol{C}_h \in \mathbb{C}^{N_a \times N_s}$. Therefore the aim of this section is to seek stationary points of that real-valued function of complex variable. The easiest way to solve this complex differentiability problem is to formulate the problem in terms of real variables [21]. Note that (4.24) is a sum of several terms, and we cannot ensure that is a convex function, thus local minimum may not corresponds to global minimum. The unknown filter's coefficients $\boldsymbol{C}_\ell$ are therefore separated to split the problem on $N_a N_s L_c$ complex variables into $2N_a N_s L_c$ real ones by defining:

$$\boldsymbol{C}_h = \boldsymbol{C}_{h,I} + \mathrm{i}\,\boldsymbol{C}_{h,Q} \quad \forall h. \tag{4.26}$$

The matrix calculus to obtain the derivative of $J = \mathbb{E}\left[\boldsymbol{e}_k^H \boldsymbol{e}_k\right]$ as function of $\boldsymbol{C}_h$ are described in Appendix B. Collecting all the resulting terms we obtain:

$$\frac{\partial J}{\partial \boldsymbol{C}_h} = 2\alpha^2\kappa^2 \sum_p \sum_q \hat{\boldsymbol{H}}_{p-h}^H \hat{\boldsymbol{H}}_q \boldsymbol{C}_{p-q} - 2\alpha^2\kappa^2 \sum_p \hat{\boldsymbol{H}}_{p-h}^H \boldsymbol{G}_p, \tag{4.27}$$

and therefore, in order to find the local minimum of J, we impose the previous expression to be null:

$$\frac{\partial J}{\partial \boldsymbol{C}_h} = \boldsymbol{0} \quad \Rightarrow \quad \sum_p \sum_q \hat{\boldsymbol{H}}_{p-h}^H \hat{\boldsymbol{H}}_q \boldsymbol{C}_{p-q} = \sum_p \hat{\boldsymbol{H}}_{p-h}^H \boldsymbol{G}_p = \boldsymbol{W}_h \in \mathbb{C}^{N_a \times N_s}. \tag{4.28}$$

Albeit all the above summations goes from $-\infty$ to $+\infty$, most of the term are null since all the involved filters have FIR. Regarding the right side, the set of indices p where terms of the summation are non-null is:

$$p \in \mathcal{G}(h) \subset \mathbb{Z} : \begin{cases} g_{min} \leq p \leq g_{max} & \text{due to } \boldsymbol{G}_p, \\ h + h_{min} \leq p \leq h + h_{max} & \text{due to } \hat{\boldsymbol{H}}_{p-h}^H, \end{cases} \tag{4.29}$$

whereas for the left side the corresponding sets are:

$$\begin{aligned} q \in \mathcal{T}(p) \subset \mathbb{Z} : & \begin{cases} h_{min} \leq q \leq h_{max} & \text{due to } \hat{\boldsymbol{H}}_p, \\ p - c_{max} \leq q \leq p - c_{min} & \text{due to } \boldsymbol{C}_{p-q} \end{cases} \\ p \in \mathcal{P}(h) \subset \mathbb{Z} : & \; h + h_{min} \leq p \leq h + h_{max}. \end{aligned} \tag{4.30}$$

Note that all these sets depend on the value of h.

4.2.5 Optimum Filter

Using the results of the previous Section 4.2.4, we found the expression to minimize the MSE as function of $\boldsymbol{C}_h$. However since the filter $\boldsymbol{C}$ has L_c taps,

to find the optimum coefficients for our problem we should impose the above for all its terms:

$$\boldsymbol{C}_{opt} : \nabla_{\boldsymbol{C}} J = \boldsymbol{0} \quad \Leftrightarrow \quad \frac{\partial J}{\partial \boldsymbol{C}_{c_{min}}} = \cdots = \frac{\partial J}{\partial \boldsymbol{C}_{c_{max}}} = \boldsymbol{0}, \tag{4.31}$$

corresponding to the following system of matrix equations:

$$\boldsymbol{C}_{opt} : \begin{cases} \sum_p \sum_q \hat{\boldsymbol{H}}^H_{p-c_{min}} \hat{\boldsymbol{H}}_q \boldsymbol{C}_{p-q} = \boldsymbol{W}_{c_{min}}, \\ \qquad \vdots \\ \sum_p \sum_q \hat{\boldsymbol{H}}^H_{p-h} \hat{\boldsymbol{H}}_q \boldsymbol{C}_{p-q} = \boldsymbol{W}_h, \\ \qquad \vdots \\ \sum_p \sum_q \hat{\boldsymbol{H}}^H_{p-c_{max}} \hat{\boldsymbol{H}}_q \boldsymbol{C}_{p-q} = \boldsymbol{W}_{c_{max}}. \end{cases} \tag{4.32}$$

In order to find the solution $\boldsymbol{C}_{opt}$, the problem is rearranged to express the above equations as an explicit linear system $\boldsymbol{A}\boldsymbol{C}^\star = \boldsymbol{W}^\star$. Let us define the following block matrices:

$$\boldsymbol{C}^\star = \begin{bmatrix} \boldsymbol{C}_{c_{min}} \\ \vdots \\ \boldsymbol{C}_{c_{max}} \end{bmatrix} \in \mathbb{C}^{L_c N_a \times N_s} \qquad \boldsymbol{W}^\star = \begin{bmatrix} \boldsymbol{W}_{c_{min}} \\ \vdots \\ \boldsymbol{W}_{c_{max}} \end{bmatrix} \in \mathbb{C}^{L_c N_a \times N_s} \tag{4.33}$$

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_{1,1} & \boldsymbol{A}_{1,2} & \dots & \boldsymbol{A}_{1,L_c} \\ \boldsymbol{A}_{2,1} & \boldsymbol{A}_{2,2} & \dots & \boldsymbol{A}_{2,L_c} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{A}_{L_c,1} & \boldsymbol{A}_{L_c,2} & \dots & \boldsymbol{A}_{L_c,L_c} \end{bmatrix} \in \mathbb{C}^{L_c N_a \times L_c N_a}, \tag{4.34}$$

where the blocks of $\boldsymbol{A}$ are defined as:

$$\boldsymbol{A}_{h,\ell} = \sum_p \hat{\boldsymbol{H}}^H_{p-h} \hat{\boldsymbol{H}}_{p-\ell} \in \mathbb{C}^{N_a \times N_a}. \tag{4.35}$$

Then using the above matrices we can express the problem ad a classic linear system whose solution is:

$$\boldsymbol{C}^\star = \boldsymbol{A}^{-1} \boldsymbol{W}^\star. \tag{4.36}$$

Thereby $\boldsymbol{C}^\star$ can be reshaped to obtain the elements of $\boldsymbol{C}_{opt}$, solution for the problem in (4.10).

4.3 Sub-optimal LS Iterative Method

An alternative approach to obtain the signal $\boldsymbol{x}_\ell$ is described in this section. In this method we do not consider the space channel, but only the target spoofing signal.
The idea is to find an initial solution for $\ell = \ell_0$ and then track the evolution of $\boldsymbol{d}_k$. First of all let us define an equivalent matrix formulation for the ground channel in (3.21):

$$\begin{aligned} \boldsymbol{y}_\ell &= \sum_{h=h_{min}}^{h_{max}} \hat{\boldsymbol{H}}_h \boldsymbol{x}_{\ell-h} = \bar{\boldsymbol{H}} \bar{\boldsymbol{x}}_\ell \\ \text{where: } \bar{\boldsymbol{H}} &= \left[\hat{\boldsymbol{H}}_{h_{min}}, \ldots, \hat{\boldsymbol{H}}_{h_{max}} \right] \in \mathbb{C}^{N_p \times N_a L_h} \\ \bar{\boldsymbol{x}}_\ell &= \left[\boldsymbol{x}_{\ell-h_{min}}^T, \ldots, \boldsymbol{x}_{\ell-h_{max}}^T \right]^T \in \mathbb{C}^{N_a L_h \times 1}. \end{aligned} \tag{4.37}$$

Then the steps of this method are:

1. Find the initial solution of

$$\boldsymbol{d}_{\ell_0} = \bar{\boldsymbol{H}} \bar{\boldsymbol{x}}_{\ell_0} + \boldsymbol{e}_{\ell_0}, \tag{4.38}$$

than minimizes the square of the error $\boldsymbol{e}_{\ell_0}$, providing

$$\hat{\boldsymbol{x}}_{start} = \left(\bar{\boldsymbol{H}}^H \bar{\boldsymbol{H}} \right)^{-1} \bar{\boldsymbol{H}} \boldsymbol{d}_{\ell_0}, \tag{4.39}$$

hence, a solution for the initial conditions $\hat{\boldsymbol{x}}_{\ell_0-h_{min}}, \ldots \hat{\boldsymbol{x}}_{\ell_0-h_{max}}$ is obtained. Note that for $\ell < \ell_0$ there is a transitory effect and $\hat{\boldsymbol{y}}_\ell$ will differ from the target $\boldsymbol{d}_\ell$.

2. For $\ell = \ell_0 + 1$ we have

$$\boldsymbol{d}_\ell - \sum_{h=h_{min}+1}^{h_{max}} \hat{\boldsymbol{H}}_h \hat{\boldsymbol{x}}_{\ell-h} = \boldsymbol{e}_\ell + \hat{\boldsymbol{H}}_{h_{min}} \boldsymbol{x}_{\ell-h_{min}}, \tag{4.40}$$

where the left side of the equation is know. Therefore we find for a solution for the unknown vector $\boldsymbol{x}_{\ell-h_{min}}$ using the LS approach that minimizes the square of the error $\boldsymbol{e}_\ell$:

$$\hat{\boldsymbol{x}}_{\ell-h_{min}} = \left(\hat{\boldsymbol{H}}_{h_{min}}^H \hat{\boldsymbol{H}}_{h_{min}} \right)^{-1} \hat{\boldsymbol{H}}_{h_{min}} \left(\boldsymbol{d}_\ell - \sum_{h=h_{min}+1}^{h_{max}} \hat{\boldsymbol{H}}_h \hat{\boldsymbol{x}}_{\ell-h} \right). \tag{4.41}$$

3. Repeat the step 2 for $\ell = \ell_0 + 2, \ell_0 + 3, \ldots$ until the norm of the error $\boldsymbol{e}_\ell$ does not exceed a threshold β and then start again from step 1.

Step 3 is important because step 2 appears to accumulate error in some cases. Note that this method does not ensure the minimization of MSE, however as we will se in Chapter 5 it is a valid alternative of the method presented in 4.2, and in some cases, it has a lower complexity.

Chapter 5

Simulations and Results

In this chapter, we summarize the performance obtained for the spatial spoofing attack by using the methods presented in Chapter 4 . The parameters that mostly affect the results will be commented, and their impact on the final positioning estimation will be outlined.

5.1 Reconstruction Performance

Both proposed solutions aim at minimizing the reconstruction error $\boldsymbol{e}_\ell$. Let $P_{\boldsymbol{d}}^{(j)}$ and $P_{\boldsymbol{e}}^{(j)}$ be the power of the signals $\boldsymbol{d}_\ell$ and $\boldsymbol{e}_\ell$ respectively, in the j-th points of the grid. In order to evaluate the reconstruction performance we define signal to error ratio (SER), associated to the j-th point, as

$$\mathrm{SER}^{(j)} = \frac{P_{\boldsymbol{d}}^{(j)}}{P_{\boldsymbol{e}}^{(j)}}. \tag{5.1}$$

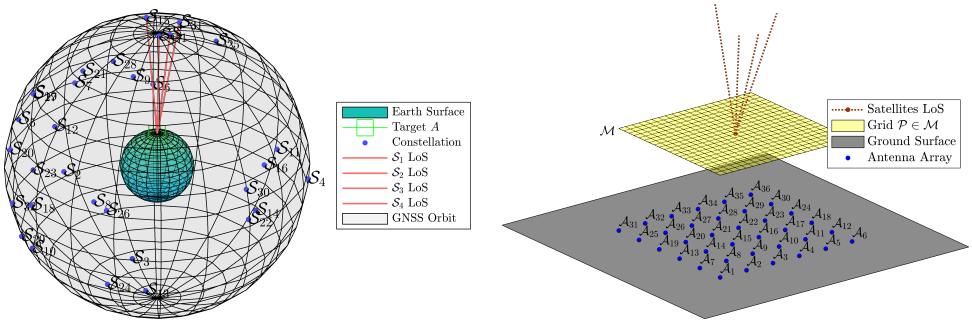
Another useful metric is the *overall* SER [1] in the grid, defined as

$$\mathrm{SER} = \frac{P_{\boldsymbol{d}}}{P_{\boldsymbol{e}}} = \frac{\mathbb{E}\left[\boldsymbol{d}_k^H \boldsymbol{d}_k\right]}{\mathbb{E}\left[\boldsymbol{e}_k^H \boldsymbol{e}_k\right]}. \tag{5.2}$$

The analytic expression of $\mathbb{E}\left[\boldsymbol{d}_k^H \boldsymbol{d}_k\right]$ is:

$$P_{\boldsymbol{d}} = \mathbb{E}\left[\boldsymbol{d}_k^H \boldsymbol{d}_k\right] = \alpha^2 \kappa^2 \sum_{h=g_{min}}^{g_{min}} \mathrm{tr}\left(\boldsymbol{G}_h^H \boldsymbol{G}_h\right), \tag{5.3}$$

[1] Note that the overal SER is not the average value $\frac{1}{N_p}\sum_j \mathrm{SER}^{(j)}$ but the ratio between the two expected values $\mathbb{E}\left[\boldsymbol{d}_k^H \boldsymbol{d}_k\right]$ and $\mathbb{E}\left[\boldsymbol{e}_k^H \boldsymbol{e}_k\right]$.



(a) *Emulation of the GNSS constellation. Target Location A: North Pole.*

(b) *Representation of the scenario at Location B: Anywhere in the world.*

Figure 5.1: Emulation of the spatial spoofing scenario through the use our simulator.

whereas $\mathbb{E}\left[\boldsymbol{e}_k^H \boldsymbol{e}_k\right]$ can be obtained as in Section 4.2.3. Note that when we use the iterative method, it is not possible to get an analytic expression and numerical estimations should be used. Moreover, another metric that can be used to characterize the performance is the minimum among the SER on the grid, namely:

$$\mathrm{SER}^{(\min)} = \min_{j \in \{0,\dots,N_p-1\}} \mathrm{SER}^{(j)} \,. \tag{5.4}$$

For each of the defined metric, the subscript dB indicates that the quantity is expressed in Decibel. Clearly the SER takes inspiration from the classic signal to noise ratio (SNR) whereas instead considering signals corrupted by noise we evaluate the reconstruction noise that affect the output $\boldsymbol{y}_\ell$.

5.1.1 Simulation Framework

In order to simulate the attack a MATLAB® simulator has been built. The simulator follows the procedure presented in Section 4.1 to generate the environment required for the simulation. We chose to simulate the most basic *L1 C/A Signal* of the GPS, hence all the GNSS parameters were set accordingly. The emulation of the GNSS is achieved by placing uniformly the satellites on the medium earth orbit (MEO) at 20180 km from the earth surface. More advanced descriptions of the constellation, which take into account real GNSS orbits, are postponed to future versions of the simulator. Among the 32 satellites of the constellation, only the nearest N_s satellites from the target location are considered to produce the target signal.
In Fig. 5.1 the emulated constellation and the map under attack are shown for $N_a = 36$, $N_s = 4$ and map side 40 m long. The corresponding spoofed

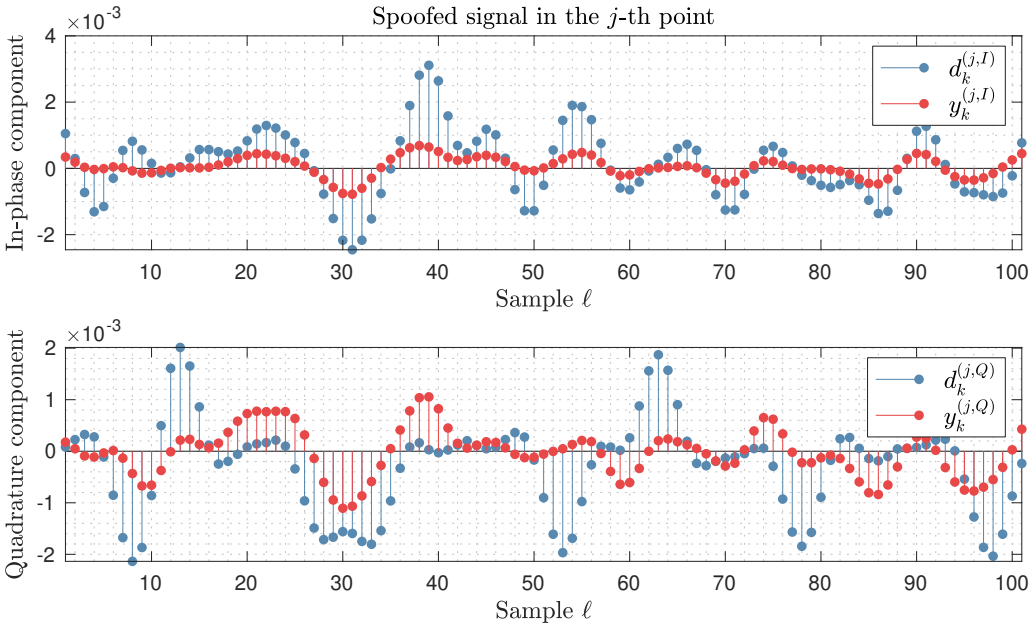


Figure 5.2: Qualitative comparison between the target $d_\ell^{(j)}$ and the spoofed signal $y_\ell^{(j)}$.

signal, observed at $j = 1$ where $\mathrm{SER}^{(j)} = 2.1438\,\mathrm{dB}$, can be qualitatively compared with the target signal in Fig. 5.2.

5.1.2 Number of Antennas and Satellites

The parameters which affect the reconstruction performance are numerous. We start considering the impact of the parameter N_a. Note that number of antennas is a fundamental parameter from the attacker's point of view, since he must estimate the resources he needs. Another important parameter is the number of satellites we would like to spoof. Albeit orthogonality among satellites in ensured by PRN sequences, the bigger N_s, the more signals overlap in $\boldsymbol{d}_k$ making the target signal more complex. To evaluate the results for the SER metrics as a function the aforementioned parameters, we simulated the combinations of the two parameters using the configuration described in Tab. 5.1. Each combination have been averaged by randomly changing the GNSS constellation for $K = 100$ times. In Fig. 5.3 the results are reported. The first observation is that for a low number of antennas, the $\mathrm{SER}_{\mathrm{dB}}$ goes to 0. This behavior comes from the criterion used to carry out the attack, in fact, when the resources are insufficient to replicate $\boldsymbol{d}_k$ on the map, the best way to minimize the MSE over the grid is to reduce the amplitude of

Parameters	Value
Grid points N_p	900
Map $\mathcal{M}$ size	40×40 m^2
Grid step-size δ	1.3793 m
Observation time Δt	1 ms
Oversampling factor κ	3
Map height h	50 m

Table 5.1: Configuration A.

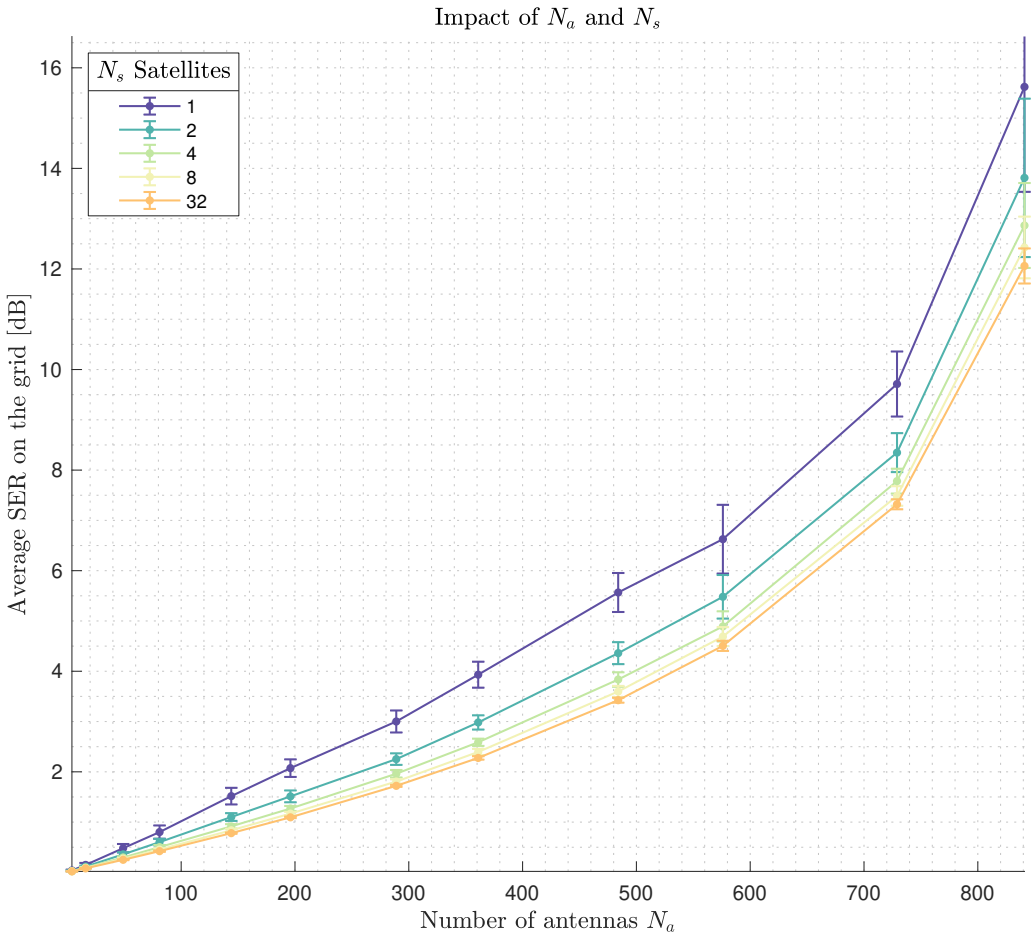


Figure 5.3: Average SER as a function of N_a for the configuration described in Table 5.1.

$\boldsymbol{x}_k$ until reaching the extreme case where $\boldsymbol{e}_k = \boldsymbol{d}_k$ and thus $\text{SER}_{\text{dB}} = 0\,\text{dB}$. The second observation regards the behavior of the growth. We note that in the first region the SER grows linearly with N_a , while for values of N_a close to N_p the increase is exponential. Another observation is that, for the considered configuration, N_s has a small impact the on the spoofing performance.
The last observation is about the SER values in absolute terms. Albeit their values might seem very low and the spoofed signal looks different from the target one (also for Fig. 5.2), note that the GNSS signals are quite robust to noise and they are designed on purpose. Typically, received signals are received well below the noise floor [12]. Note that since we are working on baseband signals, the reader should not confuse SNR with carrier to noise ratio (CNR) values that are commonly higher [22].

5.1.3 Memory Effect and Filter Length

The memory effect described in Section 3.3.1 is another key aspect we need to focus on. In this section we evaluate how the length of the ground channel filter, namely L_h, and the design parameter L_c of the filter $\boldsymbol{C}_{opt}$ are related. In Fig. 5.4 the results of a simulation are depicted, the simulated map is fixed whereas the oversampling rate κ is changed to increase L_h. The high variance of the results is due to the reduced number of points N_p to maintain

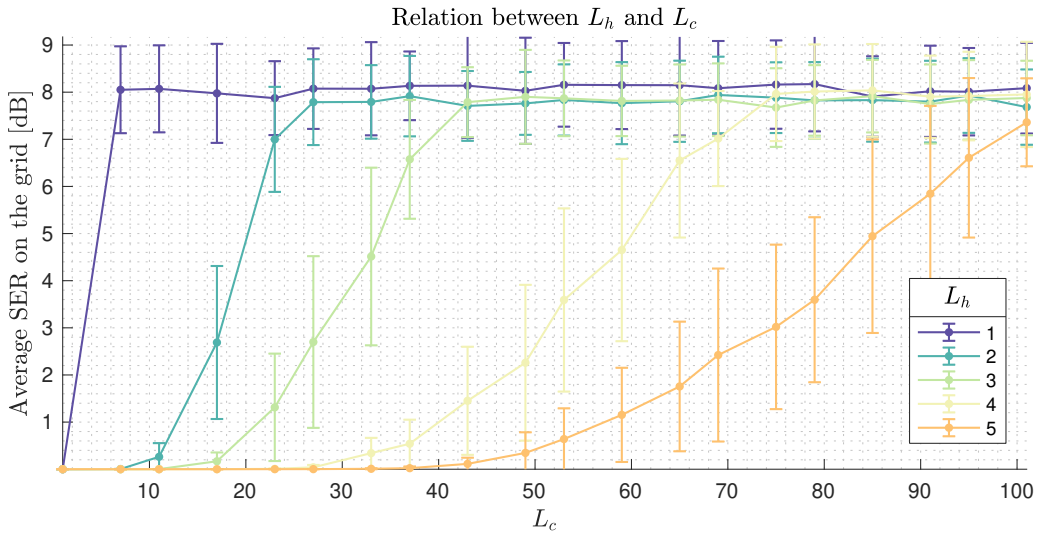


Figure 5.4: Relation between the memory effect on the map L_h and the length of the designed filter $\boldsymbol{C}_{opt}$.

the complexity low. As expected if L_h grows, L_c should be larger in order to achieve the same SER. Notice that once reached the required length for the filter, the SER saturates, making superfluous additional filter taps. Albeit polyphase implementation [18] for filters is used the computational complexity increases considerably with L_c, as can be seen in (4.37).

5.1.4 Grid Density and Map Properties

The results presented so far denote that to achieve good SER values, the number of antennas N_a should be close to N_p. In this section the stepsize of grid $\mathcal{M}$ will be discussed.
An appropriate value for the grid density, required to properly conduct the attack, is still an open question. It is not easy to predict how GNSS receivers, placed in the spoofed region may behave, because so many factors affect the tracking procedure. Our guess is that, if the grid density is not dense enough, the spoofing attack might overfit the target signal for the considered points, performing bad on external grid points. In order to face this issue, the stepsize δ should be decreased, however, notice that for a fixed map size N_p grows as the square of $1/\delta$, and requiring the condition $N_a \approx N_p$ may result too demanding.
However, we notice an interesting phenomenon. When the stepsize decreases, the signals received in the grid points become more correlated and this translates in local correlation between entries of the channel filters. More correlation among the filter coefficients reduces the rank of the matrices involved and thus less antennas are required to achieve high SER. Let λ be ratio between the number of antennas and the number of grid points, namely

$$\lambda = \frac{N_a}{N_p}. \tag{5.5}$$

To analyze λ and its relation with the stepsize δ, some tests have been conducted. In the first one, we fixed a map with side of 10 m and keeping fixed the λ ratio, we decreased the stepsize δ. The results are shown in Fig. 5.5 where we can clearly see that after a certain threshold, the continuity of the channel appears and the computed solutions perform better keeping fixed the ratio λ. Thus if we set the stepsize below the carrier wavelength λ_c, the condition $N_a \approx N_p$ is not mandatory anymore and we can save resources by using less antennas to achieve good results. Notice that working with $\delta < \lambda_c$ has an important consequence, since the number N_p grows rapidly as the size of the map increases and therefore the computational complexity may become prohibitive.

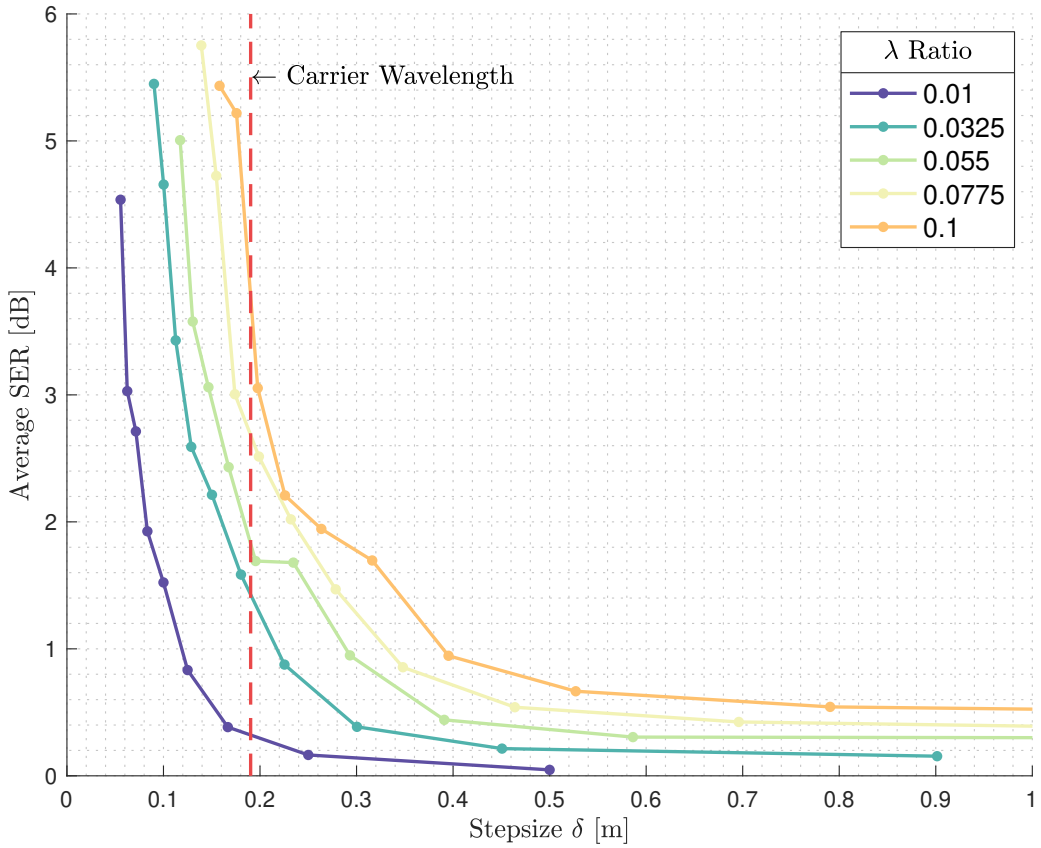


Figure 5.5: The occurrence of local correlation phenomenon as function of the stepsize.

A notable effect occurs at the border with lower values of SER. The performance over the map can vary a lot depending on the target locations we would like to spoof. An example of the the different performance is shown in Fig. 5.6 where using the same configurations for the region under attack on location B, two realizations are obtained from two different emulated constellations. In those examples there are $N_a = 64$ antennas, $N_s = 3$ satellites, the stepsize is $\delta = 0,02$ m, and the map side is 2 m long. As we can observe in the pictures, there are zones where we reach high $\text{SER}^{(j)}$ values and other ones where the spoofing performance is poor.

5.1.5 Suboptimal Method Comparison

In most of the cases, the SER values obtained by using the suboptimal iterative LS solution appears to be similar to the ones performed by the optimum solution. Albeit this occurs for most of the cases, sometimes the

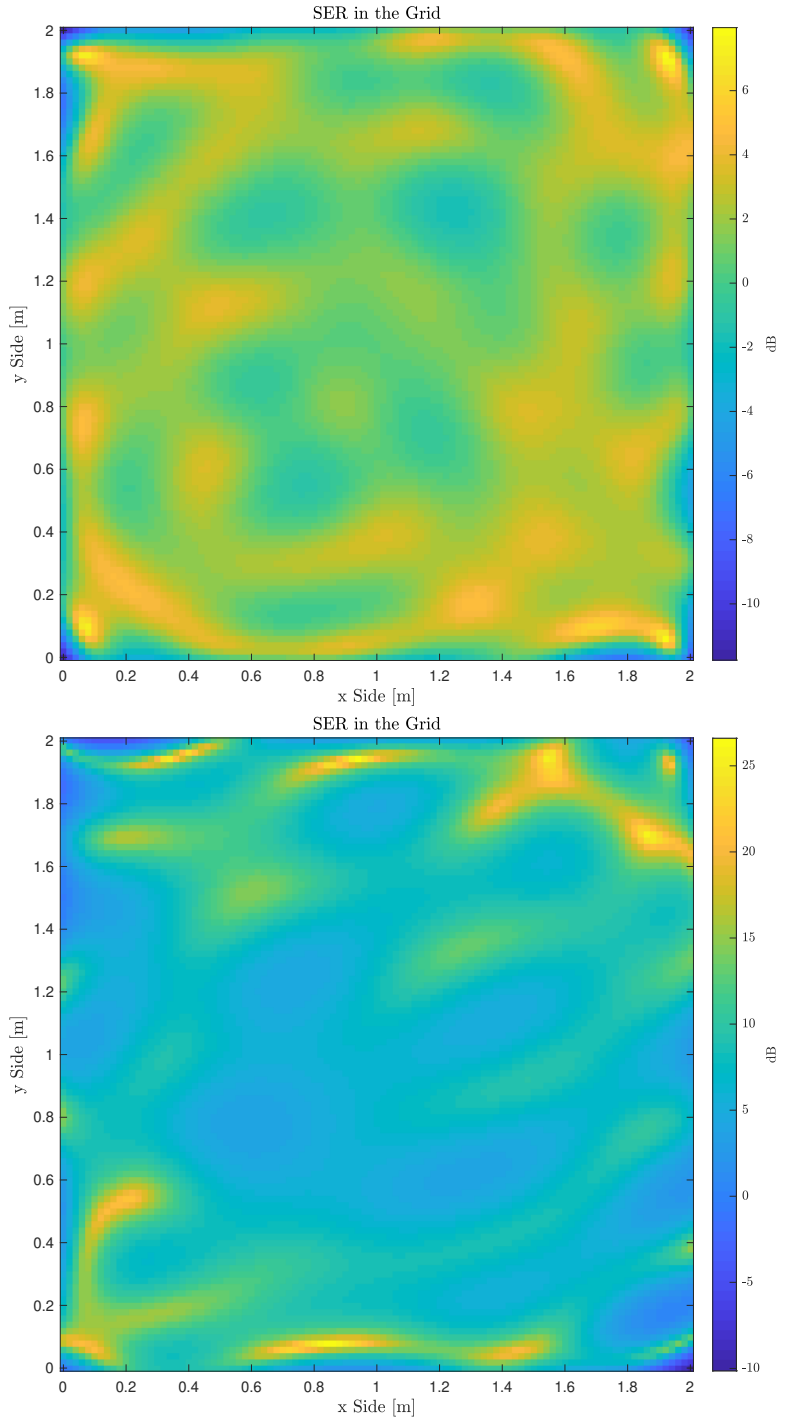


Figure 5.6: Example of SER distribution over the map for two different constellations.

iterative method quickly accumulates error over time, requiring the use of the method's third step (reinitialization step) too frequently to make the solution sustainable. Investigations about the factors that imply error accumulation are still going on.
As long as L_c is large enough to reach the performance saturation region seen in Section 5.1.3, the average SER is clearly better by using the optimum solution compared with the iterative one. Note that in the special case where the map is memoryless the two solutions are always equivalent, hence in this case, the use of the LS method is of course preferred for complexity purposes. In general, the suboptimal solution should preferably be adopted in cases where the required L_c would be too large, otherwise the Wiener approach always overcomes.

5.2 Satellites Acquisition Process

So far, the spoofing performance has been evaluated by using the SER metric, however, some questions arise to the point. Is the SER the right metric in the perspective of the GNSS field? Do receivers base their decision on the goodness of reconstructed signals? In general, not necessarily. As presented in Section 3.4, GNSS receivers use cross-correlation techniques to pull out the information they need to obtain pseudoranges. However, the relationship between SER and the quality of correlation metrics remains unclear.
Albeit the MSE minimization of $\boldsymbol{e}_\ell$ might not be the optimum formulation to perform the spoofing attack, and consequently it may prove a waste of effort, other criteria based on the preservation of correlation properties could lead to dead ends due to the complexity involved. If we cannot use other criteria to optimize the attack, at least we can evaluate correlation metrics to get an assessment about the performance, comparing them to the SER metrics.
The signal acquisition process performed by GNSS receivers can be simplified and reduced to the search for values $m^*_{i,j}$ which maximize the problem presented in (3.35). We use this basic approach to model the SPS positioning, allowing us to express the goodness of our spoofing in terms of inaccuracies committed during the code phase estimation. Namely, if $m_{i,j} \neq m^*_{i,j}$ then the estimation on the j-th point for the i-th pseudorange will be affected by an additional error of $c\left|m^*_{i,j} - m_{i,j}\right| T_s$ meters. Let us define the normalized local replica correlation (LRC) function for $y^{(j)}_\ell$ as:

$$\bar{R}^{(i,j)}_m = \left| \frac{R^{(i,j)}_m}{R^{(i,j)}_{m^*_{i,j}}} \right| \in [0,1]. \tag{5.6}$$

Note that LRC can be defined also for signals $\tilde{c}_\ell^{(i)}$, $d_\ell^{(j)}$ and $u_\ell^{(j)}$. In Fig. 5.7 we examine those signals by comparing their LRC for one realization under the configuration described in Tab. 5.2. Looking at one single point (e.g. $j = 500$) and using $M = \kappa N_c$ samples we compute the LRC for all the N_s spoofed satellites.
Considering $\tilde{c}_\ell^{(i)}$, we can see that its LRC has a triangle shape in accordance with the theoretical results for the BPSK modulation [1]. For the other signals, the LRC is smoother since interpolation/transmission filters reduce the signals bandwidth. In this example, 4 out of 6 satellites are correctly tracked (Sat2 and Sat5 are not correctly acquired) for $y_\ell^{(j)}$. Using the same configuration , we report in Fig. 5.8 the number of correctly acquired satellites over the map and the corresponding $\mathrm{SER}_{\mathrm{dB}}^{(j)}$ values. Albeit high SER values ensure the correct acquisition of all the satellites, this does not imply the opposite. For example in the right-down corner, the $\mathrm{SER}^{(j)}$ is below $-6\,\mathrm{dB}$ and surprisingly all the satellites are properly tracked. The explanation is clear by looking on the spoofed signal, in fact, all the properties of the signal are preserved and the only error comes from a wrong replication of residual carrier phase term, namely $e^{-\mathrm{i}\,2\pi f_c \tau_{k,j}^{(\mathcal{S})}}$, which highly affects the SER metrics but not the LRC function. In general, we note the lack of clear law that relates the SER and the quality of the LRC function.
The last simulation we performed is similar to the one did for Fig. 5.6, we investigated the number of correctly acquired satellites for several values of δ. The configuration adopted in the simulation is reported in Tab. 5.2 (configuration C). The results are reported in Fig. 5.9, where the empirical PDF for the number of acquired satellites distribution on the map is depicted. We note that as the stepsize decreases the distribution shift to the right side as expected from the previous results.
In conclusion, the presented phenomena make the evaluation of results very difficult, underling the necessity of more research on the subject to identify the factors that mainly affect the pseudorange estimation. Once all phenomena and parameters will be fully understood, it will be possible to improve our spatial spoofing attack accordingly.

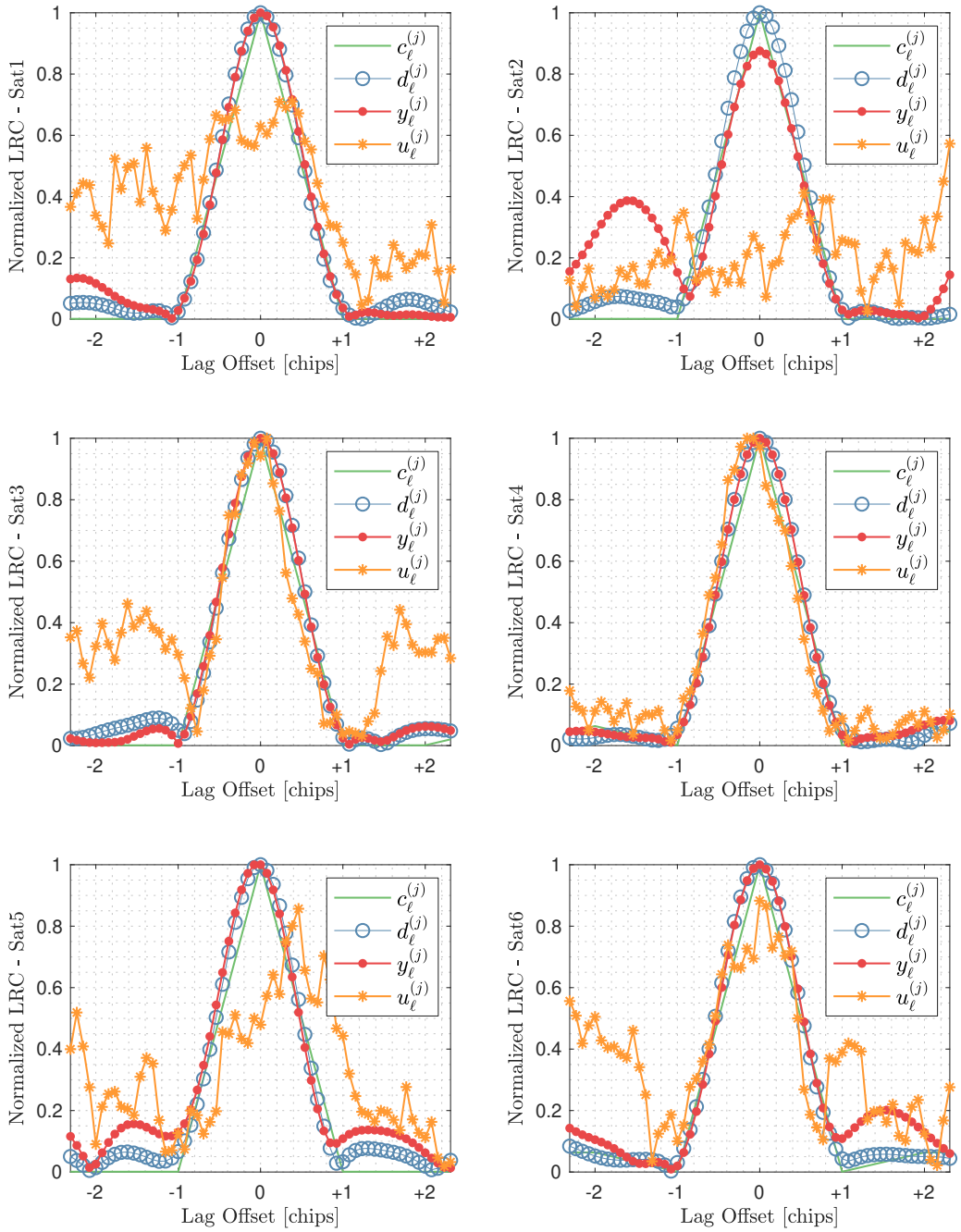


Figure 5.7: Comparison between LRC function for signals of interest.

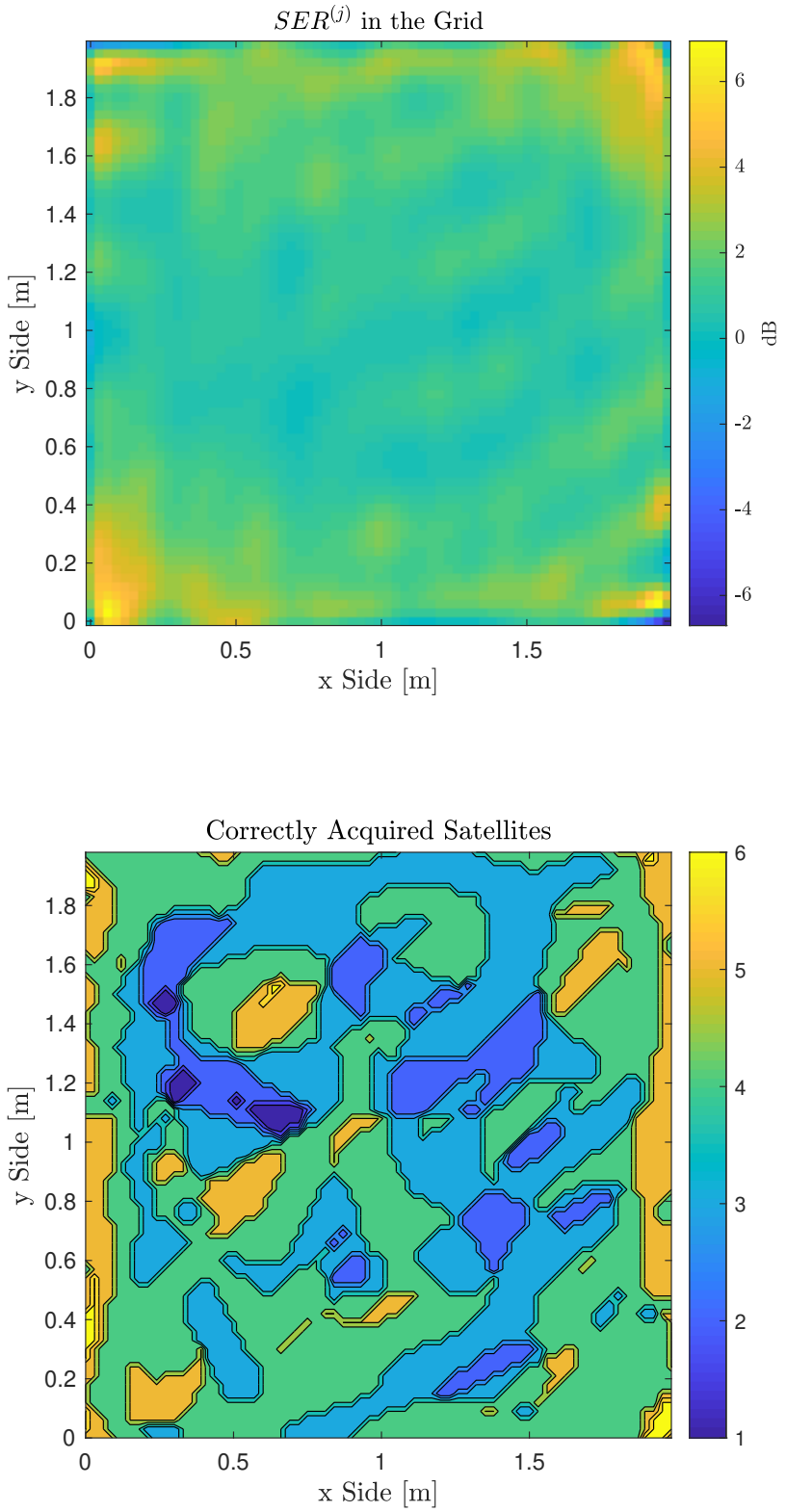


Figure 5.8: Number of correctly tracked satellites over the map in comparison with the $\mathrm{SER}_{\mathrm{dB}}^{(j)}$ values.

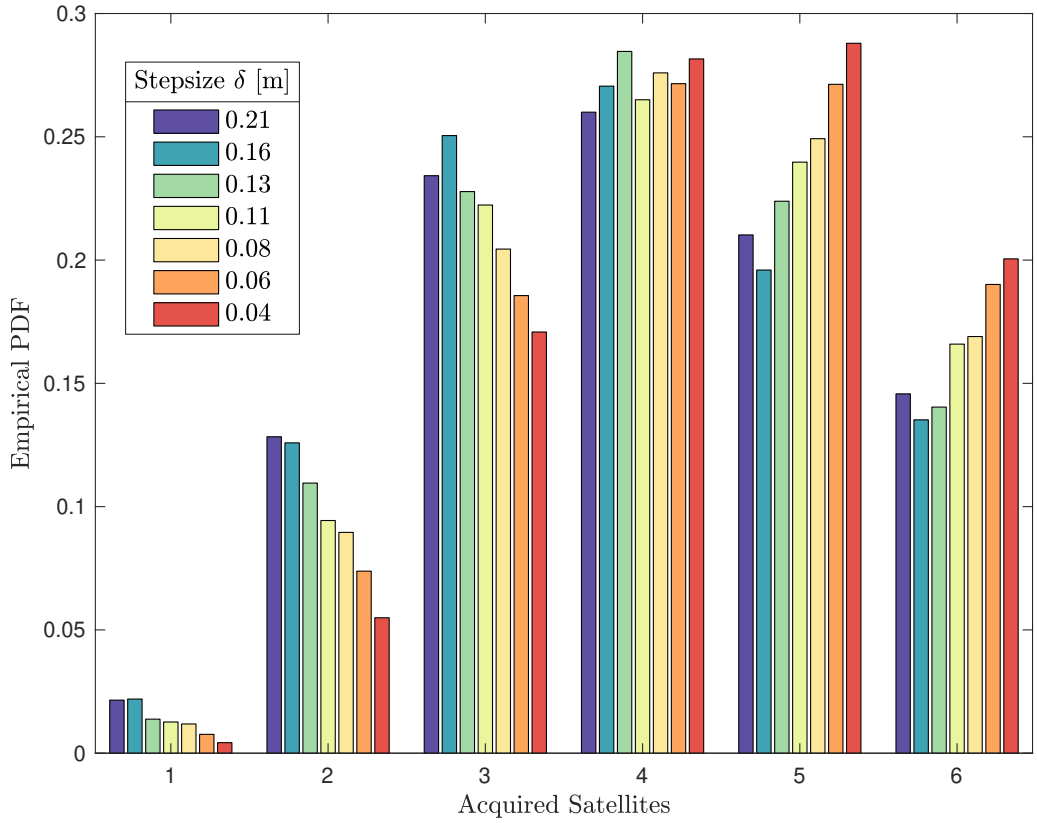


Figure 5.9: Empirical PDF of the acquired satellites over the map.

Parameters	Value
Ground antennas N_a	49
Spoofed satellites N_s	6
Grid points N_p	4489
Map $\mathcal{M}$ size	2×2 m^2
Grid step-size δ	0.03 m
Observation time Δt	1 ms
Oversampling factor κ	13
Filter length L_c	40
Map height h	50 m

Parameters	Value
Ground antennas N_a	$9 - 400$
Spoofed satellites N_s	6
Grid points N_p	Variable
Map $\mathcal{M}$ size	2×2 m^2
Grid step-size δ	Variable
Observation time Δt	1 ms
Oversampling factor κ	5
Filter length L_c	40
Map height h	50 m

Table 5.2: Configuration B (left), configuration C (right).

Chapter 6

Conclusion Remarks

The first part of this thesis was devoted to presenting the spatial spoofing. The novelty of this approach lies in the act of spoofing an entire region instead of pursuing multiple target-oriented attacks. In the swarm of drones, this concept could be worthwhile especially when the number of UAVs is large. Moreover, the spatial approach can inherently ensure consistency between spoofed locations, preventing its detention when drones can collaborate by exploiting all available data to spot inconsistencies and detect attacks.
In the second part, the problem has been modeled and the optimum solution, in terms of MSE, has been carried out by exploiting a multidimensional extension of the Wiener filter. A signal processing scheme to conduct the attack from an antenna array was thus proposed. In order to reduce the computational complexity, an additional sub-optimal method, based on computing the LS solution iteratively, has been derived.
In the third part, the spatial spoofing performance obtained through the proposed methods has been analyzed. Two metrics have been considered, the first one is the SER and the second one is based on emulating the acquisition process performed in GNSS receivers. The results are very variable and the parameters which affect the performance are numerous. Some considerations about the grid used to represent the map have been drawn. A notable effect occurs when the stepsize of the grid approach the carrier wavelength which allows making use of fewer resources to operate the attack.
This work lays the bases for the so-called spatial spoofing approach, however, we do not pretend to fulfill all the details to conduct the attack. So far many assumptions have been used, leaving enough work for future developments: 3D regions extension, advanced channel modeling, and the use of realistic tracking loops simulation are some of the aspects to better analyze the feasibility and the potential of the spatial spoofing. Notice that hijacking or capturing a group of drones is a much broader task than the mere spoofing

itself [23]. To be effective, spoofing attacks should gradually be introduced to prevent their detection and other problems to the drone navigation systems, and once receivers are locked to attacker's signals, complex post-capture control is required to prudently navigate the swarm.
In conclusion, the proposed spatial spoofing has the right credentials to become an effective GNSS spoofing approach, especially for drone swarms according to the aforementioned reasons. By its nature, the attack requires several antennas placed on the ground, making the configuration of the attack a bit laborious. However, this technique could be suitable as a defense mechanism, alternative to jammers, to protect strategic infrastructures against malicious UAVs.

Appendix A

Iterative Least Squares SPS Positioning Algorithm

The purpose of this well-known algorithm is to determine the receiver coordinate $\boldsymbol{p} = (x, y, z)$ and the reference time t by using a set of pseudorange measurements $\{\hat{\rho}_i\}_{i=0}^{N_s-1}$ of at least 4 satellites in view. Since in our work we assume that the receives is already synchronized, t is not estimated and thus the minimum required number of satellites is 3. The i-th pseudorange is approximated by the following quantity:

$$\hat{\rho}_i \approx \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}. \tag{A.1}$$

If we linearize the previous equation at the approximative solution $\boldsymbol{p}_0 = (x_0, y_0, z_0)$:

$$\hat{\rho}_i = \hat{\rho}_{i,0} + \frac{x_0 - x_i}{\hat{\rho}_{i,0}} dx + \frac{y_0 - y_i}{\hat{\rho}_{i,0}} dy + \frac{z_0 - z_i}{\hat{\rho}_{i,0}} dz, \tag{A.2}$$

with $dx = x - x_0$, $dy = y - y_0$, $dz = z - z_0$. We obtain a system of 3 equations in 3 unknowns

$$\boldsymbol{y} = \begin{bmatrix} \hat{\rho}_a - \hat{\rho}_{a,0} \\ \hat{\rho}_b - \hat{\rho}_{b,0} \\ \hat{\rho}_c - \hat{\rho}_{c,0} \end{bmatrix} = \begin{bmatrix} \frac{x_0 - x_a}{\hat{\rho}_{a,0}} & \frac{y_0 - y_a}{\hat{\rho}_{a,0}} & \frac{z_0 - z_a}{\hat{\rho}_{a,0}} \\ \frac{x_0 - x_b}{\hat{\rho}_{b,0}} & \frac{y_0 - y_b}{\hat{\rho}_{b,0}} & \frac{z_0 - z_b}{\hat{\rho}_{b,0}} \\ \frac{x_0 - x_c}{\hat{\rho}_{c,0}} & \frac{y_0 - y_c}{\hat{\rho}_{c,0}} & \frac{z_0 - z_c}{\hat{\rho}_{c,0}} \end{bmatrix} \begin{bmatrix} dx \\ dy \\ dz \end{bmatrix} = \boldsymbol{A}\boldsymbol{x}, \tag{A.3}$$

whose solution for dx, dy, dz, $\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{y}$, can improve the position estimation:

$$\boldsymbol{p}_1 = \boldsymbol{p}_0 + [dx, dy, dz]^T. \tag{A.4}$$

Then we repeat the same procedure with $\boldsymbol{p}_1$, until:

$$|\boldsymbol{p}_{i+1} - \boldsymbol{p}_i| < \gamma. \tag{A.5}$$

It has been proved that, even if the initial guess of position $\boldsymbol{p}_0$ is inaccurate, this method converges in few iterations. For more than 3 satellites the system is over-determined, due to errors on the measurements that makes the system in (A.3) inconsistent. To solve this problem the *Least-Squares method* [1] can be used:

$$\hat{\boldsymbol{x}} = \left(\boldsymbol{A}^T \boldsymbol{A}\right)^{-1} \boldsymbol{A}^T \boldsymbol{y}. \tag{A.6}$$

Appendix B

Derivation of the MSE Terms

In this appendix we calculate the derivative of all the terms of(4.24) and (4.25), namely $\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)$, $\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)$, $\mathrm{tr}\left(\boldsymbol{F}^{(p,p)H}\right)$, and $\mathrm{tr}\left(\boldsymbol{B}^{(p,p)H}\right)$. In Appendix C a fundamental proposition widely used in this section is stated. Note the the derivatives are calculated with respect to both $\boldsymbol{C}_{h,I}$ and $\boldsymbol{C}_{h,Q}$.

- $\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)$:

$$\begin{aligned}\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} &= \sum_{q} \frac{\partial \,\mathrm{tr}\left(\boldsymbol{C}_{p-q}^{H}\hat{\boldsymbol{H}}_{q}^{H}\boldsymbol{G}_{p}\right)}{\partial \boldsymbol{C}_{h,I}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{C}_{h}^{H}\hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}\right)}{\partial \boldsymbol{C}_{h,I}} \\ &= \frac{\partial \,\mathrm{tr}\left(\left(\boldsymbol{C}_{h,I}^{T} - \mathrm{i}\,\boldsymbol{C}_{h,Q}^{T}\right)\hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}\right)}{\partial \boldsymbol{C}_{h,I}} = \hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}.\end{aligned} \tag{B.1}$$

  Note that this and the following partial derivatives with respect to $\boldsymbol{C}_{h}$ (real and imaginary components) we consider only $c_{min} \leq h \leq c_{max}$.

$$\begin{aligned}\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,Q}} &= \frac{\partial \,\mathrm{tr}\left(\left(\boldsymbol{C}_{h,I}^{T} - \mathrm{i}\,\boldsymbol{C}_{h,Q}^{T}\right)\hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}\right)}{\partial \boldsymbol{C}_{h,Q}} \\ &= -\,\mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}.\end{aligned} \tag{B.2}$$

  Then by summing the two components:

$$\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} + \mathrm{i}\,\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,Q}} = 2\hat{\boldsymbol{H}}_{p-h}^{H}\boldsymbol{G}_{p}. \tag{B.3}$$

- $\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)$:

$$\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)}{\partial \boldsymbol{C}_{h,I}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)*}\right)}{\partial \boldsymbol{C}_{h,I}} = \hat{\boldsymbol{H}}_{p-h}^{T}\boldsymbol{G}_{p}^{*} \tag{B.4}$$

$$\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)}{\partial \boldsymbol{C}_{h,Q}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)*}\right)}{\partial \boldsymbol{C}_{h,Q}} = +\,\mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{T}\boldsymbol{G}_{p}^{*}. \tag{B.5}$$

Then by summing the two components:

$$\begin{aligned}\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)^H}\right)}{\partial \boldsymbol{C}_{h}} &= \frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)}{\partial \boldsymbol{C}_{h,I}} + \mathrm{i}\,\frac{\partial \,\mathrm{tr}\left(\boldsymbol{D}^{(p,p)H}\right)}{\partial \boldsymbol{C}_{h,Q}} \\ &= \hat{\boldsymbol{H}}_{p-h}^{T}\boldsymbol{G}_{p}^{*} - \hat{\boldsymbol{H}}_{p-h}^{T}\boldsymbol{G}_{p}^{*} = \boldsymbol{0}.\end{aligned} \tag{B.6}$$

- $\mathrm{tr}\left(\boldsymbol{F}^{(p,p)H}\right)$ has no dependence on the interested coefficients, thus:

$$\frac{\partial \,\mathrm{tr}\left(\boldsymbol{F}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{F}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} = \frac{\partial \,\mathrm{tr}\left(\boldsymbol{F}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,Q}} = \boldsymbol{0}. \tag{B.7}$$

- $\mathrm{tr}\left(\boldsymbol{B}^{(p,p)H}\right)$ get a bit tedious:

$$\begin{aligned}
\frac{\partial\,\mathrm{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} &= \sum_{q_1}\sum_{q_2}\frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{p-q_1}\hat{\boldsymbol{H}}^H_{q_1}\hat{\boldsymbol{H}}_{q_2}\boldsymbol{C}_{p-q_2}\right)}{\partial \boldsymbol{C}_{h,I}} \\
&= \frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{h}\hat{\boldsymbol{H}}^H_{p-h}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h}\right)}{\partial \boldsymbol{C}_{h,I}} + \sum_{q_1\neq p-h}\frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{p-q_1}\hat{\boldsymbol{H}}^H_{q_1}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h}\right)}{\partial \boldsymbol{C}_{h,I}} \\
&\quad + \sum_{q_2\neq p-h}\frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{h}\hat{\boldsymbol{H}}^H_{p-h}\hat{\boldsymbol{H}}_{q_2}\boldsymbol{C}_{p-q_2}\right)}{\partial \boldsymbol{C}_{h,I}} \\
&\quad + \sum_{q_1\neq p-h}\sum_{q_2\neq p-h}\frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{p-q_1}\hat{\boldsymbol{H}}^H_{q_1}\hat{\boldsymbol{H}}_{q_2}\boldsymbol{C}_{p-q_2}\right)}{\partial \boldsymbol{C}_{h,I}} \\
&= \frac{\partial\,\mathrm{tr}\left(\left(\boldsymbol{C}^T_{h,I}-\mathrm{i}\,\boldsymbol{C}^T_{h,Q}\right)\hat{\boldsymbol{H}}^H_{p-h}\hat{\boldsymbol{H}}_{p-h}\left(\boldsymbol{C}_{h,I}+\mathrm{i}\,\boldsymbol{C}_{h,Q}\right)\right)}{\partial \boldsymbol{C}_{h,I}} \\
&\quad + \sum_{q_1\neq p-h}\frac{\partial\,\mathrm{tr}\left(\boldsymbol{C}^H_{p-q_1}\hat{\boldsymbol{H}}^H_{q_1}\hat{\boldsymbol{H}}_{p-h}\left(\boldsymbol{C}_{h,I}+\mathrm{i}\,\boldsymbol{C}_{h,Q}\right)\right)}{\partial \boldsymbol{C}_{h,I}} \\
&\quad + \sum_{q_2\neq p-h}\frac{\partial\,\mathrm{tr}\left(\left(\boldsymbol{C}^T_{h,I}-\mathrm{i}\,\boldsymbol{C}^T_{h,Q}\right)\hat{\boldsymbol{H}}^H_{p-h}\hat{\boldsymbol{H}}_{q_2}\boldsymbol{C}_{p-q_2}\right)}{\partial \boldsymbol{C}_{h,I}}.
\end{aligned} \tag{B.8}$$

Considering that for the generic matrix $\boldsymbol{P}$:

$$\begin{aligned}
\left(\boldsymbol{C}^T_{h,I}-\mathrm{i}\,\boldsymbol{C}^T_{h,Q}\right)\boldsymbol{P}\left(\boldsymbol{C}_{h,I}+\mathrm{i}\,\boldsymbol{C}_{h,Q}\right) &= \boldsymbol{C}^T_{h,I}\boldsymbol{P}\boldsymbol{C}_{h,I}+\mathrm{i}\,\boldsymbol{C}^T_{h,I}\boldsymbol{P}\boldsymbol{C}_{h,Q} \\
&\quad -\mathrm{i}\,\boldsymbol{C}^T_{h,Q}\boldsymbol{P}\boldsymbol{C}_{h,I}+\boldsymbol{C}^T_{h,Q}\boldsymbol{P}\boldsymbol{C}_{h,Q},
\end{aligned} \tag{B.9}$$

then:

$$\begin{aligned}\frac{\partial \operatorname{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} &= \left(\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h} + \hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\right)\boldsymbol{C}_{h,I} \\ &\quad + \mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h,Q} - \mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\boldsymbol{C}_{h,Q} \\ &\quad + \sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} + \sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &= \hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\boldsymbol{C}_{h}^{*} + \hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h} \\ &\quad + \sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} + \sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &= \sum_{q}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} + \sum_{q}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q}\end{aligned} \tag{B.10}$$

$$\begin{aligned}\frac{\partial \operatorname{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,Q}} &= +\mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\boldsymbol{C}_{h,I} - \mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h,I} \\ &\quad + \left(\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h} + \hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\right)\boldsymbol{C}_{h,Q} \\ &\quad + \mathrm{i}\sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} - \mathrm{i}\sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &= \mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{p-h}^{*}\boldsymbol{C}_{h}^{*} - \mathrm{i}\,\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{p-h}\boldsymbol{C}_{h} \\ &\quad + \mathrm{i}\sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} - \mathrm{i}\sum_{q\neq p-h}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &= \mathrm{i}\sum_{q}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*} - \mathrm{i}\sum_{q}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q}\end{aligned} \tag{B.11}$$

$$\begin{aligned}\frac{\partial \operatorname{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h}} &= \frac{\partial \operatorname{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,I}} + \mathrm{i}\,\frac{\partial \operatorname{tr}\left(\boldsymbol{B}^{(p,p)}\right)}{\partial \boldsymbol{C}_{h,Q}} \\ &= \cancel{\sum_{q}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*}} + \sum_{q}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &\quad - \cancel{\sum_{q}\hat{\boldsymbol{H}}_{p-h}^{T}\hat{\boldsymbol{H}}_{q}^{*}\boldsymbol{C}_{p-q}^{*}} + \sum_{q}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q} \\ &= 2\sum_{q}\hat{\boldsymbol{H}}_{p-h}^{H}\hat{\boldsymbol{H}}_{q}\boldsymbol{C}_{p-q}.\end{aligned} \tag{B.12}$$

Appendix C

Matrix Calculus Propositions

Proposition. *Let $\boldsymbol{P}$ be a complex $m \times n$ matrix and $\boldsymbol{X}$ a real $n \times m$ matrix. We have the following properties:*

$$i.\ \frac{\partial \operatorname{tr}(\boldsymbol{PX})}{\partial \boldsymbol{X}} = \boldsymbol{P}^T \in \mathbb{C}^{n \times m}$$

$$ii.\ \frac{\partial \operatorname{tr}\left(\boldsymbol{X}^T \boldsymbol{P}^T\right)}{\partial \boldsymbol{X}} = \boldsymbol{P}^T \in \mathbb{C}^{n \times m}$$

$$iii.\ \frac{\partial \operatorname{tr}\left(\boldsymbol{X}^T \boldsymbol{PX}\right)}{\partial \boldsymbol{X}} = \left(\boldsymbol{P} + \boldsymbol{P}^T\right) \boldsymbol{X} \in \mathbb{C}^{m \times m}.$$

Proof. :

i. Note that in this case we must have that $\boldsymbol{P} \in \mathbb{C}^{m \times n}$ otherwise the claim is ill-posed, since the trace loses its meaning. Let $\boldsymbol{A}$ be the product between the two matrices:

$$\boldsymbol{A} = \boldsymbol{PX} \qquad \Rightarrow \qquad a_{ij} = \sum_{k=0}^{m-1} p_{ik} x_{kj}, \tag{C.1}$$

then the output of the trace operation is the following scalar:

$$\gamma = \operatorname{tr}(\boldsymbol{A}) = \sum_{i=0}^{n-1} a_{ii} = \sum_{i=0}^{n-1} \sum_{k=0}^{m-1} p_{ik} x_{ki}. \tag{C.2}$$

Therefore by differentiating that quantity with respect to $\boldsymbol{X}$ we get:

$$\boldsymbol{Q} = \frac{\partial \operatorname{tr}(\boldsymbol{PX})}{\partial \boldsymbol{X}}, \tag{C.3}$$

where the dimensions of $\boldsymbol{Q}$ are:

- $n \times m$ using the *Jacobian formulation* (Numerator layout)
- $m \times n$ using the *Hessian formulation* (Denominator layout)

Since in this case the numerator is scalar we pefer to use the denominator layout. By proceeding element-wise calculus we get:

$$q_{rt} = \sum_{i=0}^{n-1} \sum_{k=0}^{m-1} \frac{\partial [p_{ik} x_{ki}]}{\partial x_{rt}} = p_{tr} \qquad r = 0, \ldots, m-1 \quad t = 0, \ldots n-1, \tag{C.4}$$

hence $\boldsymbol{Q} = \boldsymbol{P}^T$.

ii. The proof is obtained from the property that a square matrix and its transpose have the same trace, $\operatorname{tr}(\boldsymbol{A}) = \operatorname{tr}\left(\boldsymbol{A}^T\right)$, and then using i.

iii. In this case n is required to be equal to m, then $\boldsymbol{P}$ has to be a square matrix $m \times m$. Let $\boldsymbol{A}$ now be equal to the product $\boldsymbol{X}^T\boldsymbol{PX}$. Their elements are:

$$a_{ij} = \sum_{\ell=0}^{m-1} \sum_{k=0}^{m-1} x_{\ell i} p_{\ell k} x_{kj}. \tag{C.5}$$

As did before we define:

$$\boldsymbol{Q} = \frac{\partial \operatorname{tr}\left(\boldsymbol{X}^T\boldsymbol{PX}\right)}{\partial \boldsymbol{X}}, \tag{C.6}$$

which elements are:

$$
\begin{aligned}
q_{rt} &= \sum_{i=0}^{n-1}\sum_{\ell=0}^{m-1}\sum_{k=0}^{m-1}\frac{\partial\left[p_{\ell k}x_{\ell i}x_{ki}\right]}{\partial x_{rt}} = \sum_{\ell=0}^{m-1}\sum_{k=0}^{m-1}\frac{\partial\left[p_{\ell k}x_{\ell t}x_{kt}\right]}{\partial x_{rt}} \\
&= \frac{\partial\left[p_{rr}x_{rt}^2\right]}{\partial x_{rt}} + \sum_{\substack{\ell=0\\ \ell\neq r}}^{m-1}\frac{\partial\left[p_{\ell r}x_{\ell t}x_{rt}\right]}{\partial x_{rt}} + \sum_{\substack{k=0\\ k\neq r}}^{m-1}\frac{\partial\left[p_{rk}x_{rt}x_{kt}\right]}{\partial x_{rt}} + \cancel{\sum_{\ell\neq r}\sum_{r\neq r}\frac{\partial\left[p_{\ell k}x_{\ell t}x_{kt}\right]}{\partial x_{rt}}} \\
&= 2p_{rr}x_{rt} + \sum_{\substack{\ell=0\\ \ell\neq r}}^{m-1}p_{\ell r}x_{\ell t} + \sum_{\substack{k=0\\ k\neq r}}^{m-1}p_{rk}x_{kt} = \sum_{\ell=0}^{m-1}p_{\ell r}x_{\ell t} + \sum_{k=0}^{m-1}p_{rk}x_{kt} \\
&= \sum_{h=0}^{m-1}\left(p_{hr}+p_{rh}\right)x_{ht},
\end{aligned}
\tag{C.7}
$$

thus by inspection the claim follows.

□

Bibliography

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

[2] B. Gao, G. Hu, S. Gao, Y. Zhong, and C. Gu, "Multi-sensor optimal data fusion for INS/GNSS/CNS integration based on unscented kalman filter," *International Journal of Control, Automation and Systems*, vol. 16, no. 1, pp. 129–140, 2018.

[3] A. Rawnsley, "Iran's alleged drone hack: tough, but possible," *Wired*, 2011.

[4] "Gatwick runway reopens after drone chaos," *BBC News*.

[5] M. Nichols, "South korea tells UN that north korea GPS jamming threatens boats, planes," *Reuters, Newspaper*, 2016.

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

[7] G. Caparra and N. Laurenti, "On the use of CSK for GNSS anti-spoofing," in *2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–7, IEEE, 2018.

[8] F. Formaggio, S. Tomasin, G. Caparra, S. Ceccato, and N. Laurenti, "Authentication of galileo GNSS signal by superimposed signature with artificial noise," in *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 2573–2577, IEEE, 2018.

[9] O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–6, IEEE, 2010.

[10] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of applied research and technology*, vol. 13, no. 1, pp. 45–57, 2015.

[11] M. Cuntz, A. Konovaltsev, and M. Meurer, "Concepts, development, and validation of multiantenna gnss receivers for resilient navigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1288–1301, 2016.

[12] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust gnss receivers by array signal processing: theory and implementation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1207–1220, 2016.

[13] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194–199, IEEE, 2017.

[14] M. Karaim, H. Elghamrawy, M. Tamazin, and A. Noureldin, "Investigation of the effects of white gaussian noise jamming on commercial gnss receivers," in *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pp. 468–472, IEEE, 2017.

[15] R. Kulikov, V. Pudlovsky, A. Grebennikov, and D. Tsaregorodtsev, "Cooperative navigation of vehicles using mutual retransmission of gnss's signals," in *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, pp. 442–446, IEEE, 2019.

[16] Z. Renyu, S. C. Kiat, W. Kai, and Z. Heng, "Spoofing attack of drone," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 1239–1246, IEEE, 2018.

[17] H.-J. Kim and H.-S. Ahn, "Realization of swarm formation flying and optimal trajectory generation for multi-drone performance show," in *Proc. IEEE/SICE International Symposium on System Integration (SII)*, pp. 850–855, IEEE, 2016.

[18] S. K. Mitra and Y. Kuo, *Digital signal processing: a computer-based approach*, vol. 2. McGraw-Hill New York, 2006.

[19] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[20] N. Benvenuto and G. Cherubini, *Algorithms for communications systems and their applications*. John Wiley & Sons, 2002.

[21] D. Messerschmitt *et al.*, "Stationary points of a real-valued function of a complex variable," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2006-93*, 2006.

[22] A. Joseph, "Gnss solutions: Measuring gnss signal strength," *Inside GNSS-Engineering Solutions for the Global Navigation Satellite System Community*, vol. 5, no. 8, pp. 20–25, 2010.

[23] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via gps spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.