DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea Triennale in
Ingegneria Informatica

Physical layer challenge-response authentication for drone communications

Relatore:
Prof. Stefano Tomasin

Laureando:
Damiano Salvaterra
1189839

Anno Accademico 2022/2023

Abstract

Challenge-response is a well-known authentication protocol often implemented using encryption in upper layers. This thesis explores a new application of this mechanism at the physical layer, specifically in the context of drone communications. The objective is to leverage the characteristics of the radio channel model to establish a *partially controllable channel*. Instead of the verifier sending challenges to the drone, the verifier manipulates the physical properties of the channel and the drone's modified signal serves as the response during the verification process.

In particular, this study focuses on power fluctuations due to shadowing, given an area where the drone is free to move. It will be demonstrated that these fluctuations can be exploited to achieve the desired partially controllable channel. Finally, the effectiveness of this approach will be evaluated in terms of misdetection and false alarm probability.

Contents

Introduction

The use of drones for communications is a subject of research in several contexts, such as *Internets of Drones (IoDs)* or *flying ad-hoc networks (FANETs)*. In these contexts, drones are organized in *swarms* to perform coordinated tasks. This architecture provides a flexible communication infrastructure but also exposes the nodes to various types of attacks. Thus, it is necessary to implement an authentication mechanism that is both reliable and efficient in terms of resources, such as computability and energy. The authentication problem is usually addressed with encryption mechanisms, which are expensive since they require updates of secret keys. Other solutions for challenge-response authentication have been recently studied, such as exploiting the so-called *physical unclonable functions (PUF)*, which can be leveraged to support authentication and establish a secure key for communication. Another alternative is leveraging the signals exchanged by the agents, in order to obtain authentication on signals at the physical layer. One of the advantages of this solution is that a physical layer authentication (PLA) based on this principle does not require dedicated hardware and reuses the signal processing existing in the communication devices to achieve security. In the case of drones, or more generally in wireless communications with mobile terminals, the propagation characteristics of the channel can be used to fingerprint a message.

The idea is to leverage the shadowing realizations on different possible positions of the drone in order to obtain different channel configurations, as described in Chapter 1. To achieve this, it is necessary to have a channel model that takes into account the spatial differences across the map where the drone operates. In this regard, Chapter 2 presents a simplified model sourced from the literature, which incorporates path loss and shadowing realizations. Chapter 3 discusses the statistics of the introduced channel model, obtained from simulations with parameters sourced from the literature to gain insights into the distribution of channel configurations. Lastly, Chapter 4 examines a real-case scenario, present-

ing statistics based on experimental parameters, and demonstrates the results in terms of misdetection probability.

Chapter 1

Partially controllable channel

1.1 Physical layer Challenge-response authentication mechanism

A Challenge-response (CR) protocol is based on a secret shared between the two parties in communication, called Alice and Bob, that enables Bob to ask random questions that only Alice can answer. In this sense, a tag-based authentication can be seen as a particular case of challenge-response, in which there is only one question-answer pair. A more complete example of challenge-response is the One Time Password (OTP): in this situation, the challenge changes whenever the authentication is requested. These mechanisms are implemented with encryption schemes and, although in a case such as the OTP the key is usually communicated out-of-band, the mechanism still requires something to be shared. With the physical layer CR mechanism presented here, this is not necessary.

1.1.1 Partially controllable channel

The key concept of CR PLA authentication is the *partially controllable channel*: one or more characteristics of the channel can be controlled by Bob, which means that when Alice wants to start a communication with Bob, the latter can change the channel characteristics in order to perform a challenge to Alice. In this case, the response is the change of the channel between Alice and Bob and therefore the change of the signal received by Bob. Since Bob controls the channel, he can estimate what the characteristics of the received signal should be like, then the response can be evaluated and compared with the expected behavior and can be considered valid if the received signal is consistent with the channel alteration

introduced by the authenticator. In this scenario, the alteration of the channel model does not need to be known to Alice, as Bob is the only one who knows the controllable parameters of the channel. Ideally, Alice could be completely unaware that the authentication is happening.

Examples of partially controllable channels are [1]:

- **Intelligent reflective surfaces (IRS)**: IRSs reflect impinging radio signals with controllable phases, providing a highly controllable channel configuration with the high directivity of the signal.
- **Wireless Relays**: Relays receive radio signals from one direction and retransmit the signals in another direction using combiners and beamformers. The relay acts as the controllable part of the channel, where the configuration is a specific combination of beamformers and combiners. Also in this case the authentication is performed using the directivity of signals.
- **Swarm networks**: In this case, the controllable channel is achieved with the cooperation of multiple devices. A swarm consists of a group of drones or a group of vehicles, whose characteristic is to be mobile. Mobility is the controllable part of the channel since moving the devices implies changing the channel between the parties in communication. In this case, Bob can be considered the entire swarm, while Alice is a drone that wants to send a message. The same concept can be applied to the situation in which one drone communicates with a base station on the ground, which can order the drone to move before initiating communication.

This last point is discussed in the next section.

1.2 PLA in a drone-base station communication

As mentioned, the controllable parameter in a swarm network is the position of drones: moving a drone implies changing the Channel State Information (CSI) of the wireless link, including parameters such as distance, fading and shadowing. The large number of possible positions of the drone ensures a wide control space and a high variable channel. This means that for an eavesdropper (Eve), hijacking the communication is challenging due to the high variability of the channel parameters (and thus of the challenges proposed by Bob) [2].

Here, the focus is on the variations of power attenuation introduced by the shadowing effect. The aim is to exploit the random distribution of shadowing to

obtain a non-predictable space-varying channel. In fact, if the path loss due to distance can be easily predicted by an eavesdropper, the shadowing component can only be known by those who have already mapped the channel over the space.

In an ideal situation where the base station (which is Bob in this case) knows exactly how the shadowing is distributed, when a drone (Alice) wants to start a communication, the base orders the drone to move to a certain point $\mathbf{p}$ of the space and then transmit. Now, the base station knows what the channel configuration in $\mathbf{p}$ should be, so when it receives the signal it is compared with the estimation. If the received signal is consistent with the channel estimation, the drone is authenticated. As it will be explained in 2.1.2, shadowing affects the power attenuation additively with a random normal variable.

Therefore, for an eavesdropper who wants to hijack the communication, the only way to perform the attack is to brute-force over all the possible realizations of the shadowing. Even if the attacker (Eve) knows the statistics of shadowing (i.e. variance and mean value) and the position of the drone (thus the path loss), the best she can do is try to guess the channel configuration (here, the power attenuation) over a range of values that follow a normal distribution. Based on this, it is desirable that the range be as large as possible, in order to allow more channel configurations while decreasing the probability of interception. The range of attenuation over which the channel configurations will be identified will be discussed in Chapter 3.

Besides, in a more realistic scenario, there is another factor to take into consideration, the microscopic fading, which adds another random component that is completely unpredictable. Although the fading effect is smaller than shadowing, the result is that given the point $\mathbf{p}$ with the same hypothesis as before, Bob cannot know the exact power of the incoming signal. Therefore, if $h_{(\mathbf{p})}$ is the channel estimation at point $\mathbf{p}$, Bob has to accept the incoming signal even if it is in a neighborhood of the point $\mathbf{p}$. The width of the neighborhood where the signal has to be considered acceptable depends on the fading statistics and the range of power attenuation caused by shadowing. The consequence is that the space of attenuation has to be divided into "slots", each of which is a channel configuration. To gain authentication, Eve's attack strategy is now to guess the slot where the current channel configuration is located. She does not need to know the exact parameters of the channel between Alice and Bob. As will be discussed later, this fading behavior is also responsible for errors in detecting legitimate communication as malicious, particularly when the fading realization

is strong enough to dramatically alter the channel configuration. This implies the need to look for a trade-off between correctly determining the identity of a legitimate drone and the number of potential channel configurations (this will be discussed in Chapter 4).

PLA algorithm for drone authentication To summarize, the step-by-step algorithm for the initial channel measurements and the actual drone authentication is described here.

1. *CSI measurements*: Alice (drone) moves around the space and transmits several pilot signals from different positions chosen by Bob (base station). These transmissions are authenticated by higher-layer security mechanisms and are used by Bob to estimate the CSI over different channel configurations (i.e., positions).

2. *Random configuration*: Bob proposes a challenge to Alice by randomly choosing a position over the space in which the drone has to move to be authenticated. The specific position may not have been explored in Step 1, but the resulting CSI should be predictable based on the observations made previously.

3. *Message transmission*: Alice transmits the message, and Bob estimates the CSI from the received signal, which represents the response from Alice.

4. *Channel check*: If the estimated CSI matches the CSI predicted in step 2, Bob considers Alice authenticated.

This procedure does not use pre-shared keys, except during step 1 during channel measurement. This assumption is common also in physical-layer tag-based authentication.

Chapter 2

Channel model

As discussed before, the first step of the PLA is the channel state information measurement and the identification phase, in which the transmitter (i.e. the drone) sends *pilot signals* in order to let the receiver estimate the channel. To do that, the drone moves to several points in the space and sends signals. The base station will estimate the channel state information (CSI) over these points, each of which will have different parameters, like distance, shadowing component, carrier frequency offset, channel impulse response and so on. These features depend on the position of the device and the propagation environment, while having some correlation between two different positions. This chapter focuses on the path loss and shadowing component estimation of the radio channel over the area in which the drone can move.

2.1 Narrowband channel model

2.1.1 Derivation of the power and attenuation equations

In this section is reported the channel model in [3].
A deterministic ray model is used to evaluate the power of the received signal in the case of *line of sight* (LOS), that in the absence of obstacles between transmitter and receiver. In this case it can be assumed that only one wave (ray) propagates from the transmitter to the receiver. Under these conditions, the channel can be modeled in terms of power and attenuation as follows.

Let P_{Tx} be the power of the signal transmitted by an isotropic antenna. At

distance d from the antenna, the power density per area is

$$\Phi_0 = \frac{P_{Tx}}{4\pi d^2}\,, \tag{2.1}$$

where $4\pi d^2$ is the surface of a sphere of radius d. Here, the power density decreases with the square of the distance which means, on a logarithmic scale, that decreases by 20 dB per decade with distance. In the case of a directional antenna, the power density can be written as

$$\Phi = G_{Tx}\Phi_0 = \frac{P_{Tx}G_{Tx}}{4\pi d^2}\,, \tag{2.2}$$

where G_{Tx} is the antenna gain. At the receive antenna, the *available power* is given by

$$P_{Rc} = \Phi A_{Rc}\eta_{Rc}\,, \tag{2.3}$$

where P_{Rc} is the received power, A_{Rc} is the effective area of the receive antenna and the efficiency factor $\eta_{Rc} < 1$ represents the fact that the antenna does not capture all incident radiation. In fact, the antenna gain can be written as

$$G = \frac{4\pi A}{\lambda^2}\eta\,, \tag{2.4}$$

where A is the effective area of the antenna, $\lambda = c/f_0$ is the wavelength of the transmitted signal, f_0 is the carrier frequency and η is the efficiency factor. Combining (2.3), (2.2) and (2.4), the *Friis transmission equation* is obtained:

$$P_{Rc} = P_{Tx}G_{Tx}G_{Rc}\left(\frac{\lambda}{4\pi d}\right)^2\,, \tag{2.5}$$

from which can be derived the available attenuation of the medium in decibels:

$$(a)_{dB} = 10\log\frac{P_{tx}}{P_{Rc}} = 32.4 + 20\log d|_{km} + 20\log f_0|_{MHz} - (G_{Tx})_{dB} - (G_Rc)_{dB}\,. \tag{2.6}$$

Now, assuming the gain factors G_{Tx} and G_{Rc} are fixed since they depend on the devices used for transmitting/receiving, the attenuation that is relevant for the study of spatial variations of the channel is the *free-space path loss* due to distance, that is, in (2.6), the term:

$$(\overline{a}_{PL,fs})_{dB} = 32.4 + 20\log d|_{km} + 20\log f_0|_{MHz}\,. \tag{2.7}$$

This expresses the fact that changing the position of the drone (or the position of the receiver) in general changes the distance and hence the path loss. It is worth noting that the name *free-space* refers to a propagation model where there are no reflection and scattering phenomena and therefore the one-ray model is applicable. In fact, the factor 20 of the logarithm of distance comes from the 2-exponent of the distance in (2.5). A more complete model that takes into account multipath propagation effects would be written as:

$$(\overline{a}_{PL})_{dB} = 32.4 + \alpha 10 \log d|_{km} + 20 \log f_0|_{MHz} \,, \tag{2.8}$$

where α is the path-loss coefficient. Since the drone is supposed to be in flight and the environment is static, the model can be simplified to the case of only the LOS component, thus keeping $\alpha = 2$.

2.1.2 Shadowing effects in the channel model

This paragraph describes the shadowing -also called macroscopic fading- phenomenon and its statistics, which is the main parameter that makes the medium highly variable and enables the authenticator to select over a wide range of configurations. Experimentally, it is observed that the macroscopic fading introduces an attenuation that follows a normal distribution and, since the attenuation is expressed in decibels, the statistics of shadowing is a *log-normal distribution*. This means that the attenuation due to path loss *and* shadowing is the sum of (2.7) and a random variable in dB:

$$(a_{PL})_{dB} = (\overline{a}_{PL})_{dB} + (\xi)_{dB} \,, \tag{2.9}$$

where $(\xi)_{dB} \sim \mathcal{N}(0,\, \sigma^2_{(\xi)_{dB}})$ is a normal distribution in dB scale and $\sigma_{(\xi)_{dB}}$ is the standard deviation of the shadowing component, usually being $\sigma_{(\xi)_{dB}} \in [4, 12]$. The actual value of $\sigma_{(\xi)_{dB}}$ depends on the amount of environmental data taken into account by the model. An important result that enables the channel estimation through the space is the Gudmundson model, which gives the correlation of the shadowing components between two receivers at distance Δ:

$$r_{(\xi)_{dB}}(\Delta) = \sigma^2_{(\xi)_{dB}} \mathrm{e}^{-\frac{|\Delta|}{D_{coh}}} \,, \tag{2.10}$$

where D_{coh} is the coherence distance, i.e., the distance in space within the fading effect is strongly correlated. The value of coherence distance is proportional to

the wavelength, which is in turn inversely proportional to the (carrier) frequency. In general, D_{coh} can be approximated as:

$$D_{coh} = k\lambda = k\frac{c}{f_0}, \qquad k > 0\,, \tag{2.11}$$

where k is a coefficient that depends on the environment. For example, values of coherence distance at a base station range from 3λ to 20λ, respectively in an urban area with many obstacles and a flat rural area.
The spatial correlation between shadowing components is essential for channel estimation and thus for authentication accuracy. Therefore, based on the coherence distance and standard deviation parameters, a space model of macroscopic fading will be presented in the following section.

2.2 Discrete-space model of shadowing

Shadowing is a random variable that depends on both time and space. In this simplified model, a static channel with respect to time is considered, which means that shadowing across the space will be studied given a realization in time. The parameter that expresses the correlation between shadowing across space is the coherence distance, which is the basis for the model of shadowing spatial distribution in the following [3].
The model is generated with an algorithm that essentially produces values of $(\xi)_{dB}[\mathbf{n}]$ on a grid made by points $\mathbf{n}$, correlated according to (2.10), starting from independent and identically distributed complex Gaussian samples across the same points. The operator that generates the shadowing from the Gaussian noise is a convolution between the noise and a filter with characteristics dependent on the Gudmundson model.

Let the coordinates of the discrete (2D) space be:

$$\mathbf{c} = (c_1, c_2) = (n_1 A, n_2 A) = (n_1, n_2)A, \qquad (n_1, n_2) \in \mathcal{S} \subset \mathbb{Z}^2, \tag{2.12}$$

where A is the step size (i.e. the distance between adjacent points). Given the autocorrelation function $r_{(\xi)_{dB}}(\Delta)$, where

$$\Delta = \sqrt{c_1^2 + c_2^2} = A\sqrt{n_1^2 + n_2^2}\,, \tag{2.13}$$

The power spectral density of the autocorrelation is[1]:

$$\mathcal{P}(\mathbf{k}) = DFT_2\left[r_{(\xi)_{dB}}(A\sqrt{n_1^2+n_2^2})\right] \qquad \mathbf{k}\in\mathcal{S}\,, \tag{2.14}$$

and the filter can be calculated as:

$$\mathcal{H}_{sh}(\mathbf{k}) = \mathcal{K}\sqrt{\mathcal{P}(\mathbf{k})} \quad \text{and} \quad h_{sh}(\mathbf{n}) = DFT_2^{-1}\left[\mathcal{H}_{sh}(\mathbf{k})\right]\,, \tag{2.15}$$

where $\mathcal{K}$ is such that h_{sh} has unit energy

$$\sum_{\mathbf{n}\in\mathcal{S}}|h_{sh}(\mathbf{n})|^2 = \frac{1}{N_1N_2}\sum_{\mathbf{k}\in\mathcal{S}}|\mathcal{H}_{sh}(\mathbf{k})|^2 = 1. \tag{2.16}$$

This can be obtained by the normalization:

$$h_{sh}(\mathbf{n}) = \frac{\hat{h}_{sh}(\mathbf{n})}{\sqrt{\sum_{\mathbf{n}\in\mathcal{S}}|\hat{h}_{sh}(\mathbf{n})|^2}} \tag{2.17}$$

where

$$\hat{h}_{sh}(\mathbf{n}) = DFT_2^{-1}\left[\hat{\mathcal{H}}_{sh}(\mathbf{k})\right] \quad \text{and} \quad \hat{\mathcal{H}}_{sh}(\mathbf{k}) = \sqrt{\mathcal{P}(\mathbf{k})} \tag{2.18}$$

A complex i.i.d Gaussian noise is generated on the space $\mathcal{S}$ as

$$w(\mathbf{n}) \sim \mathcal{CN}(0,\,\sigma^2_{(\xi)_{dB}}), \quad \mathbf{n}\in\mathcal{S} \tag{2.19}$$

Then, the shadowing component $(\xi)_{dB}[\mathbf{n}]$ is obtained by the convolution

$$(\xi)_{dB}[\mathbf{n}] = \sum_{\mathbf{p}\in\mathcal{S}_h} h_{sh}(\mathbf{p})w(\mathbf{n}-\mathbf{p}), \quad \mathbf{n}\in\mathcal{S}, \tag{2.20}$$

where $h_{sh}(\mathbf{p})$ is the filter in (2.17).

[1] DFT_2 indicates the 2-Dimensional Discrete Fourier Transform

Chapter 3

Simulation of the channel model

This chapter presents the results of the channel simulation. The channel has been modeled on a square area of 225 m^2,following the procedure of Chapter 2 with the following parameters:

- step size $A = 0.15$
- Carrier frequency $f_0 = 1800$ MHz
- Coherence distance $D_{coh} = 10\lambda \approx 1.67$ m
- standard deviation of the shadowing component $\sigma_{(\xi)_{dB}} = 6$ dB
- Path-loss coefficient $\alpha = 2$
- Base station distance $d_b = 100$ m.

The last point refers to the distance from the base station, assumed to be on the ground, and the center of the square. The actual distance between the base station and the points on the space can be obtained from this distance and the distance of the points from the center:

$$d_{\mathbf{x}} = \sqrt{d_0^2 + d_b^2} \tag{3.1}$$

where $\mathbf{x} = (x_1, x_2)$ is a point on the area and $d_0 = \sqrt{x_1^2 + x_2^2}$ is the distance of $\mathbf{x}$ from the origin.

3.1 Shadowing simulation

The shadowing is generated as described in Section 2.2 with the parameters specified in the previous section. The grid on which the shadowing is generated is shown in Figure 3.1.

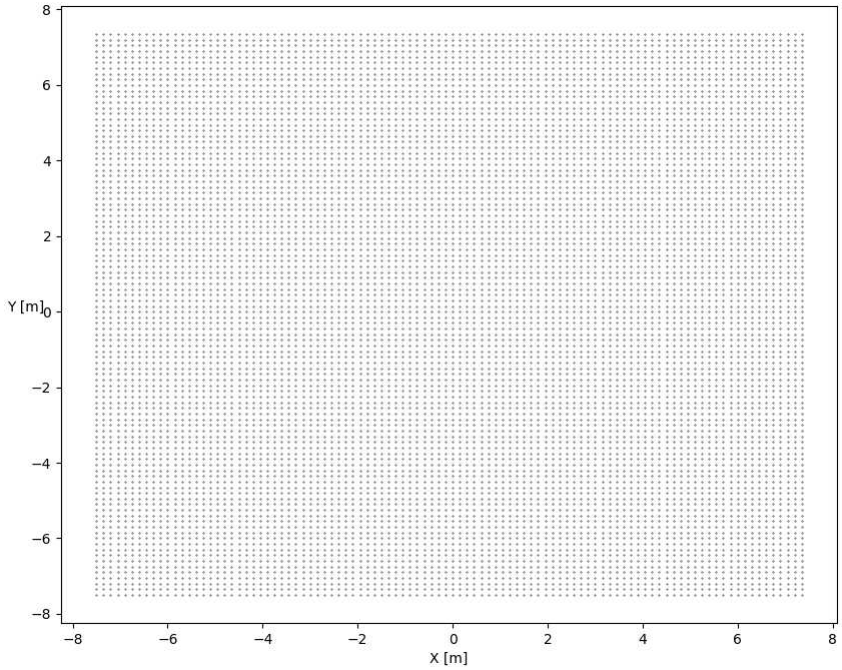


Figure 3.1: Space grid

The shadowing component has been simulated on this grid and the contour plot in Figure 3.5 shows the amplitude (in dB) of one realization of the shadowing on the space, while the module in Decibel of the filter $h_{sh}(\mathbf{n})$ used for the computation of (2.20) is plotted in Figure 3.3.

Then, the path loss is calculated on the space as in (2.7) with distance as in (3.1) for each point. As Figure 3.6 shows, the path loss does not vary widely in the space. In fact, since the base station is ideally placed at 100 meters away from the origin, the horizontal d_0 component in (3.1) has little effect on the total distance and thus on the path loss (refer to Figure 3.2). Numerically, the distance $d_{\mathbf{x}_f}$ between the furthest point from the center and the base station is

$$d_0 = \sqrt{7.5^2 + 7.5^2} = 10.6 \text{ m} \implies d_{\mathbf{x}_f} = \sqrt{100^2 + d_0^2} = 100.56 \text{ m}$$

And the path loss in $\mathbf{x}_f$ is:

$$(\overline{a}_{PL,fs}(\mathbf{x}_f))_{dB} = 32.4 + 20\log d_x|_{km} + 20\log f_0|_{MHz} = 77.554 \text{ dB}$$

while the path loss in the origin is

$$(\overline{a}_{PL,fs}(\mathbf{0}))_{dB} = 32.4 + 20\log d_b|_{km} + 20\log f_0|_{MHz} = 77.505 \text{ dB}.$$

Indeed, the instance in Figure 3.6 results from the sum of the path loss component and the shadowing component. The shape of the amplitude does not change much compared to that in Figure 3.5, except for the shift of ≈ 77 dB due to the path loss.

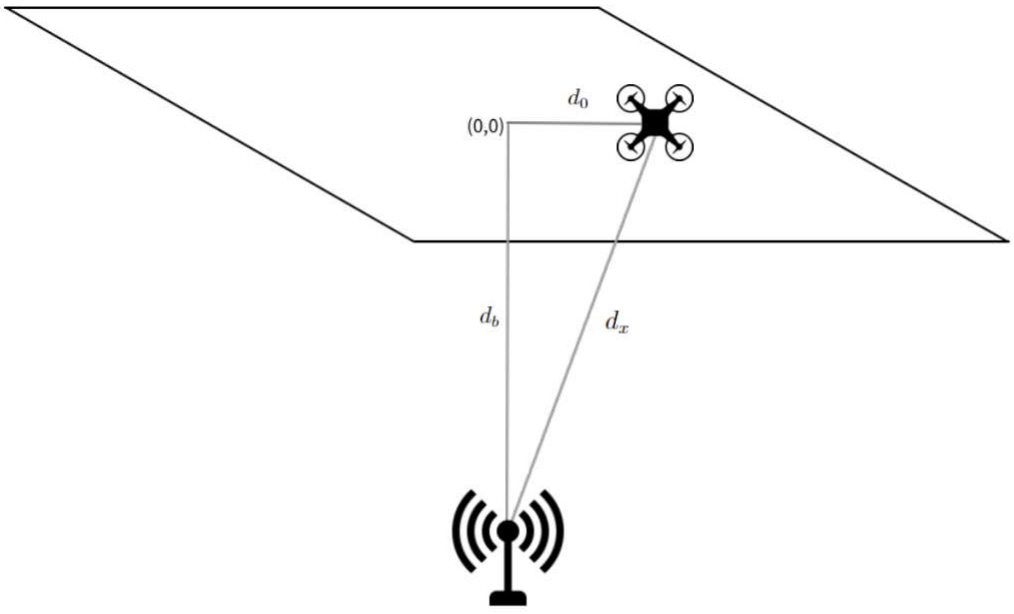


Figure 3.2: Visual representation of the space: on the ground is the base station, and the drone moves within a square area at a height of d_b.

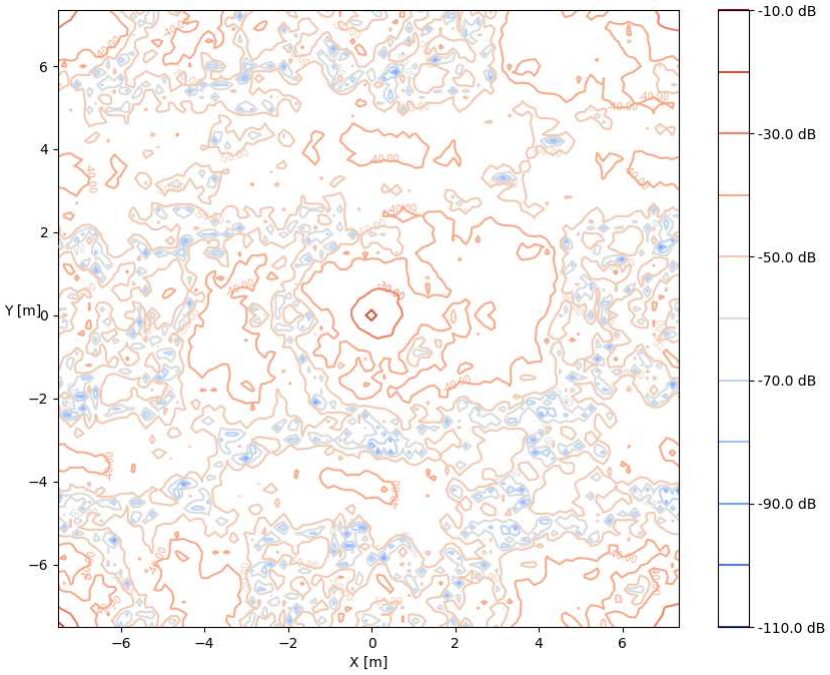


Figure 3.3: $20 \log_{10} |h_{sh}(\mathbf{n})|$

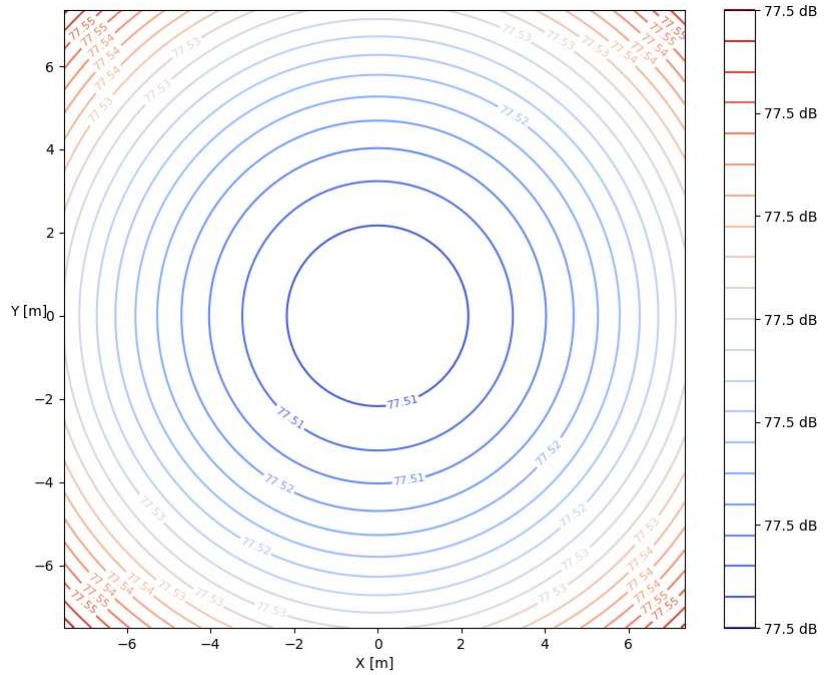


Figure 3.4: Path loss

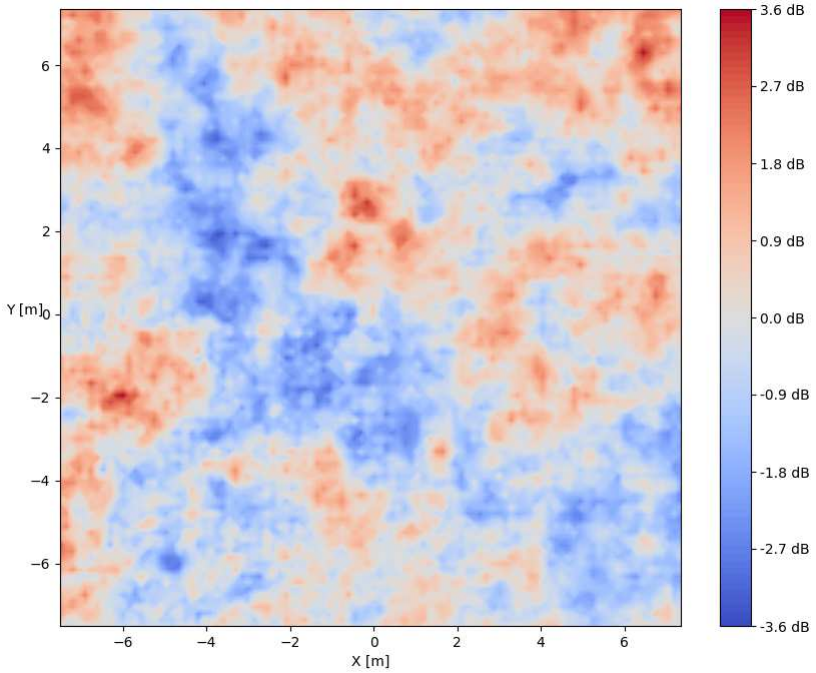


Figure 3.5: Shadowing attenuation

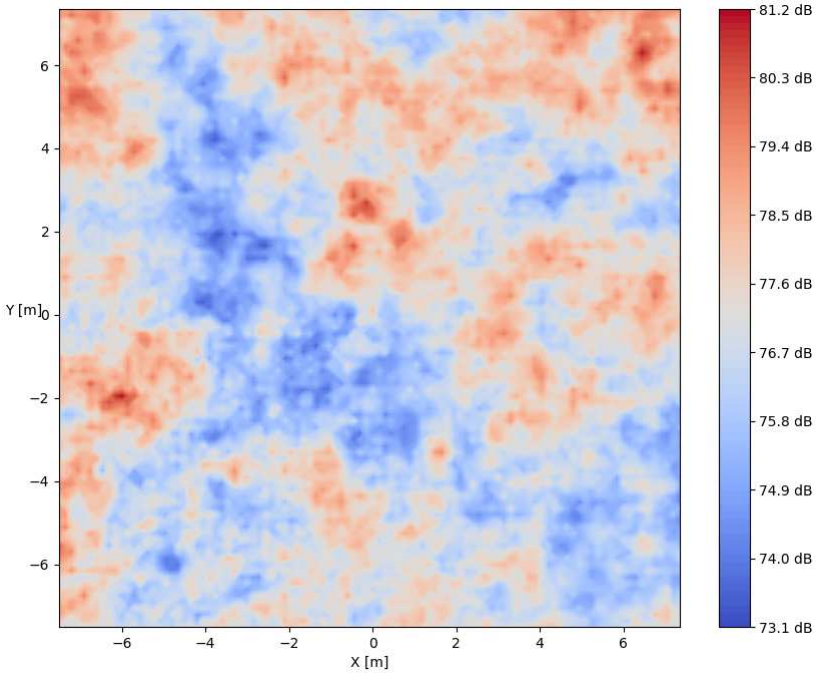


Figure 3.6: Attenuation due to path loss and shadowing

3.2 Channel statistics

The previous section showed how to simulate a channel model when shadowing occurs, but since this is a random variable that changes over time and depends on the environment, it is necessary to have a statistical idea of how the channel may vary with different realizations[1] of shadowing. As mentioned in Section 1.2, the goal is to obtain a range of power attenuation in which the channel configurations can be identified, which can be expressed as:

$$(\mathcal{R})_{dB} = (a_{max})_{dB} - (a_{min})_{dB} \tag{3.2}$$

where

$$(a_{max})_{dB} = \max_{\mathbf{x}\in\mathcal{S}} \; a_{(\mathbf{x})}$$

$$(a_{min})_{dB} = \min_{\mathbf{x}\in\mathcal{S}} \; a_{(\mathbf{x})}$$

and $a_{(\mathbf{x})}$ is obtained from (2.9).
Before going into detail, a few considerations can be made. First, as seen in the previous section, when the vertical component of the distance is much larger than the horizontal component, the path loss changes slightly across the space and the shadowing has the highest impact on $(\mathcal{R})_{dB}$. However, even if the base station stays at the same distance in each realization, the shadowing component always varies and so does the value of $(\mathcal{R})_{dB}$. Moreover, $(a_{max})_{dB}$ and $(a_{min})_{dB}$ depend on the single realization, which means that during the initial phase of the protocol (the CSI measurements) these values need to be identified to fully exploit the channel.

With this in mind, using the simulation presented in Section 3.1 a statistic of $(\mathcal{R})_{dB}$ has been generated. Figures 3.7 and 3.8 show, respectively, the probability density function (PDF) of the shadowing and the PDF of the range $(\mathcal{R})_{dB}$ across 1000 realizations.

The mean value $(\overline{\mathcal{R}})_{dB}$ is:

$$(\overline{\mathcal{R}})_{dB} = \frac{1}{M}\sum_{i=1}^{M}(\mathcal{R}_i)_{dB} = 9.14 \text{ dB} \tag{3.3}$$

where $(\mathcal{R}_i)_{dB}$ is the range value of the *i-th* instance of the model.

[1]Here, with the term *realization* is intended both shadowing realization in the same environment (e.g. the same city) at different times and realization in different environment where the shadowing parameters (as variance) are assumed to be the same.

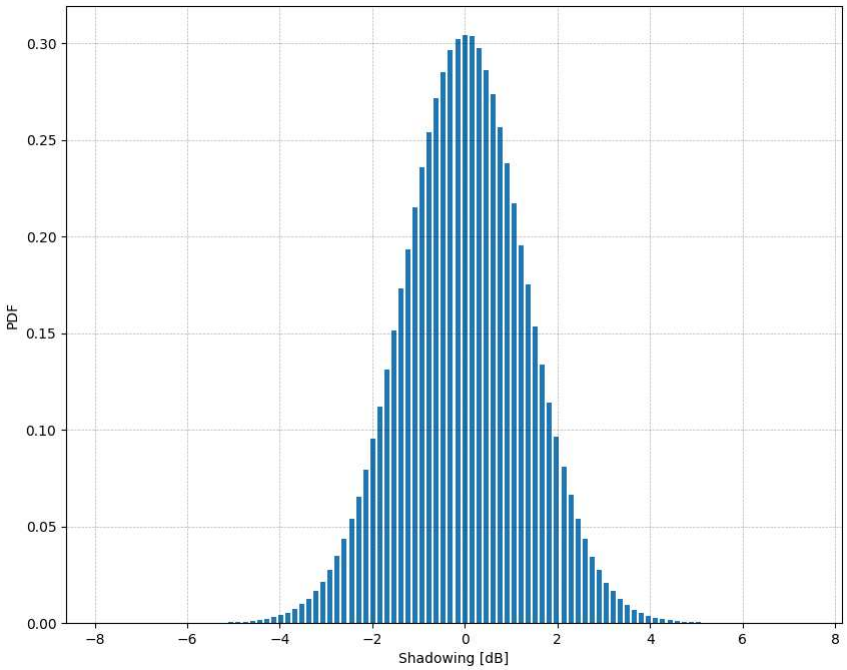


Figure 3.7: PDF of the shadowing across 1000 realizations

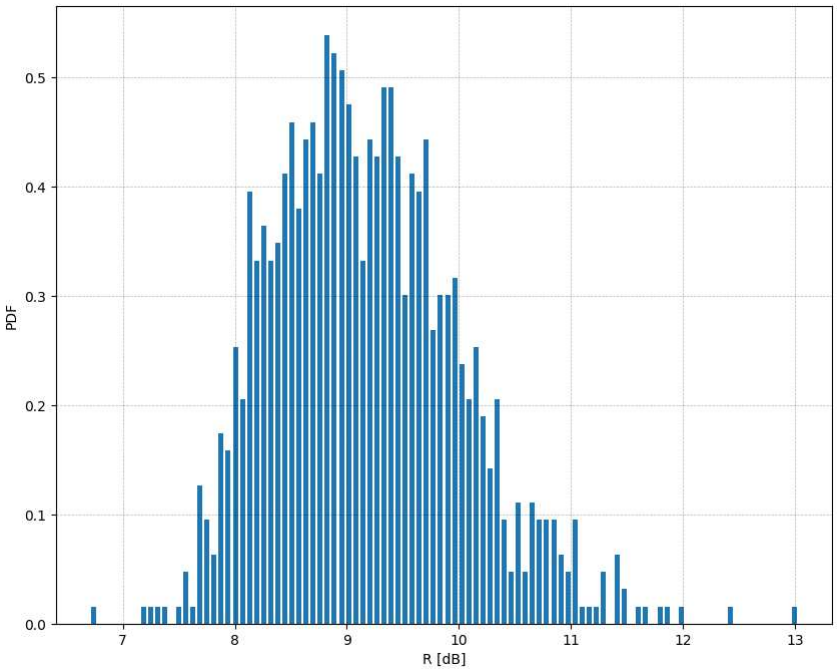


Figure 3.8: Empirical PDF of $(\mathcal{R})_{dB}$ over 1000 realizations.

On distribution of the range $(\mathcal{R})_{dB}$

The empirical PDF in Figure 3.8 displays a long-tailed distribution, possibly skewed, which is not easily described by a closed form. The range $(\mathcal{R})_{dB}$ is a random variable described by (3.2), where $(a_{max})_{dB}$ and $(a_{min})_{dB}$ represent the maximum and minimum values, respectively, of a set of correlated random Gaussian variables. A literature search was conducted to find a suitable formulation for the PDF of this range, but no similar findings were discovered.

To gain insight into the variability of this range across different realizations, several simulations were performed. The mean value of $(\mathcal{R})_{dB}$ was calculated as a function of the map's size. This approach aims to explore how $(\mathcal{R})_{dB}$ may vary as the space available for the drone to perform authentication expands. As discussed in Chapter 4, the misdetection probability is a function of the attenuation range and therefore, in order to achieve a desired misdetection probability, the appropriate choice of the map's size is crucial.

The scatter plot in Figure 3.9 shows the mean value and the 10th percentile of $(\mathcal{R})_{dB}$ calculated on a square area with a side length of $L \in [1, 100]$ meters and a coherence distance of $D_{coh} = 1.67$m, as in the previous simulations. The function decreases as L increases. This behavior is attributed to the relatively small value of the coherence distance compared to the map size. Specifically, the shadowing spatial correlation exponentially decreases with $\frac{1}{D_{coh}}$ (see Equation 2.10). This means that the variation of the range across different realizations is less affected by the realization of shadowing, as its peaks and troughs tend to stabilize when the map size is beyond a certain threshold. In fact, beyond some value of L, the dominant factor contributing to the increase of $(\mathcal{R})_{dB}$ becomes the path loss rather than the shadowing.

As a result, as the area increases, the impact of shadowing diminishes, while $(\mathcal{R})_{dB}$ becomes more sensitive to the path loss, resulting in wider extremes of $(\mathcal{R})_{dB}$. However, the growth attributed to path loss is less pronounced compared to that caused by shadowing. This concept is better illustrated in Figure 3.10, which presents the same scatter plot with the coherence distance increased by a factor of 10 (this exaggerated value has been deliberately chosen to emphasize this fact). The plot demonstrates that a larger coherence distance (which depends on the transmission frequency) results in more correlated values of $(a_{max})_{dB}$ and $(a_{min})_{dB}$, leading to a narrower overall range width. On the other hand, increasing the size of the map beyond a certain threshold appears to yield a higher value of $(\mathcal{R})_{dB}$; however, this gain is primarily driven by the path loss due to distance,

which is deterministic. As a result, a more deterministic relationship between $(\mathcal{R})_{dB}$ and the drone's position could potentially provide attackers with insights on how to carry out more effective attacks. Therefore, if it is possible to select the frequency and the spatial dimensions it could be beneficial to seek a trade-off between the transmission frequency and the size of the map.

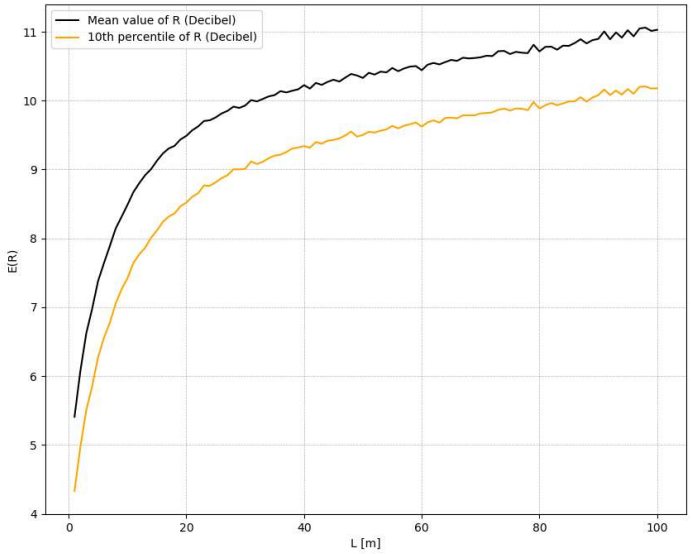


Figure 3.9: Mean value of $(\mathcal{R})_{dB}$ varying L and $D_{coh} = 1.67\text{m}$. The area covered is given by $A = L^2$.

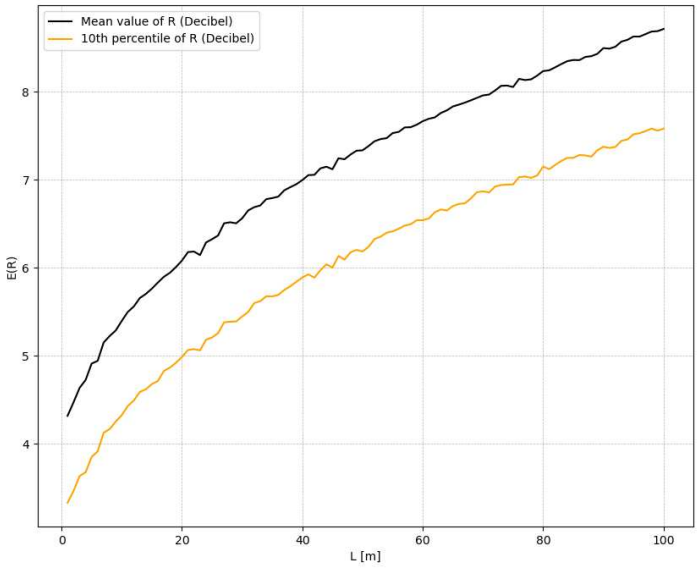


Figure 3.10: Same as Figure 3.9 but with $D_{coh} = 16.7\text{m}$.

Chapter 4

Performance analysis in a real-case scenario

The previous chapter presents the simulation of the radio channel and the statistics of the attenuation caused by shadowing, using parameters taken from the literature. As demonstrated, one parameter that strongly influences the distribution of $(\mathcal{R})_{dB}$ is the coherence distance. As observed, when D_{coh} is calculated using (2.11), the path-loss quickly dominates the growth of $(\mathcal{R})_{dB}$, resulting in a more deterministic channel as the map size increases. Moreover, this behavior is independent of the path-loss due to distance, meaning that it generally holds true even for smaller drone altitudes.

In fact, [4] demonstrates that there is no clear relationship between the coherence distance and the drone altitude. However, based on the experimental data gathered during the research, it is evident that, compared to the previous simulations, the real-case shadowing standard deviation is smaller while it is more correlated. In particular, [4] shows that in an urban environment, at an altitude of approximately 20 meters, the shadowing standard deviation barely reaches the value of $\sigma_{(\xi)_{dB}} = 2.5$ dB, decreasing even further when increasing the drone height above the rooftop level. Additionally, the coherence distance at this altitude lies around the value of 10 meters.

Based on these results, new simulations has been performed keeping the parameters as in [4], thus:

- $D_{coh} = 10$ m;
- $\sigma_{(\xi)_{dB}} = 2.5$ dB;
- drone height $d_b = 20$ m;

- carrier frequency $f_0 = 1800$ Mhz.

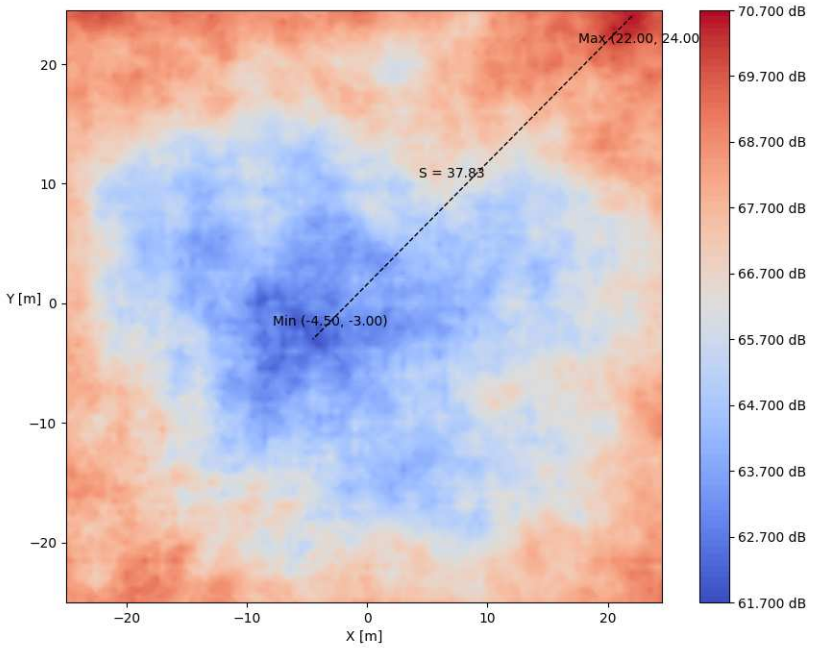
Furthermore, these experimental parameters allow for estimation of the effectiveness of the authentication system in a real scenario.

4.1 Channel profile and authentication path

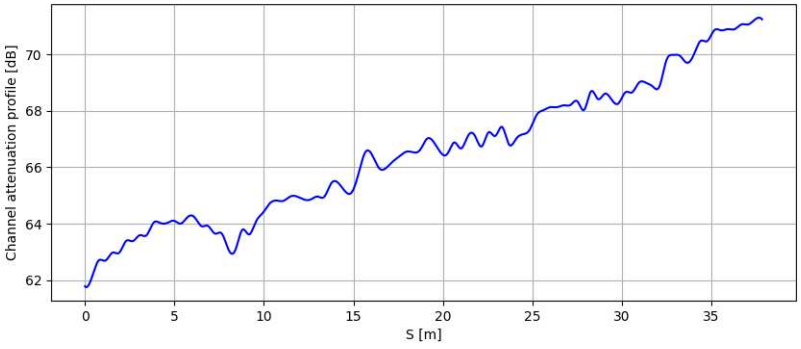
As discussed before, a lower altitude of the drone leads to a more path-loss dependent channel map. Consequently, the extremes of $(\mathcal{R})_{dB}$, $(a_{min})_{dB}$, and $(a_{max})_{dB}$ are more likely to be situated, respectively, around the origin (i.e., over the base station) and close to the borders of the map. The probability of this event is influenced by the shadowing standard deviation, as a more variable shadowing distribution implies that the channel profile could deviate significantly from the path-loss shape.

Another important consideration is the power consumption of an authentication process. When the drone undergoes authentication, it has to move around the space and this implies power usage. Given a channel realization, the mean power usage is also influenced by the position of $(a_{min})_{dB}$ and $(a_{max})_{dB}$, as they define the amplitude of $(\mathcal{R})_{dB}$ and, ultimately, the number of channel configurations. For this purpose, the fact that the extremes are found more probably in certain points of the space helps in determining the average power consumption in different realizations, although this entails a slightly more predictable channel. This situation can be advantageous or disadvantageous depending on whether power consumption or security is of greater concern. As expected, this fact insights that to improve the effectiveness of the challenge-response, more power usage is needed.

For simplicity, in this study, it is considered the case in which the drone moves along this *authentication line*. Considering one authentication line instead of all possible channel configurations over the space makes it easier for the drone to locate the "challenge" sent by the station, while considering all possible channel configurations, since every attenuation value between $(a_{min})_{dB}$ and $(a_{max})_{dB}$ can be found on this line. However, this solution is not optimal from the power consumption point of view, and further investigations are needed in order to minimize the power usage during the authentication process. Figures 4.1a and 4.2a show two realizations of the channel and the channel profile along S.

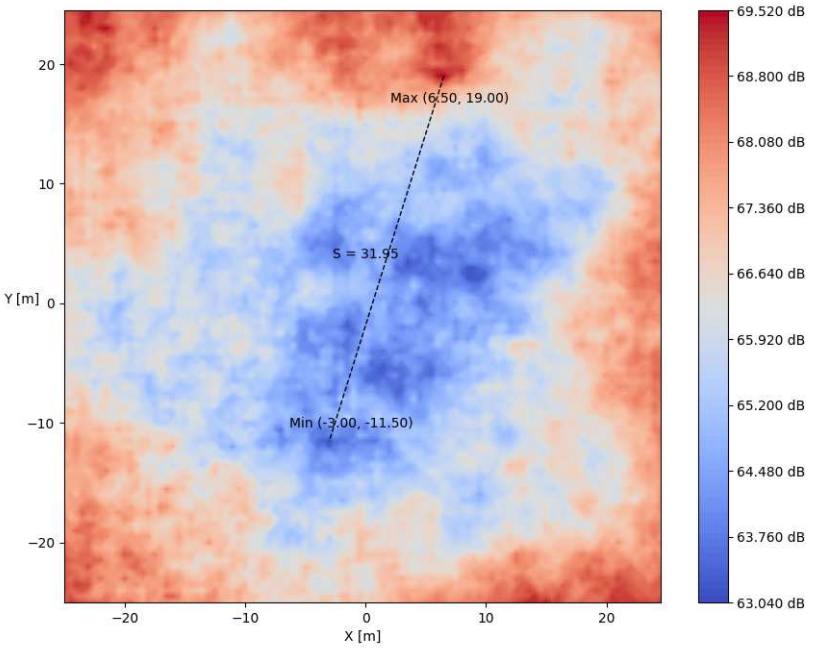


(a) Channel shape over the space

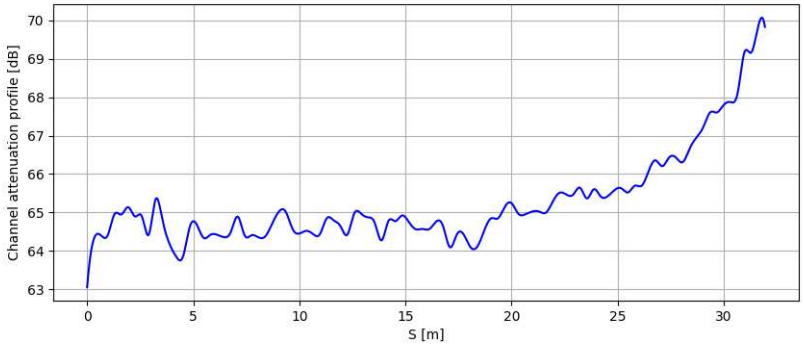


(b) Channel profile over the line S

Figure 4.1: Channel characteristics



(a) Channel shape over the space



(b) Channel profile over the line S

Figure 4.2: Channel characteristics

Now, given a drone position $s_{(t)}$ on the line at time t, when the base station requests an authentication process, it challenges the drone to move in a random[1] position $s_{(t+1)}$. The *authentication path* $p = |s_{(t+1)} - s_{(t)}|$ is what determines the power consumption during the authentication process.

The mean power consumption is then related to the mean distance traveled by the drone during several authentication processes in a specific environment. The

[1]For now, the term "random" indicates that the position is chosen with an independent uniformly random distributed variable. In other words, the base station randomly chooses a point on the line with no regard for the current position of the drone or preference for attenuation values.

plots in Figures 4.3 and 4.4 provide insights into the average size of the line S and the average authentication path length as the map size increases. In particular, the plot in Figure 4.4 is generated by simulating a random process in which the base station, for each realization[2], randomly picks 1000 attenuation values along the line S and orders the drone to move from one position $s_{(t-1)}$ to another $s_{(t)}$ consecutively. The plots show a linear dependency of the authentication line S on the size L of the map.

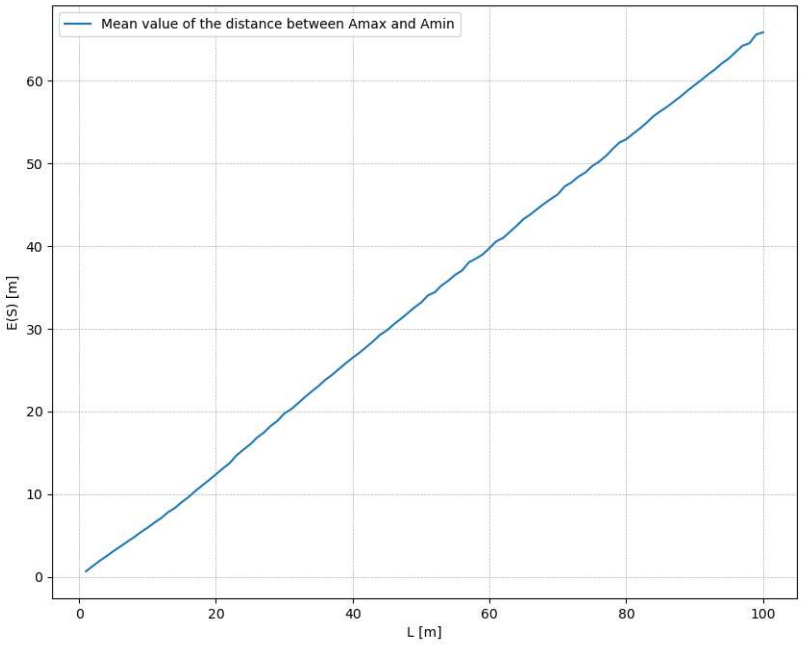


Figure 4.3: Mean value of the authentication line S

[2]For every size of L (from 1 to 100 meters), 5000 realizations have been generated

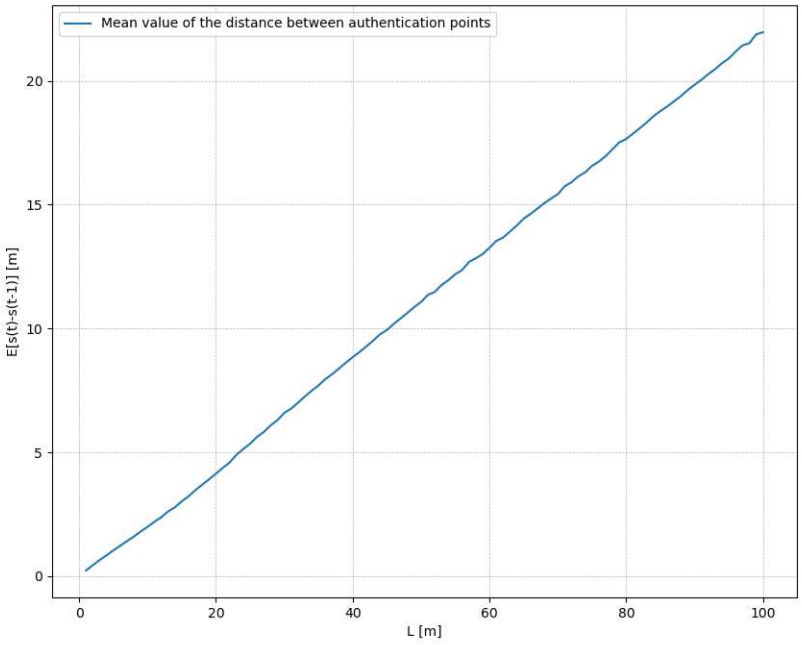


Figure 4.4: Mean value of the authentication paths length $s_{(t)} - s_{(t-1)}$

In Figure 4.5, the mean value and the 10th percentile of $(\mathcal{R})_{dB}$ are shown, as in the simulations of the previous chapter. At first glance, it may seem unexpected that in this case the value of $(\mathcal{R})_{dB}$ is larger than in the previous simulations, despite the shadowing being more correlated and having a smaller standard deviation. In reality, this result can be attributed to the fact that with a lower altitude, the path-loss distance over the points in the area varies more significantly compared to Figure 3.4.[3]

[3]Referring to Figure 3.2, since d_b is much smaller than in the previous case, for higher values of L, the distance d_0 plays a more significant role in the total distance, leading to a greater distance-dependent $(\mathcal{R})_{dB}$.

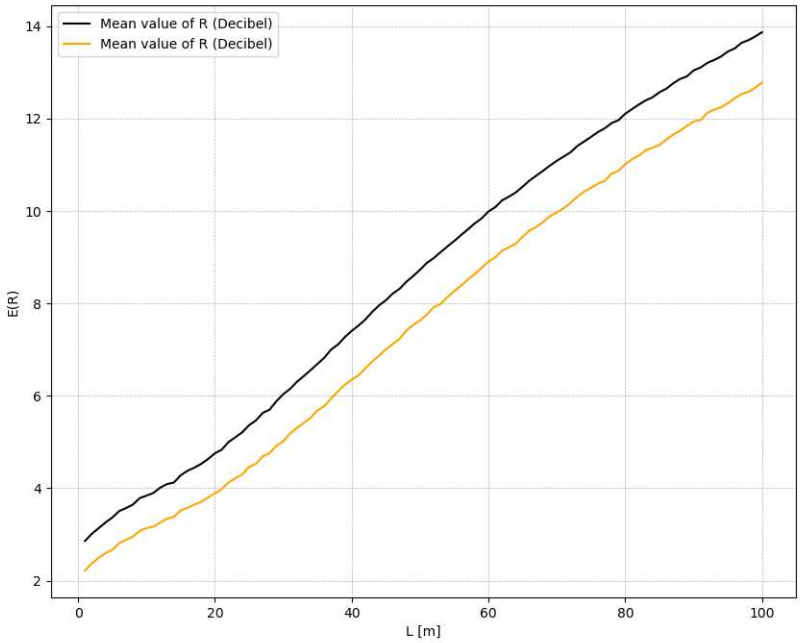


Figure 4.5: channel statistics with parameters taken from [4]

4.2 Misdetection probability estimation

As discussed in Section 1.2, when the drone is positioned at a certain location, it experiences a particular path-loss and shadowing realization. These parameters define the channel configuration that the base station expects to encounter during communication with the drone. Ideally, these parameters are also what Eve needs to guess in order to hijack the communication. However, the base station actually receives a signal that fluctuates around this channel configuration due to fading effects. This implies that in order to correctly authenticate the drone, it is necessary to have an interval $(\mathcal{I})_{dB}$ around its channel configuration within which authentication is considered valid. Since fading is a random variable, there can be a case where the drone transmits but the base station receives a signal strongly attenuated which will fall outside the interval $(\mathcal{I})_{dB}$, leading the station to reject the message as malicious, even if the transmitter is legitimate. This event, called *false alarm*, is (virtually) inevitable. What can be done is to limit the occurrence of false alarm by choosing the minimum width of $(\mathcal{I})_{dB}$ that guarantees a certain probability of false alarm (P_{FA}).

At the same time, the *misdetection probability* is the probability of consid-

ering a transmission sent by the attacker as valid[4]. Assuming that Eve has no other information available, the attack consists of randomly choosing over all the channel configurations. From her perspective, these configurations encompass all possible values contained in $(\mathcal{R})_{dB}$, as it is assumed that she does not know the width of $(\mathcal{I})_{dB}$ (otherwise, Eve could significantly reduce the attack complexity by choosing attenuation values distanced by $(\mathcal{I})_{dB}$).

The width of $(\mathcal{I})_{dB}$ is determined by choosing a value for P_{FA} and depends on fading and other noise sources that cause errors at the receiver. As an initial approximation, this effect can be represented using an additive white Gaussian noise (AWGN) channel, where noise is added to the signal transmitted by the drone. The transmitted signal reaches the receiver with an attenuation determined by the drone's position, expressed in decibels as given by (2.9).

The signal at the receiver can be written as

$$s = \frac{1}{\sqrt{A_{\mathbf{p}}}} x + n \tag{4.1}$$

where x represents the signal transmitted by the drone, n is the noise introduced, and $A_{\mathbf{p}}$ denotes the linear attenuation at a point p, defined as:

$$A_{\mathbf{p}} = 10^{\frac{(A_{\mathbf{p}})_{dB}}{10}} \tag{4.2}$$

where $(A_{\mathbf{p}})_{dB}$ is the attenuation calculated using (2.9) for the specific point of interest. This model also enables a straightforward estimation of attenuation across space by transmitting various known pilot signals and computing the mean power of the received signal. The base station will estimate the attenuation $A_{\mathbf{p}}$, introducing a certain error that depends on the noise standard deviation. Specifically, the estimated attenuation can be expressed as:

$$\hat{A}_{\mathbf{p}} = A_{\mathbf{p}} + w_A \tag{4.3}$$

where w_A is the estimation error, which is modeled as a random Gaussian distribution with a standard deviation σ_A and zero mean.

The magnitude of σ_A ultimately determines the width of the $(\mathcal{I})_{dB}$ interval (or, in the linear scale, the amplitude of $\mathcal{I}$, which is a power level ratio). In fact, in this model, P_{FA} is directly related to the distribution of w_A. For example, to achieve $P_{FA} \approx 0.05$, $\mathcal{I}$ should correspond to the 95% confidence interval, centered

[4]Refer to (4.6) and (4.7) for formal definitions.

in $A_{\mathbf{p}}$, which can be obtained as follows:

$$\mathcal{I} = 2\sigma_A \cdot \mathbf{Q}^{-1}\left(\frac{P_{FA}}{2}\right) \tag{4.4}$$

where $\mathbf{Q}$ is the complementary error function of the normal distribution. The confidence interval is independent of the drone's position (i.e., independent of the chosen CSI within the $\mathcal{R}$ interval of power attenuation) if it is assumed that the noise introduced by the receiver is not dependent on the current channel configuration. This fact results in a P_{MD} that is easily obtainable from the ratio between the range $\mathcal{R}$ of possible channel configurations and the confidence interval $\mathcal{I}$ of a single CSI. A direct relationship between P_{MD} and P_{FA} can be established:

$$P_{MD} = \frac{\mathcal{I}}{\mathcal{R}} = \frac{2\sigma_A}{\mathcal{R}} \cdot \mathbf{Q}^{-1}\left(\frac{P_{FA}}{2}\right) \tag{4.5}$$

The Figure 4.6 shows the relationship between P_{MD} and P_{FA} on the mean value of $(\mathcal{R})_{db}$.

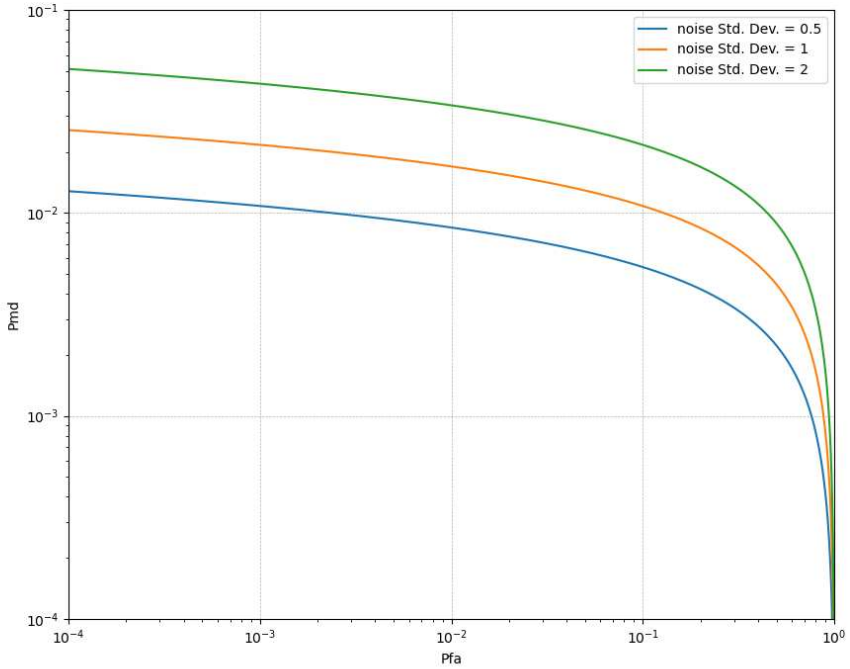


Figure 4.6: P_{MD} as a function of P_{FA} calculated on the mean value of $E\left[(\mathcal{R})_{db}\right] = 24.83$ dB of map with size $L = 100$ m

Now that the two error probabilities, P_{MD} and P_{FA}, have been derived, the authentication problem can be addressed as a binary hypothesis testing scenario, with each probability having a closed-form expression. Formally, $\mathcal{H}_0$ represents the situation in which Alice transmits a legitimate message, while $\mathcal{H}_1$ corresponds to the attack scenario, where Eve attempts to impersonate Alice.

Using this notation, P_{MD}, P_{FA}, the probability of detection P_D, and the probability of correct non-detection P_C can be defined as follows:

$$P_{MD} = (\hat{A}_e \in \mathcal{I} \mid \mathcal{H}_1) = \frac{\mathcal{I}}{\mathcal{R}} = \frac{2\sigma_A}{\mathcal{R}} \cdot \mathbf{Q}^{-1}\left(\frac{P_{FA}}{2}\right) \tag{4.6}$$

$$P_{FA} = (\hat{A}_{\mathbf{p}} \notin \mathcal{I} \mid \mathcal{H}_0) = 2\mathbf{Q}\left(\frac{\mathcal{I}}{2\sigma_A}\right) \tag{4.7}$$

$$P_D = (\hat{A}_e \notin \mathcal{I} \mid \mathcal{H}_1) = 1 - P_{MD} \tag{4.8}$$

$$P_C = (\hat{A}_{\mathbf{p}} \in \mathcal{I} \mid \mathcal{H}_0) = 1 - P_{FA} \tag{4.9}$$

Where $\hat{A}_e$ is the attenuation value guessed by Eve (there is no dependency on the specific point $\mathbf{p}$ because, as explained later, Eve can execute the attack even without knowledge of the drone's position).

Conclusions

This thesis proposes a new authentication mechanism for drone communications, based on the drone's position and the corresponding shadowing effects. The mechanism leverages the characteristics of the channel at different positions. To achieve this, the protocol initiates an initial phase of channel measurements, during which the drone traverses the space to identify the maximum and minimum attenuation values induced by shadowing and path-loss. Afterward, when Alice intends to transmit a message, Bob challenges her by selecting a position in space. He then estimates the channel characteristics at the given position and compares the estimation with the actual received signal.

The study considers a suboptimal scenario in which Bob selects points that lie along the line connecting the extreme attenuation values across space. While this approach enables the utilization of all attenuation values between the maximum and minimum, it is not efficient in terms of power consumption and further investigations are required in this regard. Once the drone is in the given position, Bob accepts the authenticity of the transmitted message only if the received signal falls within a certain range around the estimated value. The width of this range $(\mathcal{I})_{dB}$ is influenced by fading and other potential sources of errors at the base station.

To assess the effectiveness of this mechanism, numerous simulations have been conducted. Initially, the channel model and shadowing effects have been simulated using the model outlined in [3]. Statistical insights into the attenuation range $(\mathcal{R})_{dB}$ have been obtained by varying shadowing parameters, coherence distance, drone height, and map size.

Moreover, to provide insights on power consumption, the average distance between $(a_{min})_{dB}$ and $(a_{max})_{dB}$ has been found for different map sizes. This is complemented by the average drone path length for the authentication process, considering the base station's random selection of positions along the authentication line.

Lastly, by modeling the estimation error at the base station as an AWGN channel, a closed-form expression has been derived for the width of the interval $(\mathcal{I})_{dB}$. This, in turn, establishes a direct relationship between the probabilities of misdetection (P_{MD}) and false alarm (P_{FA}).

References

[1] S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Communications Magazine*, vol. 60, no. 12, pp. 138–144, December 2022.

[2] F. Mazzo, S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Physical-layer challenge-response authentication for drone networks," *2023 IEEE Global Communications Conference (GLOBECOM)*, 2023, (accepted for presentation).

[3] N. Benvenuto, G. Cherubini, and S. Tomasin, *Algorithms for Communications Systems and their Applications*. Wiley, 2021, ch. 4, pp. 193–217.

[4] M. Bucur, T. B. Sørensen, R. Amorim, M. Lopez, I. Z. Kovács, and P. Mogensen, "Validation of large-scale propagation characteristics for UAVs within urban environment," *2019 IEEE 90th Conference on Vehicular Technology (VTC)*, September 2019.