ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN

INGEGNERIA ELETTRONICA, TELECOMUNICAZIONI E TECNOLOGIE DELL'INFORMAZIONE

Ciclo 37

Settore Concorsuale: 09/F1 - CAMPI ELETTROMAGNETICI

Settore Scientifico Disciplinare: ING-INF/02 - CAMPI ELETTROMAGNETICI

PHYSICAL LAYER SOLUTIONS FOR THE SECURITY OF WIRELESS COMMUNICATIONS

Presentata da: Simone Del Prete

Coordinatore Dottorato

Davide Dardari

Supervisore

Franco Fuschini

Co-supervisore

Marina Barbiroli

Esame finale anno 2025

Contents

Introduction

The rapid growth in the number of wireless devices, driven particularly by the rise of the Internet Of Things (IOT), has significantly increased the complexity and vulnerability of communication networks. As smart cities, industry 4.0 and home automation systems become more prevalent, the need for robust security mechanisms get paramount importance. Despite the rising number of cyberattacks, security remains a secondary concern for many users and organizations.

In wireless communication, the inherent shared nature of the wireless medium creates unique challenges for security, including eavesdropping, jamming, and unauthorized access. Traditional cryptographic methods, though highly effective, are often unsuitable for many wireless devices due to their limited computational power and energy constraints. This has spurred the need for alternative solutions that can complement standard cryptography algorithms. In particular, some characteristics of the physical layer can be leveraged to enhance security without overburdening devices.

Physical Layer Security offers a promising approach by taking advantage of some inherent properties of the wireless channel, such as fading, noise, and interference, to secure communications. This thesis focuses on two major aspects of physical layer security: the analysis of wireless channels for secure key generation and the use of Frequency Diverse Arrays for geofencing applications. By studying these techniques, this work aims at providing helpful insights into the design of secure wireless systems that can meet the increasing demands of modern and safe communication networks.

The first chapter introduces the basic concept of information security, with focus on the cryptographical solutions. Then, a theoretical background of Physical Layer Security is provided, in order to understand the foundations it relies on, including its mathematical background, to prove that Physical Layer Security relies on strong mathematical foundations. In the second chapter, an analysis of the wireless channel spatial correlation is provided, employing both measurements and theoretical models. This study wants to highlight that spatial correlation follows the well known Jake's model only in a limited number of situations. The analysis is followed by a simulative work on the secure key generation in real like situations, aiming at giving a complete study on the impact of real propagation conditions on key generation from wireless channel. In the last chapter, the focus is put on securing the wireless channel using the geofencing concept. In particular, the Frequency Diverse Array concept is proposed and analysed

for secure communications. First, a general discussion on the capability of Frequency Diverse Arrays is provided, then an analysis on their actual advantages is presented.

1

Physical Layer Security

This chapter outlines the main issues about the security of data communication, with a focus on wireless communication. In particular, the fundamentals of communications security are introduced first, then the concept of Physical Layer Security (PLS) is described.

During the past decades, the number of connected wireless devices experienced a huge increase. In particular, with the introduction of Internet Of Things (IOT) paradigm, people started using more and more connected devices: smart home applications, smart cities or medical devices [1] are being installed thanks to the progress in wireless communications. As the number of connected devices increases, the number of cyberattacks upsurges as well. In [2] it is reported that 56% of internet consumers have experienced a cyber crime, and 46% of them lost money from the attack: in spite of this increasing number, security is still not seen as a big issue by people and companies.

Wireless communications require a specific effort for security: the wireless channel is inherently broadcast and might suffer many types of attacks [3], thus it requires ad hoc solutions to secure communications. In fact, wireless devices are usually battery powered (e.g. laptops, smartphones, sensors, etc.) and depending on their applications, they might have limited computational power and constrained battery consumption. Hence, they might not be able to run complex security algorithms that are suitable for plugged in devices. For these reasons, there is a need to come up with new solutions for wireless communications, that take into account the specific characteristics of the wireless channel.

1.1 Introduction to Information Security

In general, a secure transmission should meet four *security traits*:

- **Authenticity**: concerns transmitters and receivers proof of identity.
- **Availability**: refers to the capability of authorized users to access and utilize information when needed. Or, to make sure that the wireless communication

resources are always available to the assigned user, i.e. not jammed.

- **Confidentiality**: refers to the restriction of data access to the designated users exclusively to ensure that no one else has access to the information.
- **Integrity**: ensures that any information shared is received truthfully and without modification or fabrication.

Indeed, wireless networks are especially vulnerable due to the shared nature of the wireless medium, necessitating additional efforts and specific solutions for their safety. Moreover, a malicious user might be able to carry out two different types of attacks:

- **Passive attack**: an attempt to intercept the conversation with the intention of stealing the data being transferred across the channel. In this case, the attacker does not interact with the communications.
- **Active attacks**: the attackers actively interact with the communication aiming at disrupting the communication (e.g. Denial of Service, Jamming), assuming the identity of other legitimate users, modify the content of exchanged messages (hence disrupting the Integrity of Communication).

1.1.1 Cryptography

Security threats are mostly tackled using *cryptography*, the branch of computer science which studies the techniques for a secure communication between two users [4, 5]. In particular, there are two main techniques employed for cryptography: *symmetric encryption* and *asymmetric encryption*. Cryptography makes use of known standard algorithms and protocols, based on a secret key (symmetric) or a pair of keys (asymmetric): once the message is encrypted, only the users in possession of the right key will be able to decrypt the message and retrieve the original message. Cryptographic techniques often exploit complex mathematical computation and are referred to be *computationally secure*: a user with enough computational capacity, even if they do not have the right key, might be able to revert the algorithm employed, or guess the key by means of a lot of trials (brute force attack). Of course, this situation is not really possible since algorithms are designed such that modern computers will take an infeasible time to break the security (something like hundreds of years). In fact, in order to invert the algorithms the attacker has to solve complex mathematical problems like *discrete logarithm* [6, 7] and *prime number factorization* [8, 9], which present computers are not able to solve in a feasible time. However, this condition may not be true any more in the future with the introduction of *quantum computers*, which are expected to have a huge computational capacity. Research in the field of cryptography is pushing toward *quantum resistant* algorithm, *information-theoretic security* and *quantum secure communications* [10–12].

Every cryptographic solution requires the presence of a random, secret key. There are three main properties to be addressed:

- The key must be random, generated through a True Random Generator, to be

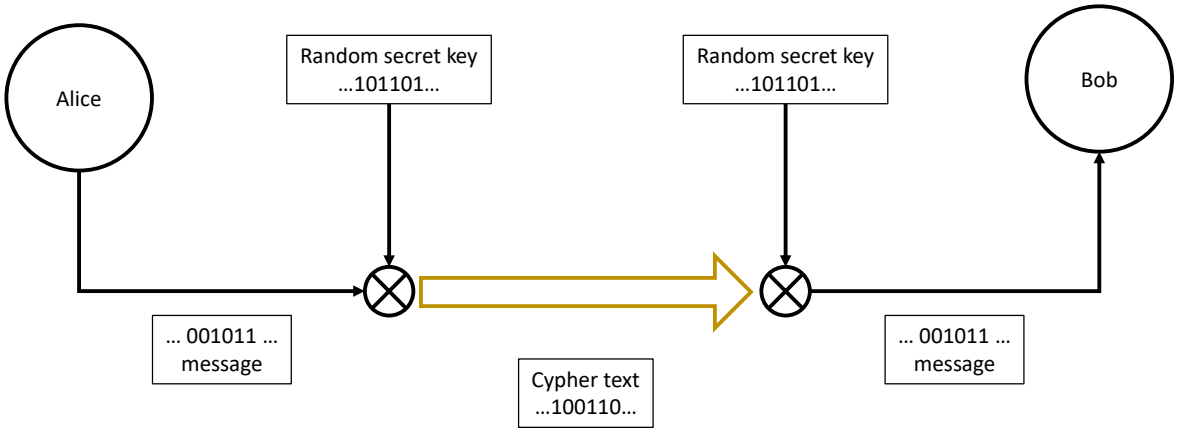


Figure 1.1: Scheme of One Time Pad mechanism.

difficult to guess.

- The key should be changed frequently since even small information about the secret key can disrupt the confidentiality of the communication.
- The key should be long enough in order to match the target security level.

The randomness requirement is the most challenging one, especially when the key has to be shared between the users after the generation. In fact, even though a secret random key might be generated, it would be insecure to share it through a public channel, since it might get intercepted. To solve this problem, the Diffie-Hellman (DH) algorithm has been proposed [7], which allows two users to agree on a private random key over an insecure channel, without sharing any information. However, this method generates computationally secure keys, since its security relies on the difficulties of computing discrete logarithm problem [6].

In 1919 G.S. Vernam introduced the concept of One Time Pad (OTP) [13], a security mechanism that allows to reach *perfect secrecy*. A simple scheme of OTP is shown in Figure 1.1: first, Alice generates a message, represented as a sequence of bits, and she encrypts it through a bit-wise `xor` between the key and the message itself. When Bob receives the text he will perform the same operation using the same key as Alice, and recover the original plain text. For OTP to be unbreakable the key must follow these rules:

- The key must be at least as long as the message to be encrypted.
- The key must be random.
- A key must be used only once.
- The key must be kept secret.

However, OTP is not suitable for practical applications, since it requires a very long key that has to be exchanged in advance between the users.

OTP falls in the family of symmetric cryptography solutions, where two users can

securely communicate thanks to the knowledge of a shared secret key, which is the same between the two users. It is worth noticing that symmetric cryptography allows to achieve the confidentiality requirements by means of simple and efficient algorithms, which do not utilize too much power. The current standard for symmetric encryption is Advanced Encryption Standard (AES), an implementation of the Rijndael algorithm [14, 15]. The algorithm employs a series of permutation and substitution, which takes as input data blocks with dimension between 128 and 256 bits, allowing only multiple of 32 bits. Each operation is influenced by the encryption key, which can be of 128, 192, or 256 bits. AES implements the same algorithm but allows only data blocks of 128 or 256 bits.

Instead, asymmetric cryptography utilizes a pair of keys for each user, one *public* and the other *private*. In particular, the public key is shared among all the users and is globally available, and the receiver's user public key is used to encrypt the message: the private key, known only to the receiver, is then used to decrypt the message. This solution allows the users to achieve all the security traits, but complex and energy-consuming algorithms have to be employed. One of the most popular algorithm for asymmetric encryption is the Rivest-Shamir-Adleman (RSA) algorithm [8], which relies on the difficulty of factoring a big number into two prime numbers. RSA allows generating the pair of public and private key, and to encrypt the message through exponentials and modulus operations employing the key. However, the security of RSA has been questioned, since it has been proven not to be secure against quantum attacks [16]. Instead, the standard for symmetric encryption AES is resistant against quantum attacks in case the employed key is 256 bits [17].

1.1.2 Wireless Communications Security Challenges

With the proliferation of wirelessly connected devices, there is a need of security solutions that take into account the specific characteristics of the wireless channel: for example, the wireless channel is exposed to eavesdropping attacks [3], Fake Base Station attacks [18, 19], fake user intrusion [20]. Moreover, recently the O-RAN paradigm is becoming popular [21], which introduces even more threats [22]: O-RAN aims at disaggregating and opening up the Radio Access Network, enabling greater flexibility, interoperability, and innovation in network deployments, through cloud implementation and virtualization of the RAN hardware and software, intelligent management and open interfaces between the different parts of the RAN including front haul to the physical radio unit.

With the recent advance of IOT technology [23–25], it has been possible to integrate technologies into people's life and work: smart environment, smart industry, and smart healthcare are just a few examples. In particular, as people and objects are more connected, the amount of private and confidential data is increasing too, leading to possible outbreaks of data leaked online.

Although classical cryptography is a powerful solution that still protects modern inter-

net communications, there are new challenges facing the security of wireless communications. Moreover, security techniques have to keep up with the increasing strength of malicious attacks, hence they are becoming more complex and requiring more computational power, which might not be feasible for simple, battery powered IOT devices.

Eventually, there is the need to come up with specific solutions for wireless communications security, which take into account the characteristics of the channel and the connected devices.

1.2 Physical Layer Security Solutions

PLS refers to a family of techniques that enables security mechanisms at the physical level. In particular, they exploit the unpredictable features of the wireless channel (e.g. time/frequency/space fading) to protect communications. PLS is inspired by Shannon's pivotal work about the communication theory of secrecy systems [26]. In particular, Shannon introduced the concept of *information-theoretic security*, or *perfect secrecy*, in which the confidentiality of a message cannot be broken since the attacker is not endowed with enough information about it. This can be formulated as follows: suppose to have a message M to be transmitted and an encryption mechanism. Then, it is possible to encode the message into a codeword C such that the knowledge of C does not bring any information about the initial message. This can be formulated as:

$$\mathbb{H}(M|C) = \mathbb{H}(M), \tag{1.1}$$

where $\mathbb{H}(\cdot)$ indicates the entropy.

PLS aims at achieving perfect secrecy by exploiting the random characteristics of the wireless channel. There are two main solutions for PLS:

- Key-less: the transmitted messages are encoded with specific codes that ensure both confidential and reliable communications.
- Key-based: users are able to agree on a common secret encryption key that will be used along with one of the common encryption algorithms (e.g. AES).

1.2.1 Key-Less Solutions

Key-less security is capable of achieving perfect secrecy without encrypting the message, whose pioneer was A.D. Wyner who published his work about the *wire-tap channel* [28] and introduced a new condition for perfect secrecy.

Consider the model depicted in Figure 1.2. Alice wants to reliably send data toward Bob while keeping confidentiality of the data. At the same tame, an eavesdropper Eve wants to intercept the message sent by Alice. Alice encodes her message M into a codeword X^n which is then sent to Bob through a noisy wireless channel. Bob receives the codeword Y^n, a noisy observation of X^n. Since the wireless channel is inherently

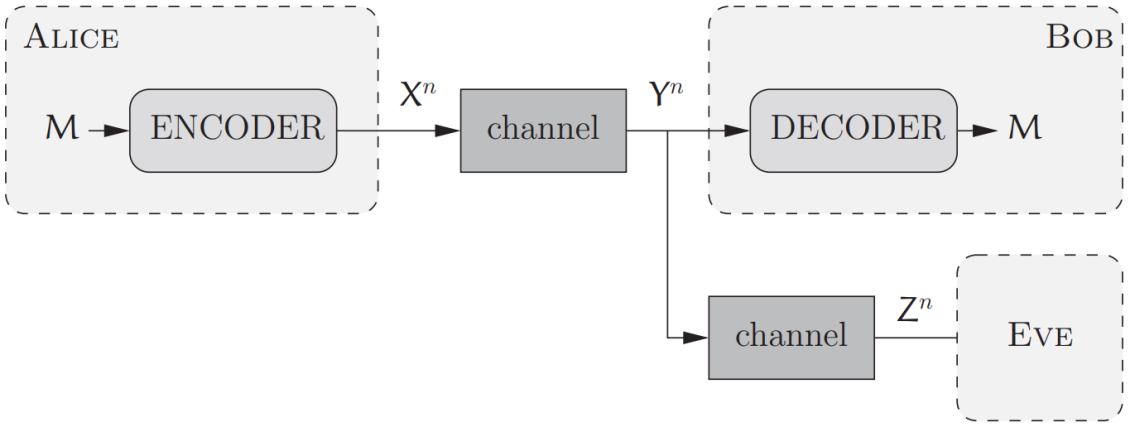


Figure 1.2: General case of the Wyner's wire-tap channel, with two users and one eavesdropper. Picture from [27].

broadcast, the message arrives to Eve who observes Z^n, a noisy observation of Y^n. Wyner introduced the concept of **equivocation rate** $\left(\frac{1}{n}\right)\mathbb{H}(M|Z^n)$ which must be arbitrarily closed to the entropy of the message $\left(\frac{1}{n}\right)\mathbb{H}(M)$ [27]. Similar to (1.1), the condition for perfect secrecy can be formalized in this way:

$$\left(\frac{1}{n}\right)\mathbb{H}(M|Z^n) \underset{n\gg 1}{\longrightarrow} \left(\frac{1}{n}\right)\mathbb{H}(M). \tag{1.2}$$

The model in (1.2) suggests the existence of a set of codes that *asymptotically* achieve perfect secrecy, and including Shannon's theory about communications, they can also achieve arbitrarily small error probability: such codes are known as *wiretap codes*.

Starting from the model in (1.2), in [29] the concept of **secrecy capacity** C_s has been introduced. With respect to Figure 1.2, suppose that the Alice-Bob channel has a capacity C_{AB} and the Alice-Eve channel has a capacity C_{AE}, the secrecy capacity C_s is defined as:

$$C_s = C_{AB} - C_{AE}. \tag{1.3}$$

C_s indicates the amount of information that can be securely exchanged on the channel without any possibility for the eavesdropper to decode the message.

Artificial Noise-Aided Security

An example of key-less security implementation can be *Artificial noise-aided security*: it is a technique that uses both *beamforming* and interfering signals to increase the secrecy capacity. Considering the previous model, suppose that Alice is equipped with a directive antenna and implements a beamforming algorithm, as shown in Figure 1.3: the main lobe will be directed toward the direction of Bob, while Eve receives the communication from the side lobes. In this way, most of the power will be directed

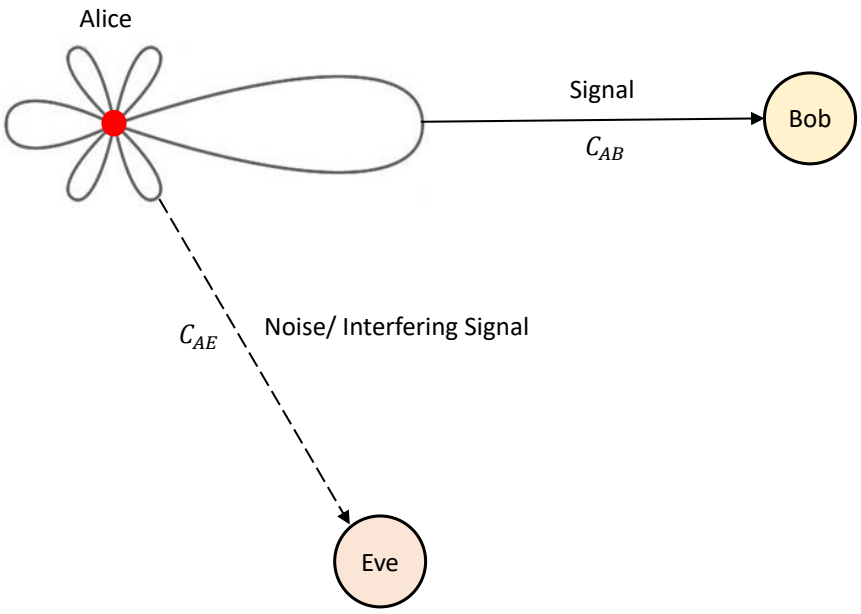


Figure 1.3: Artificial noise aided scheme.

toward Bob and Eve will experience a low Signal to Noise Ratio (SNR). Moreover, it is possible for Alice to send through the side lobes an interfering signal, or directly noise, in order to further reduce the SNR at Eve's side. In the end, the Alice-Eve capacity (C_{AE}) will be irrelevant compared to the Alice-Bob capacity (C_{AB}), which leads to a high secrecy capacity. In [30] a solution for jointly optimizing power allocation and noise in the beams is presented. Eventually, this method follows the model for perfect secrecy, since it will be impossible for Eve to decode the signal.

However, in the case of a dynamic channel it would be difficult to follow the variation of the capacity and adapt the communication rate to respect the bound of C_s. Furthermore, determining the eavesdropper's channel capacity is not straightforward.

1.2.2 Key-Based Solutions

Physical Layer based-Key generation (PLKG) aims at providing a protocol to autonomously generate a symmetric encryption key between two users, and it exploits the randomness inside the wireless channel to extract random bits. Small-scale fading is a good candidate as a source of randomness since it varies on a small spatial scale and changes fast in time, space and frequency, due to the mobility of the terminals or of the objects inside the environment. In order to extract the randomness, the two users initiate a public discussion over the channel and by means of pilot signals they observe the random fluctuations of the fading.

The multipath channel (Figure 1.4) can be modelled as a superposition of several components and the Channel Impulse Response (CIR), $h^{ab}(\tau, t)$, from transmitter a (Alice) to receiver b (Bob) can be written as:

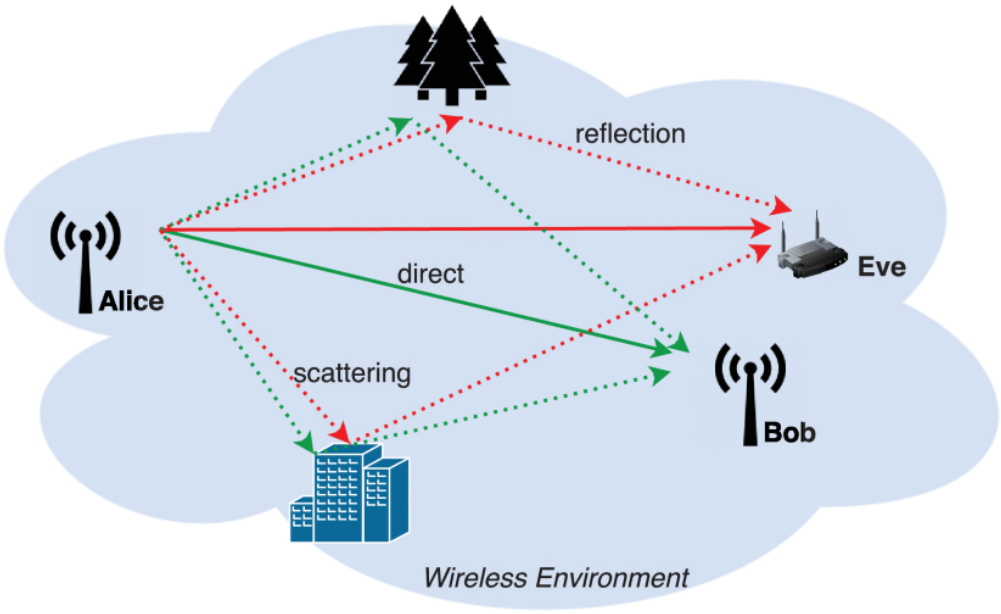


Figure 1.4: Multipath effect inside the channel. The multipath configuration changes in the different points and varies in time in case the objects in the channel move. Picture from ©2020 IEEE [3].

$$h^{ab}(\tau,t) = \sum_{l=1}^{L^{ab}(t)} \alpha_l^{ab}(t) e^{-j\phi_l^{ab}(t)} \delta\left(\tau - \tau_l^{ab}(t)\right), \tag{1.4}$$

where $\alpha_l^{ab}(t)$ is the amplitude attenuation of the l-th path, $\phi_l^{ab}(t)$ the phase shift, $L^{ab}(t)$ the total number of paths, $\delta(\cdot)$ is the Dirac function, t represents the time while $\tau_l^{ab}(t)$ the propagation delay. Then, if a signal $s(t)$ is transmitted via the multipath channel, the received signal $y(t)$ is given by the convolution:

$$y(t) = \int_0^{\tau_{max}} h^{ab}(\tau,t) s(t-\tau)\, d\tau \; + \; n^b(t). \tag{1.5}$$

where $n^b(t)$ is the noise at the receiver and τ_{max} is the maximum delay of the echoes.

The same can be written in frequency considering the Channel Transfer Function (CTF) $H^{ab}(f,t)$, which is the Fourier transform of the CIR, $H^{ab}(f,t) = \mathscr{F}\left[h^{ab}(\tau,t)\right]$:

$$Y(f,t) \; = \; H^{ab}(f,t) S(f,t) \; + \; w^b(f,t), \tag{1.6}$$

with $S(f,t)$ and $Y(f,t)$ the spectrum of the transmitted and received signals.

The spatial distribution of reflectors and scatterers in the channel determines its randomness by changing the multipath configuration. PLKG wants to observe the features of the channel and use them as a source of randomness.

Key generation leverages the following (expected) properties of the wireless channel:

- **Channel reciprocity**: the channel gains and phase shifts don't change if Alice and Bob exchange their role (from transmitter to receiver, or vice versa), provided

that this happens within the channel coherence time. In this way, every pair of legitimate users can extract the same information from the channel. Channel reciprocity holds in case the system employs a Time Division Duplexing solution, as long as the legitimate users sample the propagation channel within the same *fading coherence time*. Instead, with Frequency Division Duplexing the channel might not be reciprocal any more, and key generation becomes thorny: some hints can be found in [3].

- **Spatial decorrelation**: in general, the spatial auto-correlation of fading decreases with distance and becomes negligible after a proper coherence distance. According to Jake's model, in a rich multipath scenario the fading samples are decorrelated after a distance of about 0.4λ.
- **Fading randomness**: due to multipath and mobility, channel properties (e.g. Received Signal Strength (RSS), CTF) undergo random-like fluctuations in the spatial / frequency / temporal domain, to an extent that is usually related to the degree of "multipath richness". The greater the multipath effects, the more the channel appears as random.

1.2.3 Information Theory of Key Generation

PLKG is proven to be information-theoretically secure in [31] and [32]. Consider the model illustrated in Figure 1.5 (which will be the reference model in the following): in order to extract the random key, Alice and Bob have to exchange some information s over the public channel, which can be overheard by Eve. Alice, Bob and Eve acquire the channel observations $X^A = [x^A(1), x^A(2), \cdots, x^A(n)]$, $X^B = [x^B(1), x^B(2), \cdots, x^B(n)]$, $X^E = [x^E(1), x^E(2), \cdots, x^E(n)]$. For any ε and sufficiently large n there exists a key generation protocol $K_{ir}^A = g_A(X^A)$ and $K_{ir}^B = g_B(X^B, s)$ which satisfies ([3]):

$$P(K_{ir}^A \neq K_{ir}^B) < \varepsilon, \tag{1.7}$$

$$\frac{1}{n}\mathbb{I}(K_{ir}^A; s, X^E) < \varepsilon, \tag{1.8}$$

$$\frac{1}{n}\mathbb{H}(K_{ir}^A) > R - \varepsilon, \tag{1.9}$$

$$\frac{1}{n}\log_2|\mathcal{K}| < \frac{1}{n}\mathbb{H}(K_{ir}^A) + \varepsilon, \tag{1.10}$$

where $\mathbb{H}(\cdot)$ is the entropy, $\mathbb{I}(\cdot)$ denotes the mutual information, and $\mathcal{K}$ is the key's alphabet. R is the achievable key rate: the maximum rate at which Alice and Bob can agree on a secret key while keeping the rate at which Eve obtains information arbitrarily small [32]. In practice:

- (1.7) represents the channel reciprocity: Alice and Bob can get the same key with a high probability.
- (1.8) represents the spatial decorrelation: Eve cannot infer the key based on her observation of the public discussion.

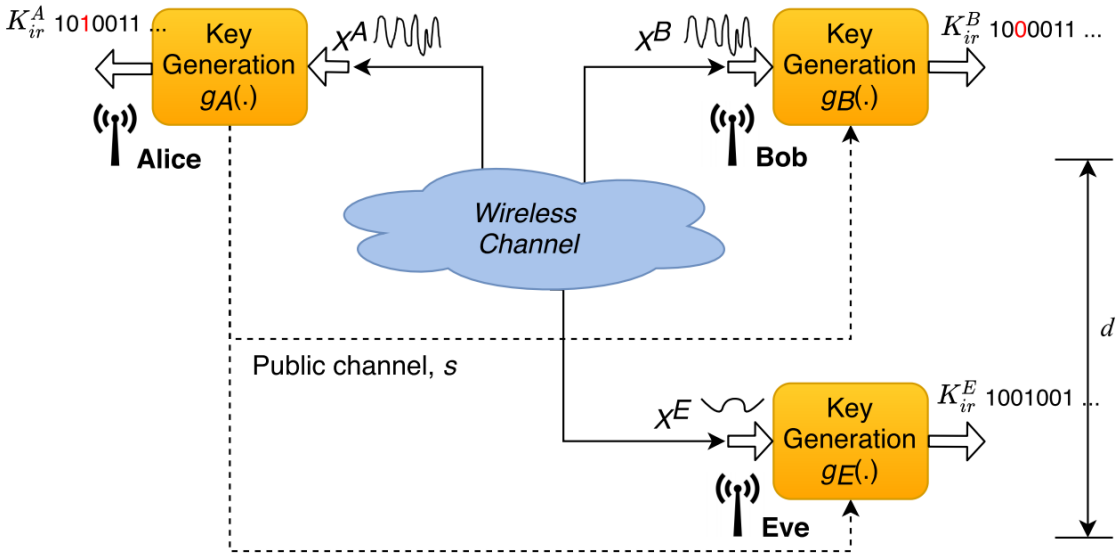


Figure 1.5: PLKG model. Alice and Bob want to generate a common key from the wireless channel, Eve wants to observe the same channel and try to extract the same key. However, thanks to the spatial decorrelation properties, Eve will unlikely extract the same key, since the observations are different from the ones of Alice and Bob. Picture from ©2020 IEEE [3].

- (1.9) refers to the capability of generating the key while preventing Eve to steal useful information: for sufficiently large n it is possible to achieve the maximum key rate.
- (1.10) represents the temporal variability, which ensures having a uniformly distributed key.

1.2.4 Physical Layer-Key Generation Protocol

In general a PLKG protocol relies on 4 main stages, as shown in Figure 1.6:

- **Channel probing**: in this phase Alice and Bob exchange some information to measure the channel and observe the random features.
- **Quantization**: both users quantize the features observed to extract a random sequence of bits.
- **Information reconciliation**: Alice sends to Bob a public message in order for Bob to correct possible mismatch in the string of bits.
- **Privacy amplification**: both users perform some operation on the bit sequence to improve the randomness and produce a usable key.

In the end, Alice and Bob are able to generate the same key and use it for encryption. In the following, a detailed explanation of the main phases is provided.

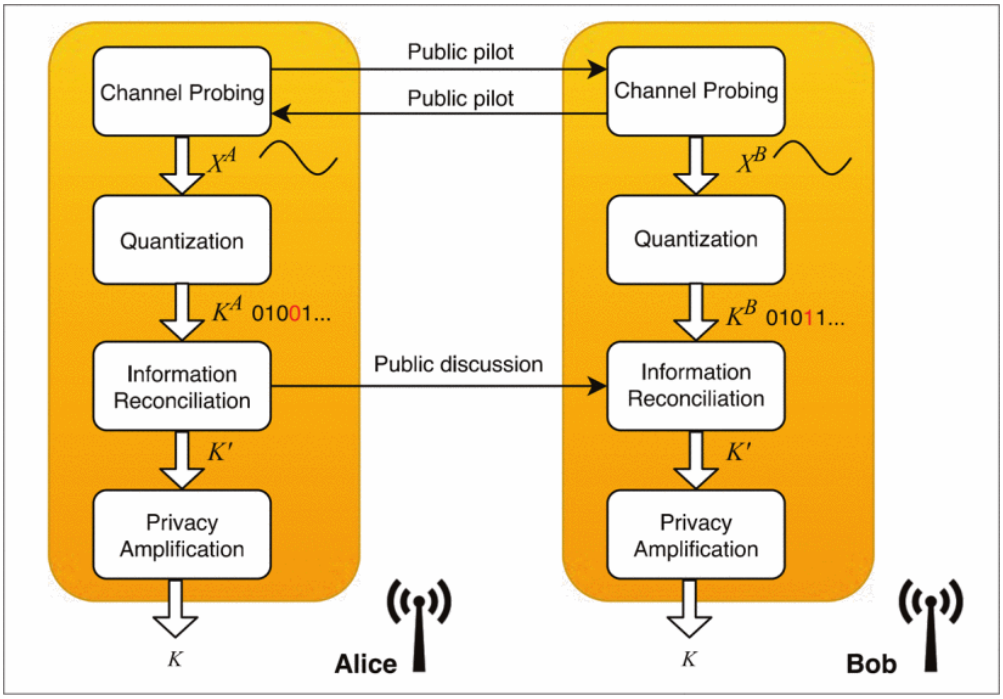


Figure 1.6: Scheme of the key generation protocol. Picture from ©2019 IEEE [33].

Channel Probing

Alice and Bob alternately measure the common channel through the exchange of dummy packets. The goal of this part is to observe the features of the channel in order to harvest entropy from it: features can be observed in time and/or frequency domain. This step highly determines the key generation time. In fact, a system using the fading fluctuation in time will have to probe the channel many times and with a certain delay greater than the coherence time of the fading. Features commonly employed are:

- Radio Signal Strength Indicator (RSSI): this quantity is already available in many IOT system like LoRA or IEEE 802.15.4. The RSSI is a measure of the received power of the packet, and it is computed for each packet. This feature changes in time thanks to the fading fluctuation due to mobility in the channel. A system using the RSSI as feature will take some time to generate the key and the users will have to exchange a lot of packets to have enough bits for the key.
- Channel State Information (CSI): this is a fine-grained quantity which can generate more information than RSSI. CSI can be either the CIR $h^{ab}(\tau, t)$ or the CTF $H^{ab}(f, t)$. Moreover, it is a complex quantity and contains both the amplitude and the phase of the channel. In addition, while the RSSI is a narrowband quantity, CSI can take into account the dispersive properties of the channel, which means that can take advantage from the time/frequency selectivity of the channel. For example, Orthogonal Frequency Division Modulation (OFDM) systems already estimate the CSI in order to equalize the transmission, although usually, this information was not readily available and thus usable. With reference to the

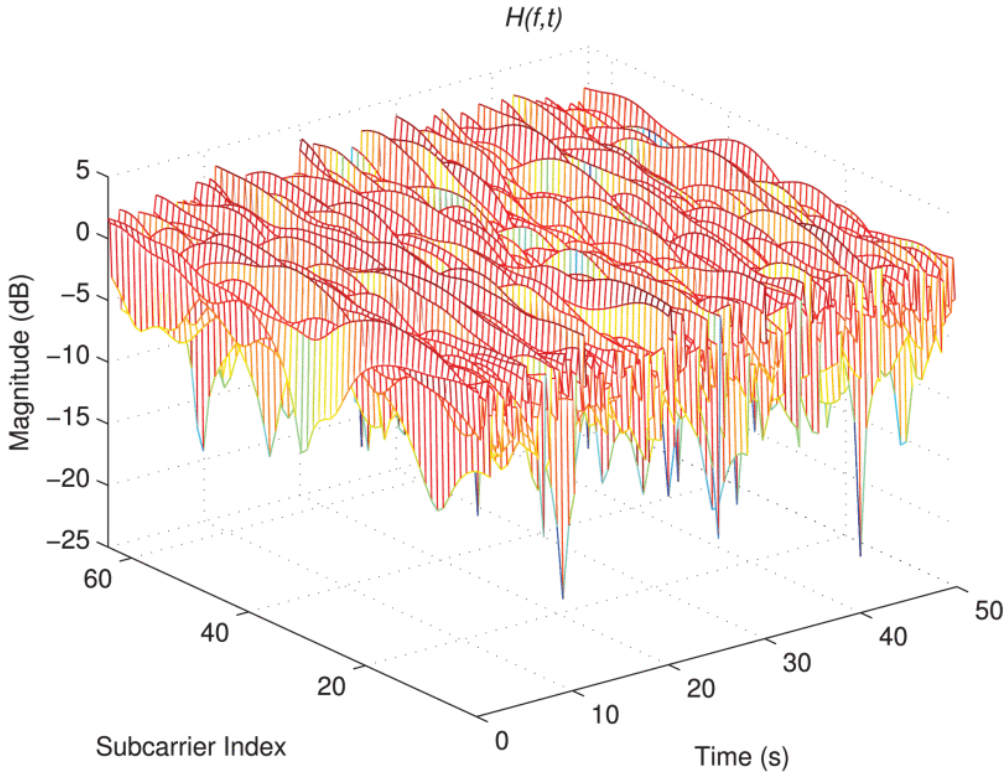


Figure 1.7: CTF of OFDM signals. CTF varies in frequency and time, which allows taking advantage of both characteristics. Picture from ©2020 IEEE [3].

equation (1.6), simple estimation can be formulated as:

$$\widehat{H}^{ab}(f,t) = \frac{Y(f,t)}{S(f,t)} = H^{ab}(f,t) + \hat{w}^{b}(f,t). \tag{1.11}$$

In case the original signal $S(f,t)$ is a known pilot signal. For the sake of this project, the CTF will be mainly referred to. In case the CTF is used, it is possible to exploit both time and frequency variability. As shown in Figure 1.7, IEEE 802.11 OFDM signals can take advantage of both frequency and time in order to generate more bits for the key.

Although most common methods for PLKG are usually based on RSSI, on the CTF (see [34] in particular Table 2) or the CIR (see [35]), any other propagation marker can be used to harvest entropy from the channel, provided that it is symmetric between the two users, and it is random: for example, there has been a proposal that takes advantage from the Doppler Effect as a source of randomness [36]. Moreover, channel Probing leverages channel reciprocity: the channel is almost reciprocal in case the communication system employs Time Division Duplexing (TDD). In case Frequency Division Duplexing (FDD) is adopted, the channel might not be the same over the two frequencies. Therefore, specific effort must be put into action in case of FDD. A comprehensive description of the problem of FDD can be found in section V of [3], since it is out of the scope of this work.

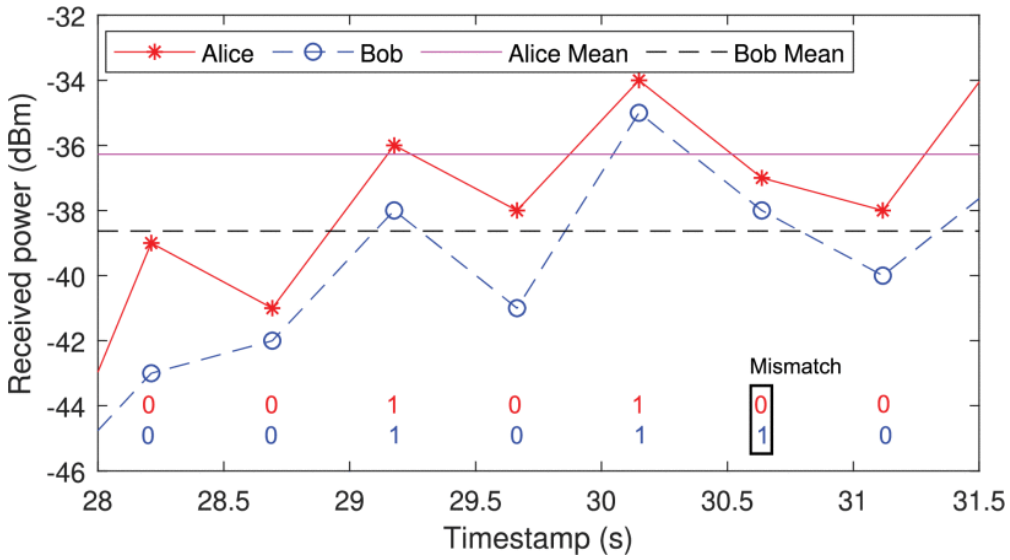


Figure 1.8: Mean and Standard Deviation-Based Quantization. Picture from ©2020 IEEE [3].

Quantization

The features extracted from the channel are analogue quantities: in order to create a string of bits, the analogue values must be quantized into digital values, similarly to what is done with an analogue to digital converter. With reference to Figure 1.6, after the channel probing phase Alice and Bob come up with the channel observation X^A and X^B, the quantization phase produces the sequence K^A and K^B. Two simple quantization algorithms can be employed: Absolute Value Based-Quantization and Differential-Based Quantization [37, 38].

Absolute Value Based-Quantization uses some threshold computed based on the statistics of the observation. A simple mechanism can be the *Mean and Standard Deviation-Based Quantization*: the users compute the mean value μ and the standard deviations σ of the channel samples. Then, they compute two thresholds:

$$\eta_+ = \mu + \alpha \times \sigma, \tag{1.12}$$

$$\eta_- = \mu - \alpha \times \sigma, \tag{1.13}$$

where α is a parameter to be tuned: what falls between η_+ and η_- is discarded, what is above η_+ is quantized in a 1 and what is below η_- is a 0. In case $\alpha = 0$, the two thresholds coincide, which is the situation depicted in Figure 1.8.

A more advanced quantization scheme is the *Cumulative Distribution Function Based Quantization* [39]: it envisages also the possibility of using multiple threshold to have multi-bit quantization [40], the thresholds are computed based on the Cumulative Distribution Function of the observations. In order to map the bit to the quantization levels, Grey Code is used to reduce the mismatch between the quantization of Bob and Alice.

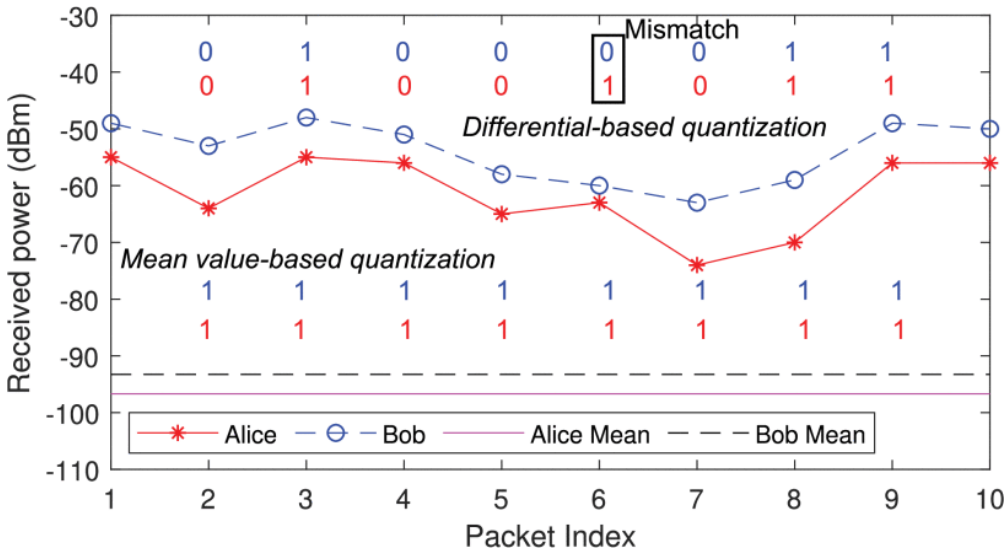


Figure 1.9: Differential-Based Quantization compared to Mean and Standard Deviation-Based Quantization. Here, the discrimination between 0 and 1 stands in the difference between two consecutive values. Picture from ©2020 IEEE [3].

In **Differential-Based Quantization** no threshold is employed. Instead, the choice between 0 and 1 stands in the difference between two consecutive channel samples. Let's consider the case in which Key Generation utilizes the RSSI: Alice and Bob exchange many packets in time and measure the RSSI from each one. Then, they look at two consecutive power values: if the current sample is greater than the previous one, a 1 is produced, instead a 0 is produced. Furthermore, usually an additional margin is considered in order to protect from possible fluctuations of the noise. In terms of algorithm it can be written as in Algorithm 1.

Algorithm 1 Differential-Based Quantization Algorithm

```
if x(i) > x(i − 1) + ϵ then
    K(i) = 1
else
    if x(i) < x(i − 1) − ϵ then
        K(i) = 0
    end if
else
    x(i) is discarded
end if
```

This method is suitable for channels with low variability: in fact, even a small variation of the channel results in a different bit, which may not be true in the Absolute Value Based-Quantization. At the end of the quantization, Alice and Bob produces the keys K_q^A and K_q^B.

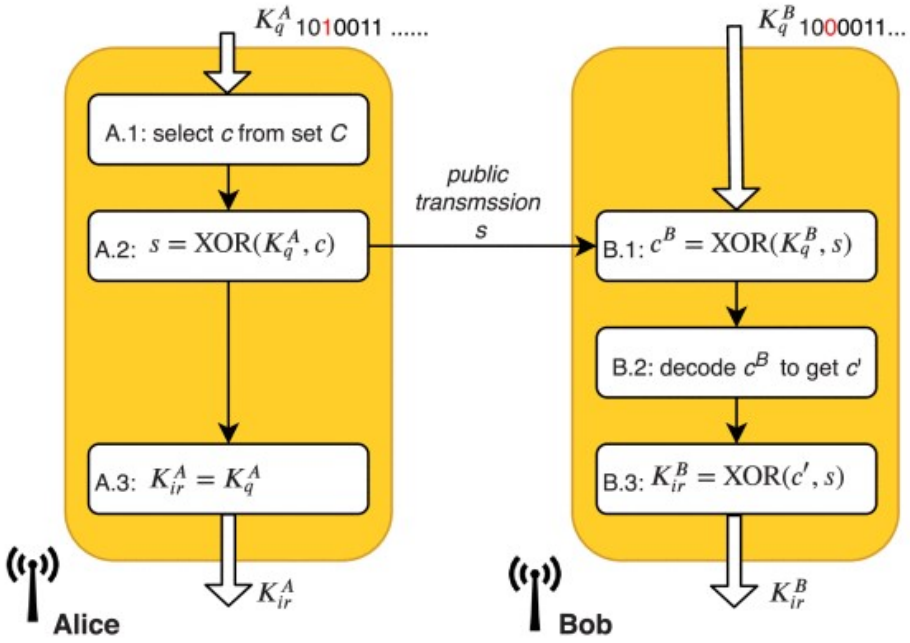


Figure 1.10: Scheme of Information Reconciliation. Picture from ©2020 IEEE [3].

Information Reconciliation

Despite channel reciprocity, the extracted features may be slightly different, which results in possible mismatch between the two generated keys: errors are caused by thermal noise, not perfect channel reciprocity, possible interferences and hardware imperfections. The Information Reconciliation phase allows the users generating the key to correct the errors in the key via a public discussion. A comprehensive summary of the possible schemes can be found in [41].

Reconciliation is a specific case of Forward Error Correction (FEC), and it can be implemented by using Bose-Chaudhuri-Hocquenghem (BCH) codes, Reed-Solomon, turbo codes, polar codes, LDPC codes. The choice of the code impacts the reconciliation effectiveness: in fact, it is equal to the error correction capability of the code. As an example, a BCH(n, k, t) has an n-bit codeword, a k-bit message and can correct up to t errors: a BCH(15, 3, 3) can correct 20 percent mismatch. In case the errors in the key are larger than the reconciliation capability of the code, the keys cannot be corrected. Moreover, it is worth mentioning that the Reconciliation methods, but also Privacy Amplification, are borrowed from the Quantum Key Distribution [42]. First, Alice and Bob must agree on a code to be used and a codebook C. Then, as shown in Figure 1.10, the reconciliation works as follows:

1. Alice selects a random codeword c and sets $K_{ir}^A = K_q^A$.
2. Alice computes $s = \texttt{XOR}(K_q^A, c)$ and sends it to Bob.
3. Bob receives s and computes $c^B = \texttt{XOR}(K_q^B, s)$
4. Then Bob decodes the codeword c^B into a codeword c', which is the original

codeword c chosen by Alice

5. In the end, Bob can generate the reconciliated key $K_{ir}^{B} = \texttt{XOR}(K^{B}, c')$

Privacy Amplification

During the key generation process there is an exchange of public information: during the channel probing the pilot signals, but also the codeword exchanged during the Information Reconciliation phase. For this reason, the privacy amplification is a mandatory phase to protect against possible information leakage. In fact, from the public discussion Eve may be able to infer the key, or at least identify some bits of the key. Even gaining the knowledge of few bits represents a negative occurrence, since it reduces the search space in case Eve performs a *brute force attack*.

Privacy amplification employs the so-called *universal hash families*, such as the *leftover hash lemma* [43], the *cryptographic hash function* [44] and the *Merkle-Damgård hash* [45]. Therefore, it distils a shorter key from the one generated after the Information Reconciliation, in order to reduce Eve's attack capability and to spread the entropy along the key. Hence, Alice and Bob might want to generate a longer key from the previous phase, which is then shorted but still a usable and secure key (e.g. with 256 bits).

1.2.5 Evaluation Metrics of Key Generation

First, it is possible to compute the cross-correlation (also called the *Pearson coefficient*) to evaluate the similarity between the measurements of two users a and b (e.g. Alice-Bob or Bob-Eve):

$$\rho^{ab} = \frac{\mathbb{E}\{X^a X^b\} - \mathbb{E}\{X^a\}\mathbb{E}\{X^b\}}{\sigma^a \sigma^b}. \tag{1.14}$$

Of course, a high correlation between Alice and Bob's samples is desired, while a small one should be found between Bob and Eve's samples.

Then, Autocorrelation Function (ACF) is used to quantify the correlation among the channel samples. If the channel is represented by the random process $X(t)$, then the ACF is written as:

$$r(t, \delta t) = \frac{\mathbb{E}\{(X(t) - \mu)(X(t + \delta t) - \mu)\}}{\sigma_u^2}, \tag{1.15}$$

where μ is the mean value of $X(t)$.

Another important metric is the Key Disagreement Rate (KDR): it quantifies the mismatch between the keys generated by two users after the quantization phase K_q^a and K_q^b [46]. It is expressed as:

$$\mathrm{KDR}^{ab} = \frac{\sum_{i=1}^{n_k} |K_q^a(i) - K_q^b(i)|}{n_k}. \tag{1.16}$$

This quantity should be less than the correction capacity of the code used in the information reconciliation phase.

Secrecy Key Rate (SKR) is the upper bound of the number of bits per channel observation that Alice and Bob can extract from the channel, without the possibility for Eve to obtain any useful information. Of course, this is the theoretical limit, and it should be interpreted in the same way as the channel capacity defined by Shannon. Maurer provided an upper and lower bound for the SKR [32]:

$$R(X^A, X^B \parallel X^E) \geq \max[\mathbb{I}(X^A; X^B) - \mathbb{I}(X^A; X^E),\, \mathbb{I}(X^A; X^B) - \mathbb{I}(X^B; X^E)], \tag{1.17}$$

$$R(X^A, X^B \parallel X^E) \leq \min[\mathbb{I}(X^A; X^B),\, \mathbb{I}(X^A; X^B \mid X^E)]. \tag{1.18}$$

Instead, Key Generation Rate (KGR) is the actual number of bits that can be generated in a unit of time using a specific key generation method: it is usually measured in bit/s. A well-designed protocol can achieve a KGR close to the SKR.

Eventually, since the generated key is employed in a symmetric encryption scheme, it is important to verify its randomness, in order to prevent cryptanalytic attacks (attacks that aim at analysing encrypted data to find possible pattern due to not perfect random nature of the employed keys). National Institute of Standards and Technologies (NIST) [47], an agency of the United States Department of Commerce, provides a suite of fifteen tests used to evaluate the randomness of a *random number generator*. The suite of tests provided by the NIST is considered the standard set of tests to analyse the randomness of a sequence. Each test returns a P-value which is compared to a statistical significance level α: in case the P-value $> \alpha$ the test is passed. Moreover, some tests require long sequences of bits to evaluate the randomness. A summary of the test is shown in Figure 1.11.

Test	Purpose	Recommended key size n_k
Frequency (monobit) test	Proportion of zeros and ones for the entire sequence	100
Frequency test within a block	To determine whether the frequency of ones in an M-bit block is approximately $M/2$	100
Runs test	Total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits	100
Longest run of ones in a block test	Longest run of ones within M-bit blocks	n_k=128, M=8
Binary matrix rank test	Check linear dependence among fixed length substrings of the original sequence	38,912
Discrete fourier transform (Spectral) test	To detect periodic features(i.e., repetitive patterns that are near each other)	1000
Non-overlapping template matching test	To detect generators that produce too many occurrences of a given non-periodic (aperiodic) pattern	Not specified
Overlapping template matching test	To detect generators that produce too many occurrences of a given non-periodic (aperiodic) pattern	10^6
Maurer's universal statistical test	To detect whether or not the sequence can be significantly compressed without loss of information	387,840
Linear complexity test	To determine whether or not the sequence is complex enough to be considered random	10^6
Serial test	The frequency of all possible overlapping m-bit patterns across the entire sequence	Choose m and n such that $m < \lfloor(\log_2 n_k - 2)\rfloor$
Approximate entropy test	To compare the frequency of overlapping blocks of two consecutive/adjacent lengths(m and m+1) against the expected result for a random sequence	Choose m and n such that $m < \lfloor(\log_2 n_k - 5)\rfloor$
Cumulative Sums test	The maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (-1, +1) digits in the sequence	100
Random excursions test	The number of cycles having exactly K visits in a cumulative sum random walk	10^6
Random excursions variant test	To detect deviations from the expected number of visits to various states in the random walk	10^6

Figure 1.11: Summary of the NIST random test. Picture from ©2020 IEEE [3].

1.3 Physical Layer Security Challenges

In the end, PLS seems a promising solution for enhancing secure communication systems, leveraging the properties of the physical medium itself, rather than relying solely on cryptographic methods at higher layers. However, as reported in [48], there are still some challenges to be addressed.

A first set of challenges regards the adversary model, that is, the way the attacker acts against the security protocol. In particular, the possibility of active attacks are usually neglected, hence focusing only on the passive attacks. There is usually the assumption that the adversary is not able to manipulate the channel, thus, relying only on a set of channel observation, which might also be limited. Moreover, the presence of multiple attackers is often overlooked.

Then, the wireless channel is usually considered through an over simplified model, which might limit the actual effectiveness of the PLS mechanisms. In addition, it is usually assumed that the channel decorrelates rapidly in time/frequency/space, which have to be investigated more deeply. Eventually, the channel is assumed random enough for an adversary to predict, for example through a deterministic channel model such as a Ray Tracing algorithm. However, a previous work dealt with the problem of the so-called Ray Tracing Attack [49], where results showed the difficulties and the low effectiveness of this threat.

This work aims at addressing, or at least trying to provide some answers to, the challenges faced by PLS, in particular the channel related ones. In Chapter 2, a wireless channel analysis is presented, with particular focus on the spatial correlation. First, the real trend of spatial correlation is presented, to show that in real propagation scenarios correlation does not follow the classical Jake's model. Then, an analysis on the effect of the correlation on SKR is presented, highlighting that PLKG might be affected by spatial correlation. In Chapter 3, an introduction on Frequency Diverse Array (FDA) is presented, an array technology to achieve field spatial focusing by employing small frequency shifts between array elements. Moreover, FDA is discussed as possibility to protect wireless communications, along with a study on the actual capability of FDA for securing communications.

2

Wireless Channel Analysis for Physical Layer Security

Spatial correlation plays an important role for PLS, both for the key-less solutions and key-based solutions. As explained in (1.3), the secrecy capacity depends on the Alice-Bob channel and the Eve's channel. In case the two channels are correlated, the security of the communication might be severely placed at risk. Moreover, as explained by (1.17) and (1.18), the key generation effectiveness might be impaired too, since the channel observations will be similar between the users and the eavesdropper. Therefore, it is important to have a general spatial correlation model that takes into account real propagation conditions, thus providing insight into the actual correlation between the two channels. Therefore, with a more general channel mode, the actual security level in presence of an eavesdropper can be assessed.

Many studies have been carried out with the aim of analysing the security of the channel in terms of secrecy capacity or secrecy key rate, usually through simulative work. However, few studies investigated the spatial correlation of the wireless channel with the focus on PLS applications. As highlighted in [48], spatial correlation represents one of the main threats involving a close adversary, even though usually overlooked. In fact, spatial correlation is usually assumed to be compliant with the Jake's model, which assumes scattering coming with a uniform angular distribution; hence, the correlation drops to zero around half wavelength. However, it is known that Jake's model is particularly ideal and is not necessarily representative of the real propagation conditions. Therefore, it is necessary to investigate spatial correlation in real scenarios, e.g. when in the channel includes a dominant component such as the Line Of Sight (LOS) component.

This chapter introduces a new spatial correlation model, validated also through measurements. The model aims at highlighting that spatial correlation might be significant even after the half-wavelength distance usually considered. After the model description and validation, the impact of non-zero spatial correlation on PLKG is studied. In particular, simulations are carried out using a Tapped Delay Line (TDL) model,

considering also correlated channels, to compute the SKR.

2.1 Spatial Correlation Measurement

A first assessment consists of a measurement campaign aiming at analysing spatial correlation. Measurements are carried out by means of a Vector Network Analyser (VNA), in different scenarios, and with two different kinds of antennas. In both cases, the transmitter and receiver are equipped with the same single antenna. To explore the wireless channel spatial correlation over a distance of few wavelengths, a three-axes positioner is employed, which is able to precisely move the receiver antenna with peace up to 1 mm. In the end, the correlation is computed using the measured complex CTF.

Previous works already dealt with the computation of spatial correlation from measured channels. In [50], the authors measure the channel characteristics of an outdoor Multiple Input-Multiple Output (MIMO) channel at 2.6 GHz with a 50 MHz bandwidth, using a 128 elements linear array at the base station and different user location, both in LOS and Non-Line Of Sight (NLOS) conditions. Authors measure the uplink channel through a VNA and determine different channel characteristics, including spatial correlation. In [51], the authors perform similar measurements but in an indoor scenario with an Ultra-Wideband system. Authors of [52] measure the MIMO broadband channel at 5 GHz in a modern office environment, including both LOS and NLOS conditions. Measurements are performed with a custom designed channel sounder. An interesting scenario is considered in [53], where measurements are performed inside a cabin of an aircraft. A channel sounder is employed at 3.52 GHz, with a bandwidth of 40 MHz, still in a MIMO communication system. Measurements in [54] are performed in an indoor office environment, with a channel sounder at 5.2 GHz. In addition, the measurements are compared with the results of a MIMO stochastic channel model. Authors in [55] perform measurements of spatial correlation in high-speed railway channels. They consider different scenarios (viaduct, cutting, and station), a Single Input-Multiple Output (MIMO) system using LTE channel parameters and a channel sounder. In [56], channel correlation is studied in an indoor office environment. Authors focus their attention on the impact of different polarization patterns on channel correlation. They employ a 4x4 MIMO system with a channel sounder, which limits the spatial correlation assessment at a distance of 1.5 wavelength. Moreover, they only consider LOS propagation condition.

All the described works lack in analysing the correlation characteristics of different environments and propagation conditions. Instead, an overview of the spatial correlation characteristics over different kind of environments and propagation conditions is here provided, highlighting the different trends of spatial correlation.

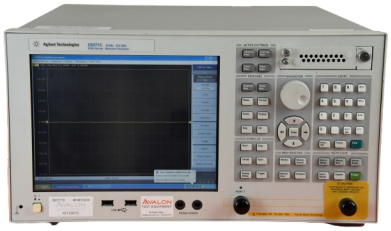
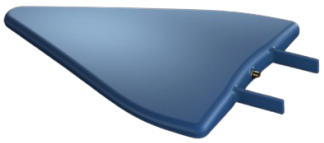


Figure 2.1: Agilent Technologies E5071C VNA.

(a) OmniLOG® PRO.



(b) HyperLOG® 7060.

Figure 2.2: Antennas used for measurements.

2.1.1 Measurement Setup

Regarding the measurement instrument, a VNA, the Agilent E5071C shown in Figure 2.1, has been used. The VNA ranges from 9 kHz to 8.5 GHz, with a maximum of 1601 points. The VNA is used to measure the S_{21} values, which can be interpreted as the CTF of the wireless channel: in this way, it is possible to evaluate the spatial correlation through the wideband channel. The VNA has always been calibrated to filter out the effects of the cable connecting the two antennas. Moreover, the central frequency has been set to 5 GHz, with a correspondent wavelength equals to 6 cm, and with a span of 500 MHz.

Two types of antennas have been employed: a pair of wideband omnidirectional antennas and a pair of log-periodic directive antennas. Omnidirectional antennas are the Aronia OmniLOG PRO 1060 (shown in Figure 2.2a) [57], which are broadband dipole antennas with a magnetic base, ranging from 150 MHz to 6 GHz. In the considered frequency range, the antennas have a gain around 0 dBi. These antennas are equipped with a built-in 3.5 m long SMA cable that cannot be removed. Therefore, measurements with the omnidirectional antennas might suffer from the effects of the above-mentioned cable. Directive antennas are the Aronia HyperLOG (shown Figure 2.2b) [58] broadband log-periodic antennas, ranging from 700 MHz to 6 GHz, with a maximum gain of 5 dBi and a half-power beam width of around 30° in both horizontal and vertical plane.

(a) Side view of the positioner. **(b)** Back view of the positioner.

Figure 2.3: Wooden positioner used for the measurements.

2.1.2 Three-Axis Positioner

In order to move the receiver antenna in space over distances of the order of the wavelength, a self-made three-axis positioner has been used, which is shown in Figure 2.3. It consists of a wooden table with wheels to move it, three mechanical positioners to move the antenna in the space, some electrical motors with their controller. The motors can be controlled from a laptop through serial port communication: in particular, a MATLAB[1] programme has been written to command the motors. The positioner can move over an 80 cm × 80 cm square area, with an extension of 40 cm on the z-axis. In addition, it is capable of moving the antenna with a step up to 1 mm.

2.1.3 Measurements Environment

Measurements have been carried out at the Cesena Campus of the University of Bologna. Three different environment have been selected for the measurements: a lecture room (in particular Room 29, in the following just "room"), a small corridor and the inner garden as outdoor scenario. In all the environments, both the LOS and the NLOS situations have been considered. To achieve the NLOS condition, a metallic whiteboard has been placed in front of the transmitter antenna, at around 10 cm distance, while the positioner and the antenna itself are kept in the same position. The whitebaord has been placed close to the antenna in order to reduce possible diffraction effects and to block the LOS path for all the receiving position, since it is pretty close to the TX

[1] `https://www.mathworks.com/products/matlab.html`

(a) Room with the dipoles in the LOS condition

(b) Room with the dipole and the whiteboard.

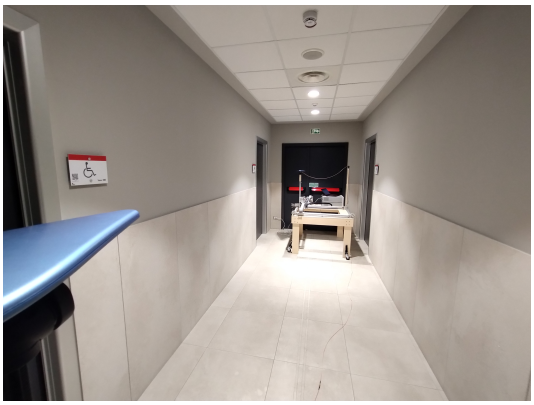
Figure 2.4: The room used for the measurement.

antenna. Figure 2.4, Figure 2.5 and Figure 2.6 show the three environments, where it is possible to see the antennas, the positioner, and the whiteboard used for the NLOS condition.

2.1.4 Measurement Procedure

The goal of the measurements is to calculate the spatial correlation of the channel in the different environments. The positioner and the VNA are controlled remotely from a laptop, which is also controlled remotely outside the environment in order to reduce at minimum the influence of people on the measurements. Measurements are performed along a line to get a curve of spatial correlation with respect to the distance. In particular, the antenna attached to port 1 of the VNA (the Transmitter (TX)) is fixed in the space, while the other antenna attached to port 2 (the Receiver (RX)) is moving on the positioner. First, the positioner is set on its initial position in the bottom right corner (see Figure 2.7). Then, the TX antenna is positioned in front of the RX antenna at 5 m distance.

For each scenario, the RX antenna is moved along the negative X axis (with reference to Figure 2.7), therefore perpendicular to the axis connecting the two antennas at the beginning. Both LOS and NLOS measurements were performed. The positioner moves the antenna with a step of 6 mm, which corresponds to $\lambda/10$ at 5 GHz, with a total of 101 measurement points. In the first measurement point, the two antennas are facing



(a) Corridor with the log periodic antennas in the LOS condition

(b) Corridor with the dipole and the whiteboard.

Figure 2.5: The corridor used for the measurement.

(a) Garden with the log periodic antennas in the LOS condition

(b) Garden with the log periodic and the whiteboard.

Figure 2.6: The garden used for the measurement.

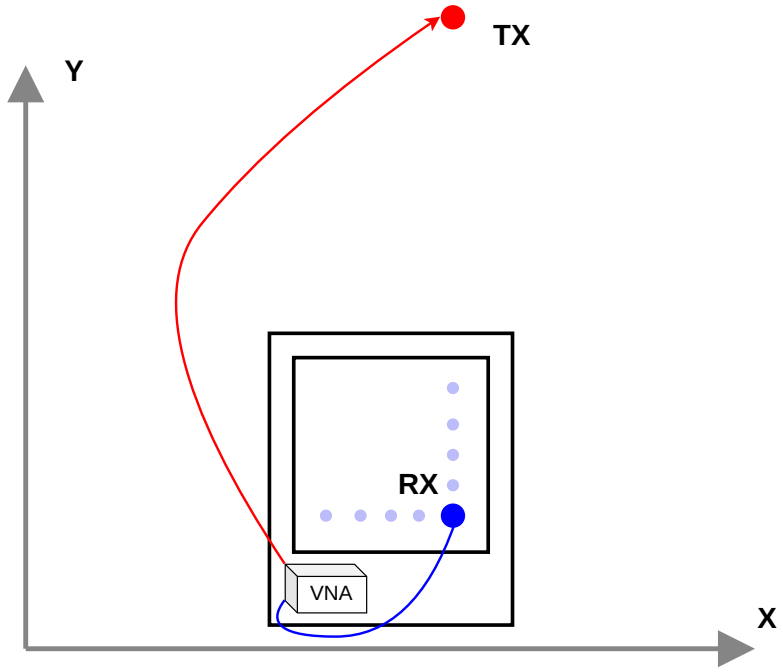


Figure 2.7: Measurement scheme

each other.

The VNA performs a scan from 4.75 GHz to 5.25 GHz with 501 points in order to have a 1 MHz frequency resolution. The average factor of the VNA is set to 20, the Intermediate Frequency to 30 kHz and the output power of the Radio Frequency (RF) signal 10 dBm, in order to increase the SNR of the measurements.

2.1.5 Correlation Computation

Usually, the correlation between complex values can be computed as follows [51]:

$$\rho(u,v) = \frac{E\{uv^*\} - E\{u\}E\{v^*\}}{(E\{|u|^2\} - |E\{u\}|^2)(E\{|v|^2\} - |E\{v\}|^2)}, \tag{2.1}$$

where u, v are complex vectors, $(.)^*$ is the complex conjugate operator, and $E\{\cdot\}$ is the mean value operator. This formula represents the complex correlation of two vectors, which can be substituted by the measured CTF from the VNA to obtain their complex correlation. In this case, CTF are 501 points complex valued arrays, hence $u \equiv H_i(f)$ and $v \equiv H_j(f)$.

This solution allows computing the correlation between two specific points in the space. Instead, a "spatial averaged" correlation has been computed in this work, to get a more generic description of the environment, and to evaluate how the correlation varies with respect to the distance between two points. In particular, the following procedure has been employed:

$d = 0$	$d = \lambda/10$	$d = \lambda/5$	$d = 3\lambda/10$		$d = 8\lambda$
$\rho(H_0, H_0)$	$\rho(H_0, H_1)$	$\rho(H_0, H_2)$	$\rho(H_0, H_3)$	$\cdots$	$\rho(H_0, H_{79})$
$\rho(H_1, H_1)$	$\rho(H_1, H_2)$	$\rho(H_1, H_3)$	$\rho(H_1, H_4)$		$\rho(H_1, H_{80})$
$\rho(H_2, H_2)$	$\rho(H_2, H_3)$	$\rho(H_2, H_4)$	$\rho(H_2, H_5)$	$\ddots$	$\rho(H_2, H_{81})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\rho(H_{20}, H_{100})$
$\vdots$	$\vdots$	$\vdots$	$\rho(H_{97}, H_{100})$		
$\vdots$	$\vdots$	$\rho(H_{98}, H_{100})$			
$\vdots$	$\rho(H_{99}, H_{100})$				
$\rho(H_{100}, H_{100})$					

Figure 2.8: Picture of the computed correlation matrix

- Collect the 101 points of measurements on the line.
- Select a target distance (d) for which computing the correlation.
- Compute the correlation between each pair of CTF which are d apart.
- Average over all the pair-wise correlation values

To better understand this procedure, consider the matrix in Figure 2.8. Each column represents the correlation values for a selected target distance value. The first column is at $d = 0$, therefore the correlation is computed always between the same vector, resulting in 1. The second column is at $d = \lambda/10$, the correlation is computed between points 0-1, 1-2, 2-3, up to 99-100. The third, the correlation is computed between 0-2, 1-3, 2-4, up to 98-100. This procedure is repeated until $d = 8\lambda$, since it is a value that allows to generate a good amount of couples for averaging the results. At the end, each column is averaged, and the final value represent a sort or spatial average of the correlation when the terminals are spaced of distance d.

2.1.6 Measurement Results

Figure 2.9 shows the absolute squared correlation for each environment, LOS and NLOS, with omnidirectional antennas. The room environment in LOS shows a correlation similar to the one in NLOS, and both are quite close to the ideal Jake's model. In fact, the correlation decreases and reaches a zero value around half wavelength, even though LOS curve keeps higher values with respect to the NLOS curve. Moving to the corridor environment, small and narrow, multipath is expected to arrive with a smaller angular spread. In fact, the correlation in both LOS and NLOS decreases faster than the room, and it is kept low for higher distances. As expected, in the outdoor scenario in LOS, spatial correlation decreases with distance while always keeping high values: in this case, obstacles of the garden are far from the antennas, hence the multipath

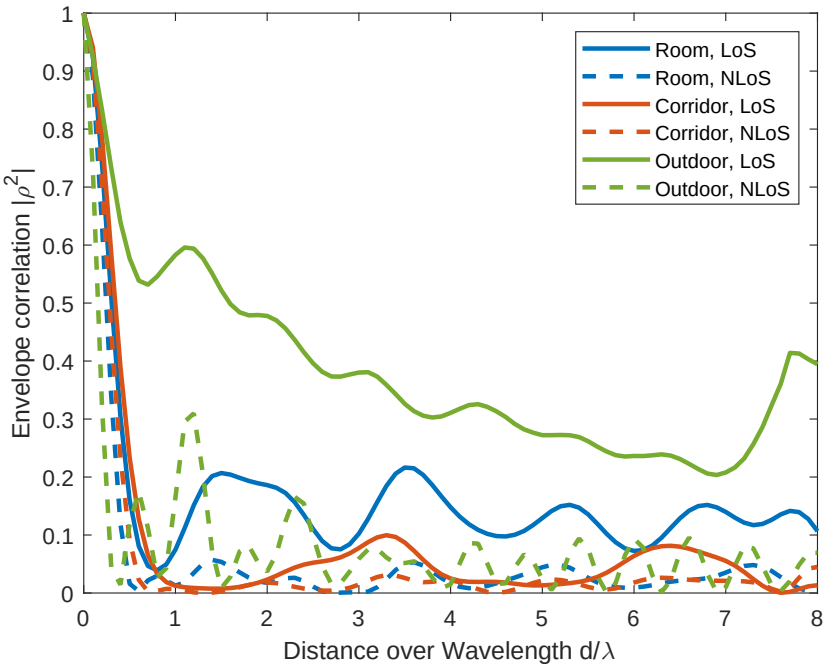


Figure 2.9: Comparison between measurements in each environment, both LOS and NLOS, with the omnidirectional antennas.

contributions have reduced intensity with respect to an indoor scenario, making the dominant component quite significant. At the same time, in NLOS case, the direct component is significantly reduced, probably arriving at the receiver with a similar amplitude as the scattered field, hence the correlation shows a trend similar to the ideal Jake's model.

A comparison between the corridor and the outdoor environment, in LOS, including also the directive antennas, is shown in Figure 2.10. By looking only at the antennas, it is clear that in LOS correlation does not follow the classical ideal trend: even with omnidirectional antennas, the correlation reaches its zero after a wavelength distance in the corridor, and does not even reach zero in the other cases. In fact, being the corridor narrow, the scattered field tends to arrive at the receiver with a similar intensity both for the direct path and for the multipath components. In the outdoor environment, on the other hand, where the scattered are at higher distances, the direct path has a higher contribution with respect to the multipath component and therefore the correlation distance increases. The usage of directive antennas increases the correlation, as in this case the dominance of the direct path is intensified, even though the directivity of the antenna is not so high. The trend for the correlation outdoor is similar, evidently with higher values with respect to the corridor.

When moving to the NLOS case, the results are of course different. As reported in Figure 2.11, the corridor with the dipoles shows a similar trend with respect to the ideal case: the whiteboard obstructing the LOS component partially reflects the fields, thus the multipath is rich. Moreover, the obstacle produces diffracted fields, which is less correlated than the reflected components: therefore, the correlation decreases

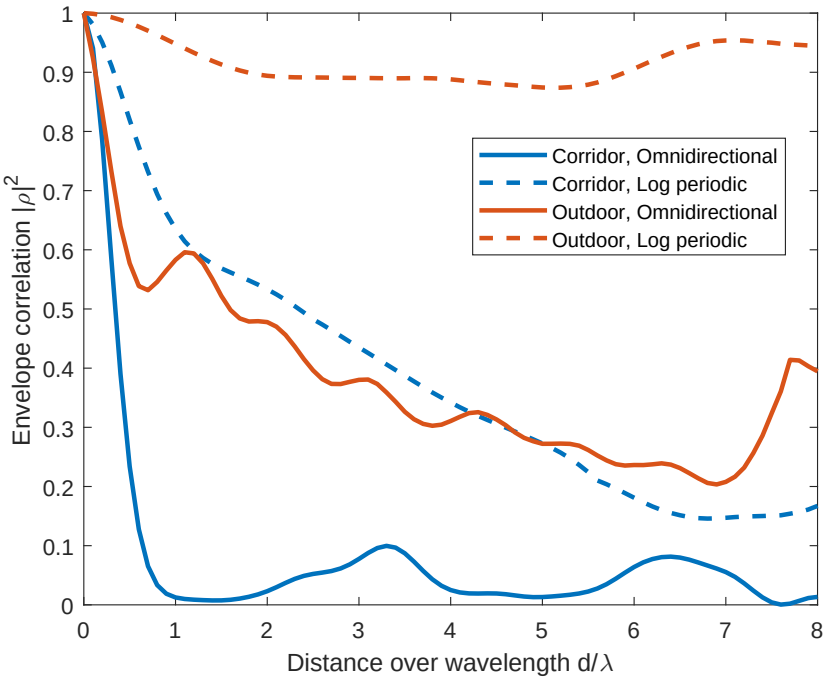


Figure 2.10: Comparison between corridor and outdoor environment, in LOS, with both antennas.

fast in space. A similar situation occurs with the directive antennas, but the values of correlation are higher. In the outdoor environment, with the omnidirectional antenna, correlation decreases pretty fast, but the oscillations of the curve reach higher peaks with respect to the ideal case: in this situation, propagation occurs mostly trough diffracted component from the obstacle, since reflected fields is lower due to the outdoor condition. Instead, when directive antenna are equipped, correlation is kept with high values. In fact, the obstacle does not entirely block the direct component, but it just attenuates it. Moreover, since the whiteboard is placed close to the antenna, it is likely that the radiation lobe illuminates the surface of the obstacle, hence still passing through the whiteboard. Therefore, the propagation is still affected by a dominant component, since the reflected field is low due to the environment. In fact, as can be seen in Figure 2.12, when the two directive antennas are aligned the LOS and NLOS wideband channels differ in the attenuation, while the multipath scheme remains similar. With respect to the LOS case depicted in Figure 2.10, the correlation is of course lower, but it still maintains high values.

In conclusion:

- In the room, spatial correlation resembles the Jake's model both in LOS and NLOS, since it is a large environment with many objects which function as scatterers.
- In the corridor, being a narrow environment, scattering has a confined angular distribution. Therefore, wireless channel shows a smaller correlation than the room when employing omnidirectional antennas, both in LOS and NLOS condi-

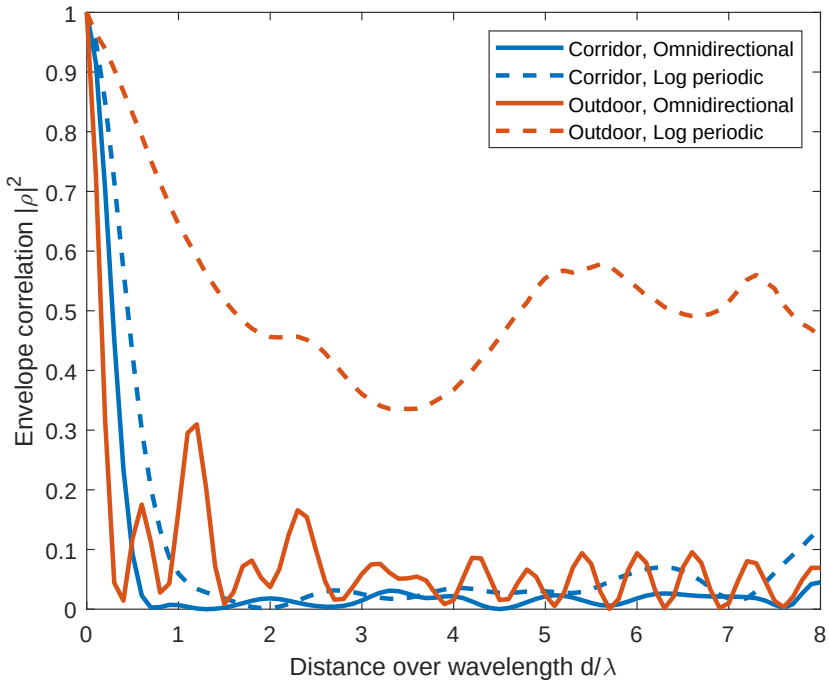


Figure 2.11: Comparison between corridor environment and outdoor, in NLOS, with both antennas.

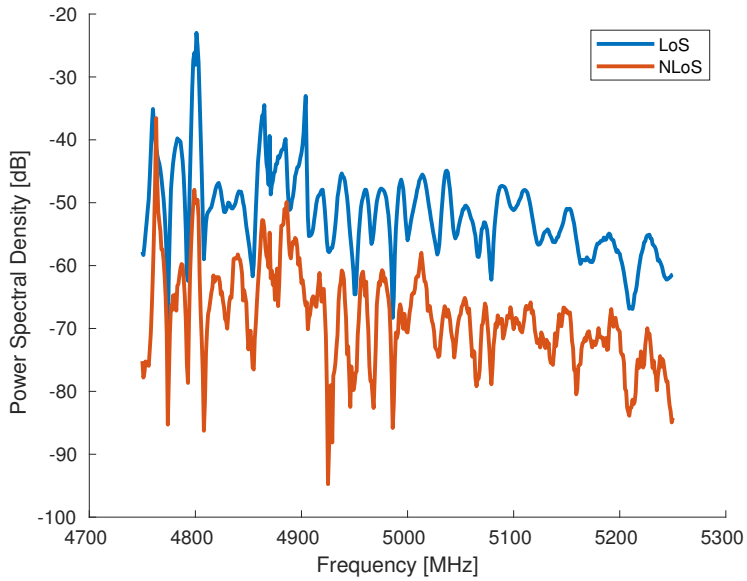


Figure 2.12: Example of LOS and NLOS channel, outdoor environment with log-periodic antenna

tion. When directive antennas are equipped in LOS, of course spatial correlation is maintained high for longer distances, while in NLOS correlation resemble the ideal case.

- In outdoor, scatterers are far from the antennas, hence the dominant component amplitude becomes significantly higher than the scattering. Except for the case with omnidirectional antennas in NLOS, the correlation remains high for large distances.

In the end, spatial correlation strongly depends on the propagation conditions. Since the usual assumption of uncorrelated channel after half-wavelength, reliability of PLS might be threatened, in particular PLKG, which strongly relies on the assumption of uncorrelated channel to avoid eavesdropping attacks.

2.2 Spatial Correlation Theoretical Model

A more general analysis can be carried out by means of a theoretical model. In particular, a model allows understanding a general trend of the spatial correlation with respect to different macro-parameter of the environment (e.g. Rice K-factor, scattering distribution, angle spreading). Even though measurements were referred to specific environment, they allowed to catch some general trends of spatial correlation. In order to provide a more general theoretical framework to the achievements extracted from the experimental activity, a theoretical model for spatial correlation assessment is discussed in this section. The model is not case specific, but is rather aims at catching the sensitivity of spatial correlation to the major channel parameters of the wireless channel. Of course, models often try to give a general insight on the phenomena, providing a satisfactory understanding of the impact of different propagation condition. However, the model will describe an "average" environment, which simplify its usage and widen the usage cases, but sacrifices the precision in particular cases which might differ a lot from the "average ideal" case. In any case, providing a general spatial correlation model might help in analysing the propagation without complex simulations or long measurement procedures.

The simplest correlation model is the well known Jake's model. The model assumes Wide Sense Stationary Uniform Scattering (WSSUS), NLOS, rich scattering, and a uniform power angular distribution: these assumptions are usually met in the ideal case of Rayleigh fading distribution. The spatial correlation can be then expressed as:

$$\rho(d) = J_0(2\pi\frac{d}{\lambda}), \tag{2.2}$$

where J_0 is the Bessel function of first kind and order 0, d is the distance and λ is the wavelength. The resulting correlation is shown in Figure 2.13: it is possible to see the classic trend of the Bessel function, having a 0 around 0.4λ.

However, Jake's model is accurate under conditions not always and automatically satisfied in every propagation scenario: hence, new correlation models are required, in

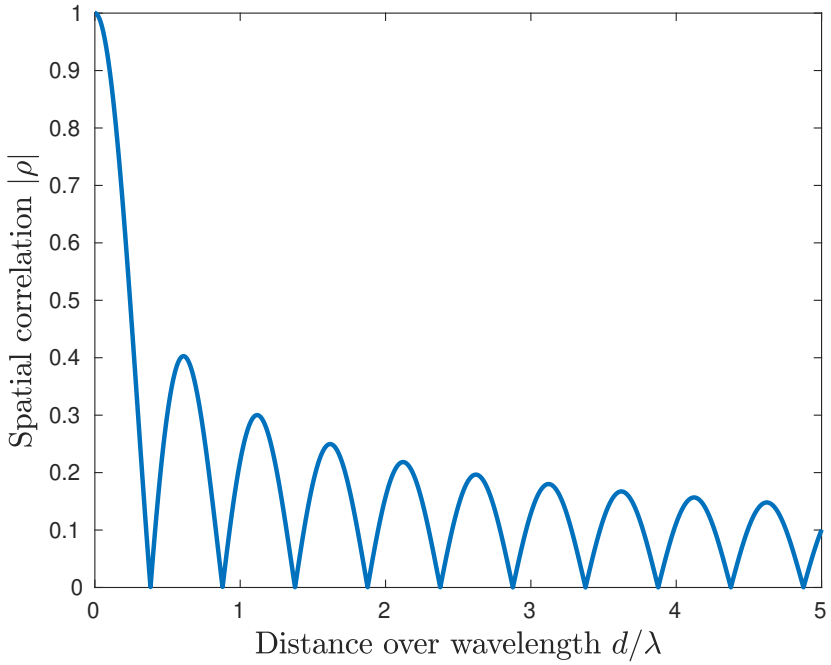


Figure 2.13: Jake's model for spatial correlation

particular targeting PLS applications. For example, in [59] a more general spatial correlation model is presented, which can be tailored to different distributions of scattering, even though the absence of a dominant component is supposed. Moreover, the scatterers are assumed to be far enough to consider the reception of planar waves at the terminal point. A similar development has been carried out in [60]. In [61], the impact of angular spread on the small scale fading statistics is investigated, including also the spatial correlation; moreover, a definition of the correlation distance (the distance after which it is possible to consider the channel uncorrelated) is provided.

Nevertheless, proposed correlation models do not take into account the possible presence of a dominant component, or a dominant multipath cluster. Moreover, the new communication technologies will rely on high frequencies, massive MIMO, and beamforming [62–65]: due to these new characteristics, new propagation models are needed, taking into account the new communication mechanisms. In particular, a new complete and realistic model of spatial correlation might be desirable, which can take into account real and future propagation scenarios.

Let's consider the wireless communication between two legitimate users Alice and Bob, under the threat of an eavesdropper Eve placed at a distance d from Alice (or Bob), as sketched in Figure 2.14. Propagation occurs in a multipath environment, where the received multipath pattern is the result of two separate, major contributions:

- A *scattering* multipath component, spread over an angular range $\sigma_s \in [0, 2\pi]$ centred in the Direction of Arrival (DOA) ϕ_s according to a Power Angle Profile (PAP) $p_s(\phi)$.

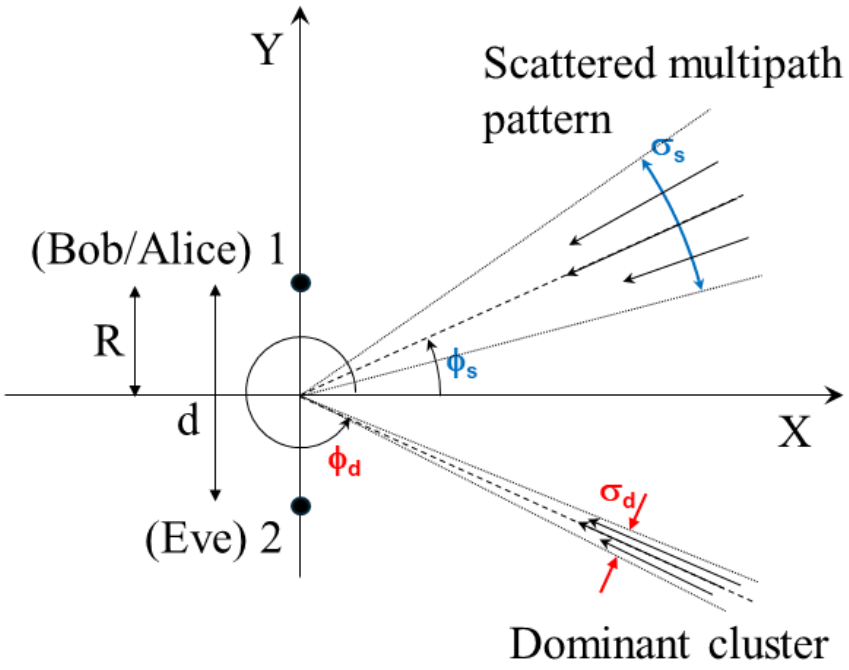


Figure 2.14: Multipath spatial distribution at the receiver.

- A *dominant* multipath cluster, limited to a narrow range of DOA around the angle ϕ_d (i.e. $\sigma_d \approx 0$ in Figure 2.14) according to a PAP $p_d(\phi)$.

Both the power angle profiles are here intended normalized in a way that:

$$\int_0^{2\pi} p_{s/d}\left(\phi\right) d\phi = 1. \tag{2.3}$$

Let's also assume the signals received from the scattered paths arrive with similar intensities and phase uniformly distributed over $[0, 2\pi]$. Then, the scattered multipath *alone* corresponds to Rayleigh fading [66]. Conversely, when the dominant cluster is also considered, then fast fading is instead expected to comply with the Rice distribution [66]. The overall normalized PAP at both Alice (or Bob) and Eve can be then expressed as:

$$p\left(\phi\right) = \frac{K}{K+1} \cdot p_d(\phi) + \frac{1}{K+1} \cdot p_s(\phi), \tag{2.4}$$

where K can be regarded as the Rice factor of the fading distribution, i.e. the ratio between the power of the dominant signal component and the power of the scattered signal contributions. Spatial correlation between the complex signal envelopes s_1 and s_2 received in points 1 and 2 of Figure 2.14 can be computed as [59]:

$$\rho = \frac{E\left[s_1 \cdot s_2^*\right]}{E\left[\left|s_1^*\right|^2\right]}. \tag{2.5}$$

Assuming a locally plane wave arriving at the receivers with DOA equal to ϕ, the difference between s_1 and s_2 simply consists of a phase shift, i.e. $s_2 = e^{j\beta dsin\phi} \cdot s_1$, being $\beta = 2\pi/\lambda$. Since many received signals are received in a multipath environment, each having its own DOA, the correlation coefficient can be then also written as [67, 68]:

$$\rho = \int_0^{2\pi} e^{-j\beta d \cdot \sin(\phi)} \cdot p(\phi)\, d\phi. \tag{2.6}$$

Based on (2.4), the complex correlation coefficient in Rice channels can be written as:

$$\rho = \frac{K}{K+1} \cdot \rho_d + \frac{1}{K+1} \cdot \rho_s, \tag{2.7}$$

where ρ_d and ρ_s can be computed through (2.6) replacing $p(\phi)$ with $p_d(\phi)$ and $p_s(\phi)$, respectively. According to (2.6), (2.7), the parameters mostly affecting spatial correlation in Rice channels are: the normalized distance between the receivers (d/λ), the Rice factor and the power angle distribution functions $p_d(\phi)$ and $p_s(\phi)$.

The simplest choice for the scattering PAP corresponds to a uniform distribution [61, 67], i.e.:

$$p_s(\phi) = \begin{cases} \frac{1}{\sigma_s}, & \text{if } \phi \in \left[\phi_s - \frac{\sigma_s}{2}, \phi_s + \frac{\sigma_s}{2}\right] \\ 0, & \text{otherwise} \end{cases} \tag{2.8}$$

The contribution of the diffuse multipath component to the spatial correlation coefficient can be then written as [67]:

$$\rho_s(\phi) = \frac{1}{\sigma_s} \cdot \int_{\phi_s - \frac{\sigma_s}{2}}^{\phi_s + \frac{\sigma_s}{2}} e^{-j\beta d \cdot \sin(\phi)} d\phi = \Re[\rho_s] + \Im[\rho_s] \tag{2.9}$$

$$\Re[\rho_s] = J_0(\beta d) + 2\sum_{k=1}^{+\infty} J_{2k}(\beta d) \cdot \cos(2k\phi_s) \cdot \operatorname{sinc}\left(2k\frac{\sigma_s}{2}\right) \tag{2.10}$$

$$\Im[\rho_s] = 2 \cdot \sum_{k=0}^{+\infty} J_{2k+1}(\beta d) \cdot sin((2k+1)\phi_s) \cdot \operatorname{sinc}\left((2k+1)\frac{\sigma_s}{2}\right) \tag{2.11}$$

Where $\Re$ and $\Im$ represent the real and the imaginary part, and J_k the Bessel function of first type and order k.

The magnitude of ρ_s is plotted in Figure 2.15 against d/λ and for different values of σ_s. As also thoroughly discussed in [61, 67], smaller values of σ_s correspond to stronger spatial correlation, to the extent that $|\rho_s| = 1$ independently of d/λ if $\sigma_s = 0$. This corresponds to an ideal case, where the scattered multipath comes down to a single received plane wave arriving from the direction ϕ_s. Real propagation conditions are in general quite different, that is why in real world contexts spatial correlation always fades - sooner or later - for increasing distance.

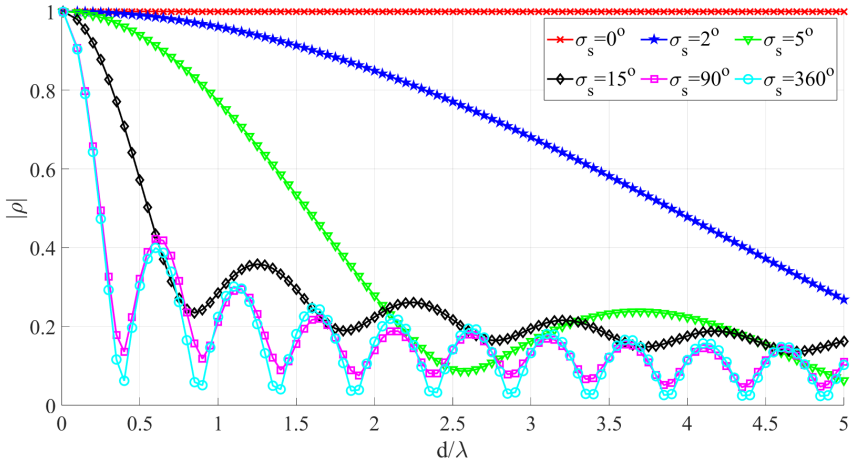


Figure 2.15: Spatial correlation in presence of a scattered multipath pattern without any dominant contribution ($K = 0$). ϕ_s=45 is assumed in the figure.

With reference to the PAP associated with the dominant contribution, the simplest choice would be $p_d(\phi) = \delta(\phi - \phi_d)$. In fact, the existence of a dominant incoming signal is expected to be related to particular, favourable propagation conditions (e.g. the presence of line of sight) that supposedly occurs in a very specific direction. Unfortunately, it has been just discussed that the Dirac distribution is a rather ideal representation, leading to results that make little physical sense (according to (2.7), at large d/λ, $|\rho|$ would simply settle at $K/(K+1)$). In order to provide the model with some physical soundness, still limiting its complexity, the same distribution is here assumed for both $p_d(\phi)$ and $p_s(\phi)$, but of course with different parameters (in particular, $\sigma_d = 1°$ is considered in the following). With reference to the simple uniform distribution case, (2.10) and (2.11) can be still relied on for the computation of ρ_d, of course replacing (ϕ_s, σ_s) with the proper (ϕ_d, σ_d).

2.2.1 Simulation Results

Since spatial correlation is known to be in general related to the multipath distribution in the DOA domain, evaluation of angle spread (σ_ϕ) in Rice multipath channel, and some results and discussion about spatial correlation under Rice propagation conditions are included in the following.

Angle Spread in Rice Multipath channels

In agreement with [61], the channel angle spread is here defined as:

$$\sigma_\phi = \sqrt{1 - \frac{|F_1|^2}{|F_0|^2}} \qquad \text{With } F_n = \int_0^{2\pi} p(\phi)\, e^{jn\phi}\, d\phi. \tag{2.12}$$

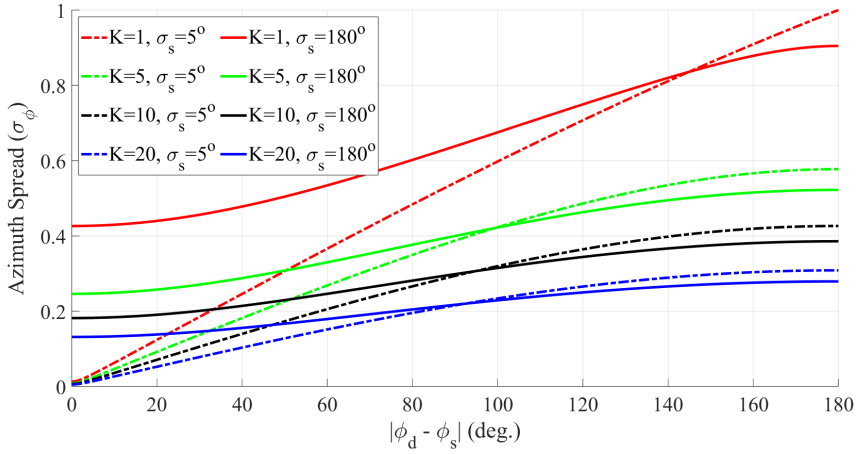


Figure 2.16: Azimuth spread for different settings of the dominant and the scattered multipath pattern. $\phi_s = 45°$ is assumed.

Since $p(\phi)$ here represents a normalized PAP, then $|F_0| = 1$. Moreover, the simple assumption of uniform distribution for both $p_d(\phi)$ and $p_s(\phi)$ easily leads to:

$$F_1 = \frac{2K}{K+1} \cdot \frac{e^{j\phi_d}}{\sigma_d} \cdot sin\left(\frac{\sigma_d}{2}\right) + \frac{2}{K+1} \cdot \frac{e^{j\phi_s}}{\sigma_s} \cdot sin\left(\frac{\sigma_s}{2}\right) \tag{2.13}$$

Based on (2.2.1), Figure 2.16 shows that σ_ϕ is affected by K, the difference between the central DOA of the dominant and scattered components ($|\phi_d - \phi_s|$), and σ_s in a somehow interleaved fashion. As a general trend, azimuth spread decreases at larger K values, that makes physical sense. Also, azimuth spread increases as $|\phi_d - \phi_s|$ gets larger, but the sensitivity to $|\phi_d - \phi_s|$ increasingly fades for greater Rice factor. This is also physically sounded, as the more the dominant path is actually dominant (i.e. the greater the K value), the weaker the expected impact of any other multipath contributions to every propagation marker. Finally, the way σ_ϕ changes with σ_s depends on $|\phi_d - \phi_s|$. If the dominant and the scattered contributions arrive from close directions, then a greater σ_s corresponds to a larger σ_ϕ (as it happens in Rayleigh channels [59–61, 67]), whereas the trend is instead reversed when the dominant and the scattered components come from opposite DOA. The turning point is likely to be K-dependent.

Spatial Correlation Properties of Rice Multipath Channels

The magnitude of the spatial correlation coefficient is plotted in Figure 2.17 against normalized distance and for different values of Rice factor. Although spatial correlation always looses its strength at increasing distance, it also gets stronger at larger values of the Rice factor, to the extent that K values mildly greater than 0 (e.g. see the case K=1 in the figure) makes anyway a clear change in the spatial correlation trend compared to the Rayleigh case ($K = 0$). Since large K values correspond to a smaller angle spread (Figure 2.16), the sort of inverse relationship between spatial correlation

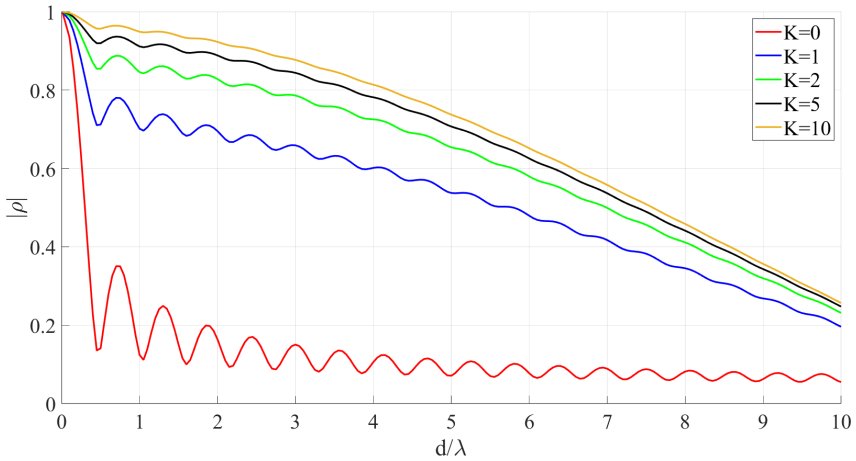


Figure 2.17: Spatial correlation coefficient vs. normalized distance for different K values ($\sigma_s = 90^o$, $\phi_d = \phi_s = 45^o$).

and angle spread already highlighted for Rayleigh fading [61] is here extended also to the Rice case.

Of course, any spatial correlation model brings information about correlation distance. With reference to a Rayleigh propagation channel, the analysis carried out in [61] came up with the following simple formula for d_c (averaged over all possible azimuthal orientations):

$$d_c = \frac{\lambda}{\sigma_\phi \cdot \sqrt{23}} \tag{2.14}$$

For instance, the correlation distance for Rayleigh fading ($K = 0$) and $\sigma_s = 360^o$ turns out to be 0.28λ, in close agreement with the Jake's model ([48, 69]). It is worth pointing out that (2.14) is based on a Gaussian approximation of the spatial correlation coefficient, which is accurate just for small d values [61]. Owing to the general relationship between spatial correlation and angular dispersion, this also means that (2.14) becomes unreliable for small azimuth spread.

The following extension of (2.14) to Rice fading conditions is here proposed:

$$d_c = \frac{1}{K+1} \cdot \frac{\lambda}{\sigma_\phi^{scat} \cdot \sqrt{23}} + \frac{K}{K+1} \cdot \frac{\lambda}{\sigma_\phi^{dom} \cdot \gamma}, \tag{2.15}$$

where σ_ϕ^{dom} and σ_ϕ^{scat} respectively represent the azimuth spread in presence of the dominant or the scattered contribution alone. Since the first term of (2.15) provides the correlation distance in Rayleigh fading conditions (K=0), it is set equal to (2.14) in agreement with [61]. Conversely, the last term represents the correlation distance when $K = \infty$, i.e. when scattering is negligible compared to the dominant component. The γ coefficient was not simply set to $\sqrt{23}$ as $\sigma_d = 1^\circ$ corresponds to a small σ_ϕ^{dom}, which might be out of the range of reliability of (2.14). Rather, the value of γ has been computed according to the following procedure:

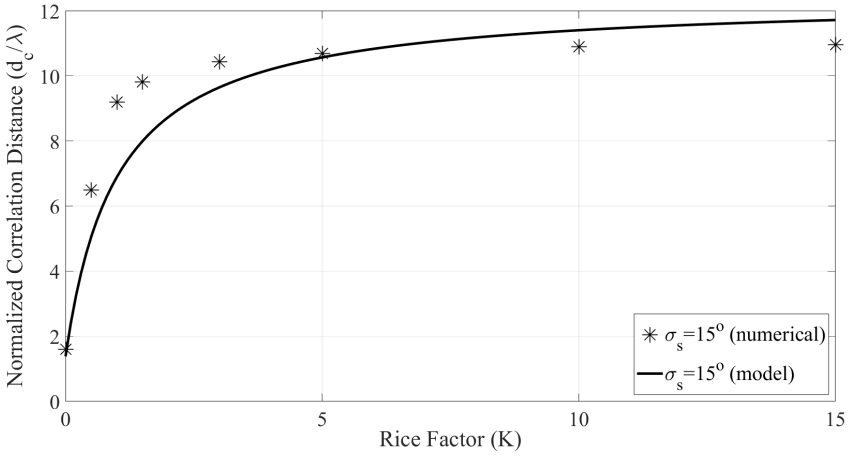


Figure 2.18: Spatial correlation distance vs. Rice factor. Comparison between numerical evaluation and simple analytical formula.

- the spatial correlation coefficient has been computed over the range $[0 \div 15 \cdot \lambda]$ for a multitude of K, ϕ_s, ϕ_d and σ_s values;
- for each considered case, the correlation distance d_c has been estimated according to its general definition ($|\rho(d_c)| = 1/e$);
- the mean correlation distance $\langle d_c(K, \sigma_s) \rangle$ has computed by averaging the d_c values over the set of considered DOA of both the dominant and the scattered contribution;
- the least square method has been applied to compute the best-fit γ that makes (2.15) the best approximation for $\langle d_c(K, \sigma_s) \rangle$.

The outcome of the procedure finally was $\gamma = 15$. The corresponding (2.15) is compared in Figure 2.18 with the numerical estimate of d_c. In case σ_s is narrow (e.g. 15^o in Figure 2.18) and/or K is not close to 0, the correlation distance turns out to be equal to some/several wavelengths, i.e. much longer than the value often assumed in many studies on physical layer security. This means the idea that the presence of an eavesdropper represents a serious concern as long as his/her distance to the legitimate users is smaller than some fraction of wavelength might be optimistic in Rice fading channels.

Regardless of the fading conditions, a high communication frequency can clearly help to reduce the correlation distance. Unfortunately, higher frequencies usually bring greater propagation losses. Since beamforming is often claimed as a technical solution to combat heavier attenuation in the forthcoming wireless systems at millimetre waves, it should be stressed that line of sight conditions might be recommended to more easily put beamforming into practice. Line of sight would of course correspond to Rice factor values most likely well greater than zero, with a negative impact on spatial correlation that might even overcome the benefits expected from the frequency increase.

In conclusion of this analysis, it is also worth noting that the starting setting $\sigma_d = 1°$,

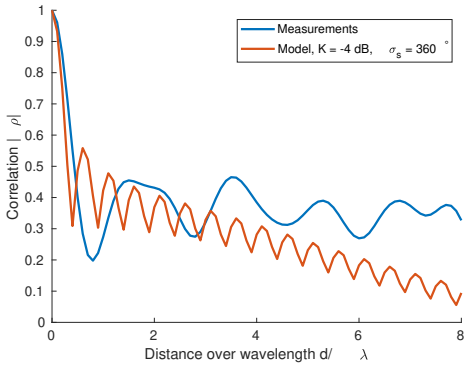
although sounded overall, was actually arbitrary. It might be of course smaller or greater, contributing to further reinforce spatial correlation if $\sigma_d < 1°o$ and instead to reduce it if $\sigma_d > 1°$. Moreover, power angle profiles different from the uniform distribution (e.g. Gaussian) would also affect the final results to some extent. Nevertheless, it is believed that the highlighted trends and relationships keep their validity irrespective of the assumptions enforced for the development of the model.

2.3 Validation of the Theoretical Model

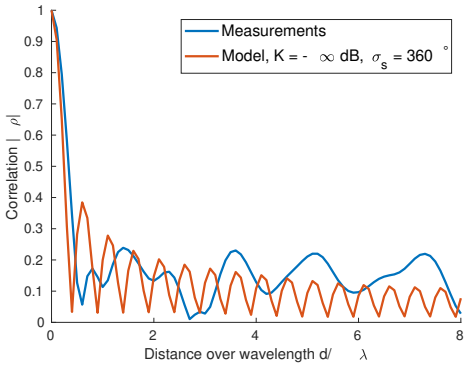
In order to check the soundness of the model, it is here compared with some use cases considered in the previous measurement campaign. In particular, the model always assumes a uniform distribution of scattering, hence tuning only the angular spread: the final goal is to understand if the trends shown by the model fit the measurement.

As a first case, consider the correlation in the lecture room. It is reasonable to assume that multipath comes uniformly from all the direction, since it is a close environment with a lot of objects inside. Hence, in the model $\sigma_s = 360°$ is assumed. A value of K that well fits the measurement in the LOS case is $K = -4\,\text{dB}$ (Figure 2.19a), while $K = -\infty\,\text{dB}$ (Figure 2.19b) suits the NLOS case. In the corridor, in particular with the log-periodic antennas, multipath spreading narrows: thus, a value of $\sigma_s = 180°$ is set. Looking at Figure 2.19c and 2.19d, the model well fits the LOS case when $K = 6\,\text{dB}$, while a lower value of $-7\,\text{dB}$ can be found in the NLOS case. As a last case, in the garden, the multipath spread can be set to 360°, since multipath comes from all the directions due to the multiple objects spread in the outdoor environment. In the LOS case, $K = 4.7\,\text{dB}$, while $K = -\infty\,\text{dB}$ is suitable for the NLOS case.

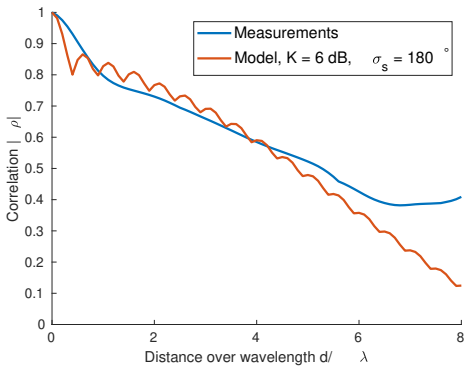
This preliminary assessment highlight that the model can be a reliable tool to predict the trend of spatial correlation, provided that reasonable scattering distribution and parameters are given. Moreover, even though the theoretical model might not be as precise as the measurements, it is able to provide a sufficient insight on the impact of the channel parameters on the correlation characteristics.



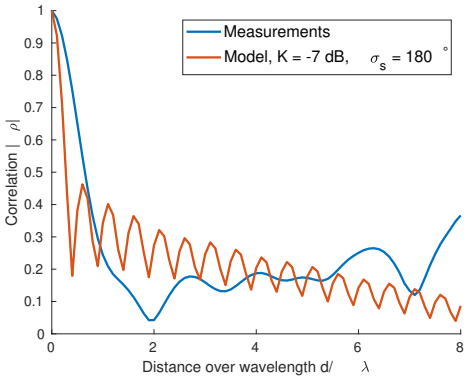
(a) Room with dipoles, LOS case.



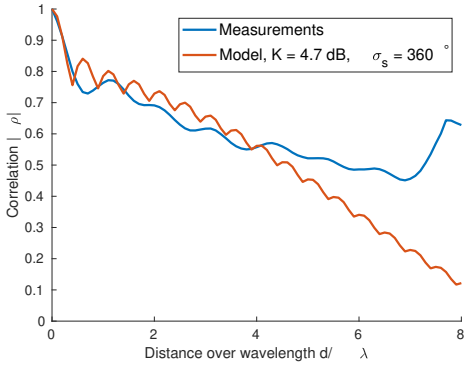
(b) Room with dipoles, NLOS case.



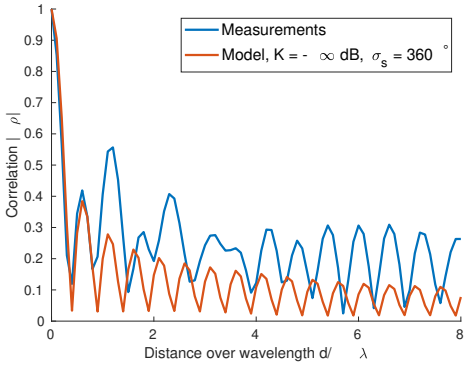
(c) Corridor with directive antennas, LOS case.



(d) Corridor with directive antennas, NLOS case.



(e) Garden with directive antennas, LOS case.



(f) Garden with directive antennas, NLOS case.

Figure 2.19: Comparison between measured and theoretical correlation.

2.4 Secrecy Analysis with Realistic Channel Model

Based on channel propagation conditions, PLKG performance varies. As discussed in section 1.2.5, SKR is an important metrics since it provides the amount of secret bits that can be extracted from the channel, without the possibility for an eavesdropper (Eve) to obtain them too.

Studies on the PLKG are mainly focused on the feasibility of the key generation process under the following conditions [3, 34]:

- The wireless channel is usually considered to be affected by Rayleigh fading.
- The possible presence of an eavesdropper is often neglected, although it represents a real limitation to the number of bits that can be reliably extracted from the channel.
- Alice and Bob are assumed to perceive perfectly symmetric channels, whereas this might not be true in real working conditions, as long as they cannot simultaneously sense the channel for whatever reason. In addition, the channel observations collected by Alice and Bob are affected by noise and/or hardware imperfections.

In fact, the SKR is usually reduced to the mutual information between the Alice and Bob [70], i.e. neglecting the presence of Eve in the channel, who nonetheless decreases the number of bits that can be securely extracted. However, in [71] authors considered the presence of the eavesdropper, but assumed Gaussian channel samples, which might not be true in reality. In addition, the generation is often assumed to happen in a NLOS scenario, i.e. under Rayleigh-like fading conditions [72], which is the ideal case for the PLKG thanks to the high entropy of the channel. Few works in the literature evaluate the PLKG under LoS conditions, e.g. [73] computed an upper bound on the key generation capability of two users communicating under LOS condition. However, they considered the case in which the eavesdropper is capable of estimating the LOS component, and they assumed perfect channel reciprocity.

In this section, the performance of the PLKG is assessed through the computation of the SKR. Monte Carlo simulations have been performed in real-like general conditions with the aim of estimating the SKR in a LOS wireless link. In addition, Eve is assumed to be present, who sees the channel from Alice with a low, but not zero, correlation: the correlation matrix of the Alice-Bob, the Alice-Eve and the Bob-Eve channel is an input parameter of the simulation. The simulations are performed with arbitrary selected values of correlation, highlighting the impact of the correlation and the dominant component, without focusing on a specific channel model. Moreover, instead of the mutual information the entire SKR, with its upper and lower bound, is computed. Additionally, the channels are generated according to a realistic 3GPP channel model. Furthermore, the reciprocity is not assumed to be perfect and the impact of non-ideal reciprocity is taken into account by generating highly correlated channels between the legitimate users, but not equals. The simulations are repeated for different channel

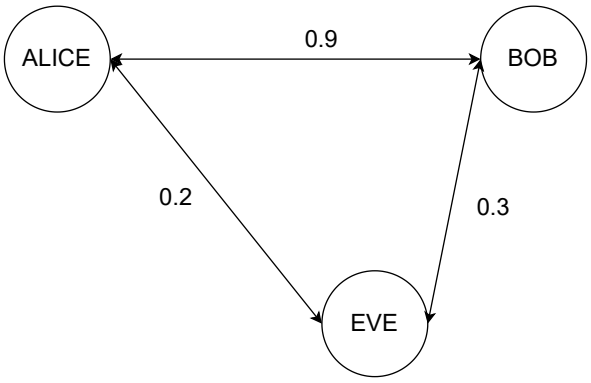


Figure 2.20: General scheme of Alice Bob and Eve on the channel: each pair of users see the channel realizations with a different non-zero correlation. From [74].

conditions: different Rice factor K, SNR, Delay Spread (DS).

2.4.1 Methodology

The main goal of the work is to assess the value of the SKR under different channel conditions in a system where the encryption keys are generated according to the previously explained PLKG protocol. Figure 2.20 outlines the presence of the users in the channel, with particular stress on the mutual correlation, whereas a summary of the simulation parameters is reported in Table 2.1. The target observation is the frequency response of the channel, processed through the filterbank method [75]. Therefore, the vectors of channel observations X^A, X^B, X^E consist of the output of the N_f filters applied to the Power Spectral Density (PSD). Moreover, the filters are supposed to be ideal pass band filters and the PSD is obtained through the square Fast Fourier Transform (FFT) of the CIR, which is generated according to a wideband Tapped Delay Model [76], where it is possible to tune the DS and the Rice factor K. Furthermore, the PSD observed by Alice Bob and Eve are generated according to some mutual correlation target. This is accomplished through the Cholesky Decomposition. Channels are generated in order to achieve a bandwidth of 160 MHz.

The SKR is computed through a Monte Carlo simulation: 5×10^5 channel realizations are generated for the same input values (DS and rice factor K) and the SKR is computed case by case according to (1.17) and (1.18).

A scheme of the simulation procedure is sketched in Figure 2.21. The first block in the simulation flow chart refers to a parameter file listing the parameters required by each simulation snapshot. The main parameters are reported in Table 2.1.

The wireless channel is generated according to the TDL "TDL-D" model described in [76]. It is a statistical channel model and consists of a set of paths with a normalized delay and power, which can be tuned to account for different propagation conditions. In particular, the channel model accounts for multipath Rice fading, i.e. the Rice factor and the DS are the tuning parameters of the model.

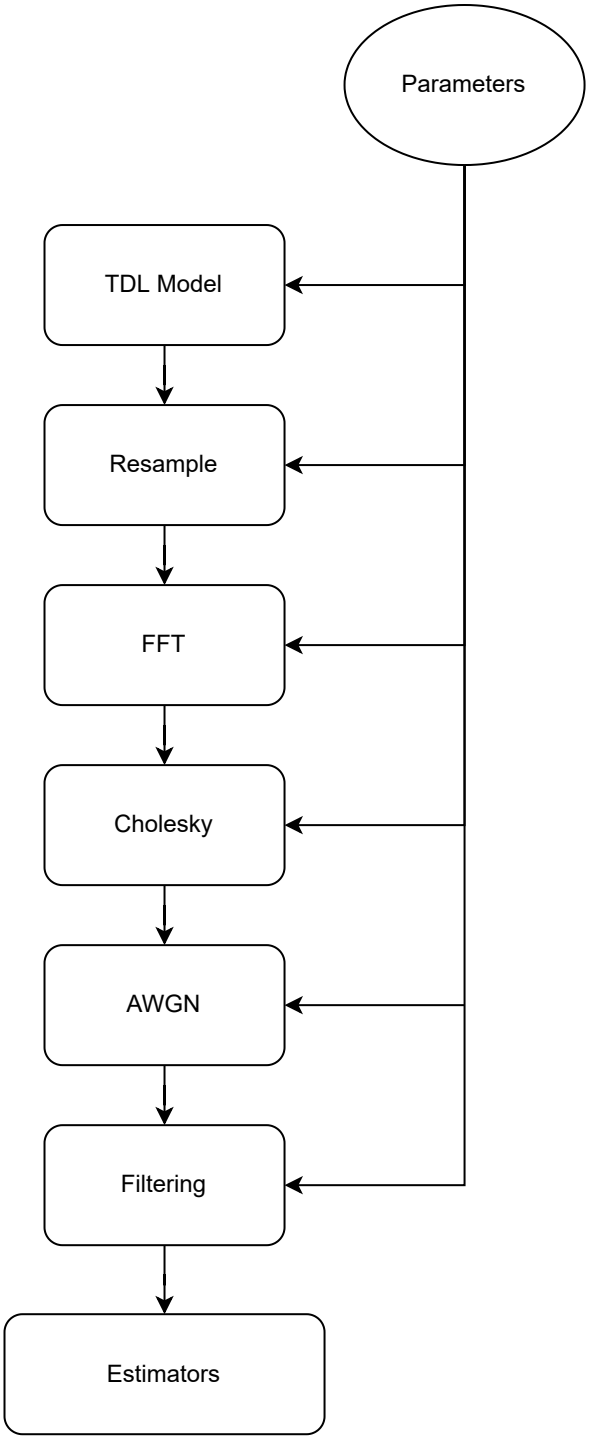


Figure 2.21: Diagram of the simulation. From [74].

Table 2.1: Main simulation parameters. From [74]

Parameter	Value
Bandwidth (MHz)	160
Sampling time	2 $\times 10^{-9}$ s
SNR reference value (dB)	10
SNR (dB)	from 0 to 30 with step of 2
Channel realizations	50000
Nfft	2048
Number of Filters	1 or 4
delay spread reference value (ns)	30
delay spread (ns)	[10, 30, 100, 300, 600, 1000, 2000, 5000]
K reference value (dB)	10
K array (dB)	from 0 to 30 with step of 2
Alice-Bob correlation	0.99, 0.9, 0.7
Alice-Eve / Bob -Eve correlation	0.1, 0.2, 0.7

To generate the channel realizations, the following procedure has been applied, as also described in [76]:

1. Modify the power and the delays of the TDL according to the procedure described at page 83 of [76], in order to have a given Rice Factor K and a DS.
2. As for the first line of the TDL, the component is generated as a Rice random variable with K-factor equal to the desired one: this represents the LOS component of the channel.
3. For each multipath line, a complex Gaussian random variable is generated, with zero-mean and a variance equal to the mean power of each line. In this way, it is possible to generate Rayleigh-fading lines with a mean power specified by the average received power of each line of the TDL.

The TDL model is then resampled in order to obtain a CIR with a continuous time axis. To this aim, a sample time is selected as the inverse of the channel bandwidth written in Table 2.1. Each delay of the TDL is transformed into the correspondent time sample, and the complex amplitudes of the taps falling within the same sample are coherently summed up.

To obtain the CTF a simple FFT is performed on the CIR, which is also zero padded to reach "Nfft" samples (see Table 2.1). For the purpose of this work, the square amplitude of the CTF, often referred to as PSD is considered. Therefore, the filtering applies to the PSD.

To explain how correlated channel samples are obtained, it can be useful studying first the simple case of correlated Gaussian samples. Let $\underline{X} = (x_1, x_2, \dots x_n)$ be an n-dimensional standard Gaussian random vector ($x_i \sim \mathcal{N}(0,1)$) made of uncorrelated samples: its covariance matrix will be the identity matrix. A set of correlated Gaus-

Table 2.2: Sumsquare error and parameters of different distributions. From [74]

Distribution	sumsquare error	parameters
gamma	0.008232	a = 42.463, loc = -1.146, scale = 0.047
lognorm	0.008412	s = 0.102, loc = -2.142, scale = 3.008
chi2	0.008457	df = 34.237, loc = -0.454, 0.038
norm	0.190884	loc = 0.881, scale = 0.311
rayleigh	1.621860	loc = 0.388, scale = 0.412

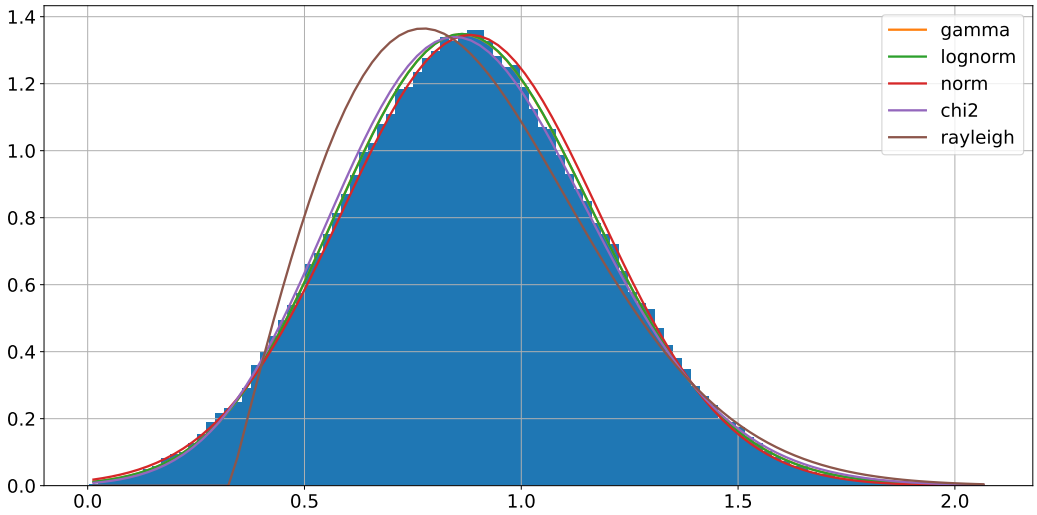


Figure 2.22: Fitting of different probability density functions to the histogram of the PSD samples. From [74]

sian random variables can be obtained applying the Cholesky decomposition on the desired correlation matrix, a method which decomposes a Hermitian matrix ($\bar{\bar{C}}$) into the product of a triangular lower ($\bar{\bar{L}}$) and a triangular upper matrix ($\bar{\bar{L}}^T$).

$$\bar{\bar{C}} = \bar{\bar{L}} \times \bar{\bar{L}}^T. \tag{2.16}$$

The vector $\bar{Y} = \bar{\bar{L}} \times \bar{X}$ will then be a Gaussian random vector with covariance matrix equals to $\bar{\bar{C}}$. The proof of this is simple and follows from the computation of the covariance matrix of $\bar{Y}$:

$$\begin{aligned} E[\bar{Y} \times \bar{Y}^T] = E[\bar{\bar{L}} \times \bar{X} \times (\bar{\bar{L}} \times \bar{X})^T] = E[\bar{\bar{L}} \times \bar{X} \times \bar{X}^T \times \bar{\bar{L}}^T] = \\ = \bar{\bar{L}} \times E[\bar{X}\bar{X}^T] \times \bar{\bar{L}}^T = \bar{\bar{L}} \times \bar{\bar{I}}_n \times \bar{\bar{L}}^T = \bar{\bar{L}} \times \bar{\bar{L}}^T = \bar{\bar{C}}. \end{aligned} \tag{2.17}$$

This method is known to be theoretically grounded for Gaussian variables, and according to [77] it is still reliable in case the variables are Gamma distributed. The Rice distribution is approximated by the Nakagami-m distribution and Gamma variables can be obtained as the square of Nakagami-m variables. By means of the `Fitter`[2]

[2] `https://pypi.org/project/fitter/`

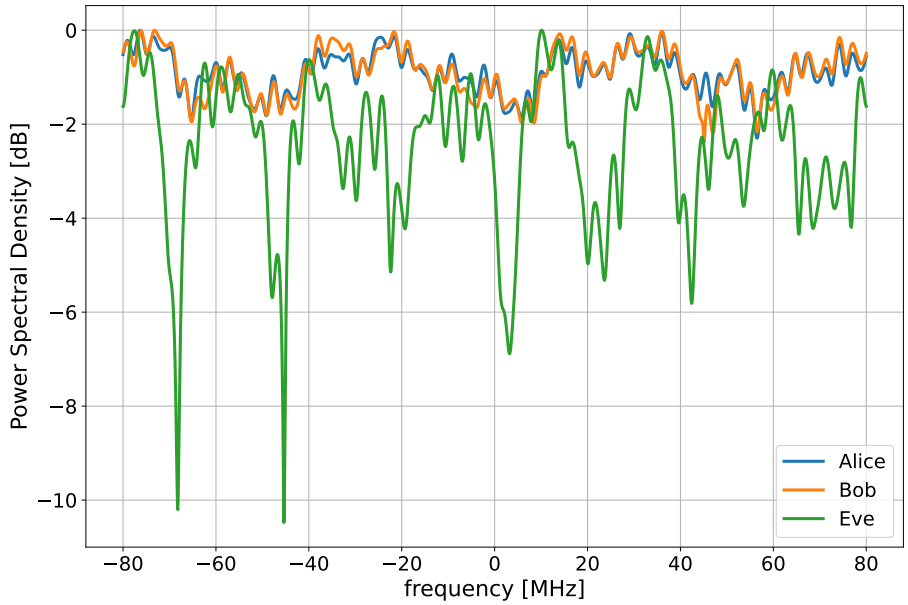


Figure 2.23: A channel realization obtained with K = 10 dB, delay spread = 30 ns, Alice - Bob correlation of 0.99, Alice-Eve and Bob-Eve correlation of 0.2. From [74]

class, the PSD samples have been fitted in order to empirically determine the distribution of the samples. By looking at Figure 2.22 and Table 2.2, where the Sumsquare error and the parameters (following the `scipy.stats` [3] notation) are reported for different distributions, the PSD samples distribution seems to fairly comply with a Gamma distribution. Therefore, it is reasonable to suppose that the PSD samples are Gamma-distributed and the method of the Cholesky decomposition is still reliable in this case. For instance, by setting the target correlation between Alice and Bob to 0.99 and the correlation between Alice/Bob and Eve to 0.1, the actual correlation levels have been then computed and turned out equal to 0.99 and 0.09.

If the matrix $\bar{\bar{C}} = \bar{\bar{L}} \times \bar{\bar{L}}^T$ is the desired correlation matrix, A'_i, B'_i, E'_i are respectively Alice's, Bob's and Eve's independent i-th realization of the PSD, the correlated channels (A_i, B_i, E_i) are obtained through a matrix multiplication:

$$\begin{bmatrix} a_{i;0} & \dots & a_{i;M} \\ b_{i;0} & \dots & b_{i;M} \\ e_{i;0} & \dots & e_{i;M} \end{bmatrix} = \bar{\bar{\mathbf{L}}} \times \begin{bmatrix} a'_{i;0} & \dots & a'_{i;M} \\ b'_{i;0} & \dots & b'_{i;M} \\ e'_{i;0} & \dots & e'_{i;M} \end{bmatrix} \tag{2.18}$$

As an example, Figure 2.23 depicts an example of channel realization, showing that for high Alice-Bob correlation the channels in frequency are quite similar, instead Eve observes an uncorrelated channel.

[3] `https://docs.scipy.org/doc/scipy/tutorial/stats.html`

After the correlation of the channel, Additive White Gaussian Noise (AWGN) is added to the PSD according to the SNR reported in Table 2.1.

The SKR is computed on the PSD after the filterbank [75] method is applied. For the purpose of this project the filters are assumed to be ideal pass-band filters. Each filter acts as a mean operator on the sub band of the PSD (or the entire PSD in case 1 filter is employed), hence the output of a filter is a single number. In practise, if $P(f)$ is the PSD, f_i is the central frequency of the i-th filter and Δf its pass band, then the output of the filter is computed as follows:

$$X_i = \frac{1}{\Delta f} \int_{f_i - \Delta f/2}^{f_i + \Delta f/2} P(f)\, df \quad i = 1, 2, \ldots, N_f. \tag{2.19}$$

Mutual Information estimators have been employed to get the mutual information required for the computation of the SKR. In particular, the Non-Parametric Entropy Estimator Toolbox[4] has been exploited, a python open source estimator of the mutual information based on the channel samples vectors. Moreover, it allows estimating the mutual information for a multidimensional sample. However, the estimator requires an exponential number of samples as the dimensionality increases (a problem known as the Curse of dimensionality [78]): therefore, the number of dimensions (number of filters of the filterbank) must be kept low. For the purpose of this work, it has been seen that by using 500000 channel realizations the estimators already converge.

2.4.2 Preliminary Gaussian Assessment

A preliminary assessment has been carried out in the Gaussian case, as the mutual information between Gaussian vectors can be expressed through analytical, closed-form formulas. The primary goal is to determine the correct behaviour of the mutual information estimators.

Consider two Gaussian signals affected by AWGN:

$$A = s_a + n_a, \tag{2.20}$$

$$B = s_b + n_b, \tag{2.21}$$

where $s_a, s_b \sim \mathcal{N}(0, 1)$, $n_a \sim \mathcal{N}(0, \sigma_a)$ and $n_b \sim \mathcal{N}(0, \sigma_b)$ and $\mathrm{corr}(s_a, s_b) = \eta$. Since A and B are sum of zero mean Gaussian random variable, they will be both Gaussian with a variance respectively σ_A and σ_B. The mutual information between A and B can be therefore expressed as:

$$\mathbb{I}(A;\, B) \;=\; h(A) + h(B) + h(A, B) \;=\; \frac{1}{2} \log_2 \left(\frac{\sigma_A^2 \sigma_B^2}{\sigma_A^2 \sigma_B^2 - \eta^2} \right). \tag{2.22}$$

In order to test the estimators, the following procedure is employed. First, independent Gaussian signals are generated, then a correlation matrix is applied. After the generation, AWGN is added to the signals:

[4] `https://github.com/gregversteeg/NPEET`

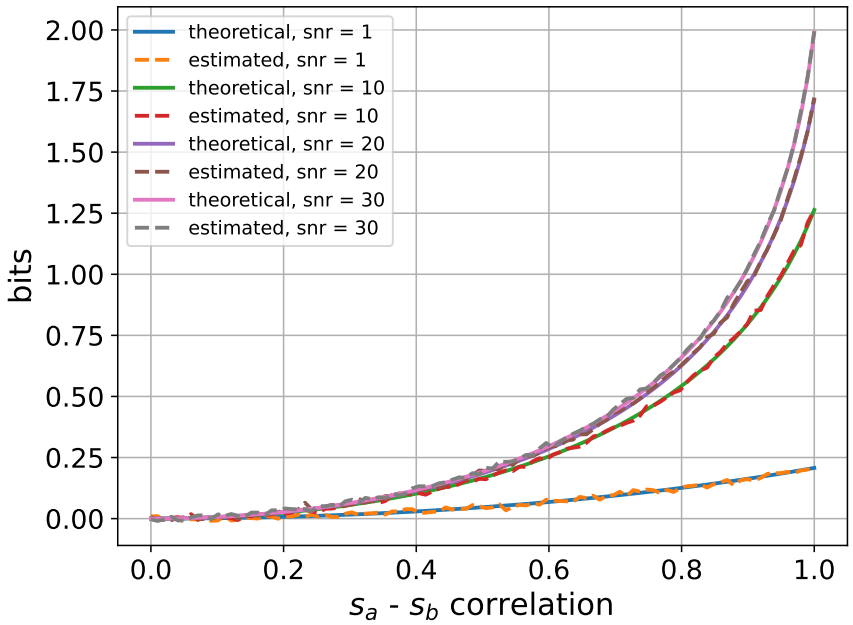


Figure 2.24: Comparison between the theoretical and estimated Mutual Information in the correlated Gaussian case, with different SNR conditions. From [74].

$$\bar{X}_1 \sim \mathcal{N}(0,1), \tag{2.23}$$
$$\bar{X}_2 \sim \mathcal{N}(0,1), \tag{2.24}$$
$$\bar{n_a} \sim \mathcal{N}(0,\sigma_a), \tag{2.25}$$
$$\bar{n_b} \sim \mathcal{N}(0,\sigma_b), \tag{2.26}$$
$$\bar{s_a} = \bar{X}_1, \tag{2.27}$$
$$\bar{s_b} = \eta\bar{X}_1 + \sqrt{1-\eta^2}\bar{X}_2, \tag{2.28}$$
$$\bar{A} = \bar{s_a} + \bar{n_a}, \tag{2.29}$$
$$\bar{B} = \bar{s_b} + \bar{n_b}. \tag{2.30}$$

Equation (2.28) comes from (2.16) and (2.18) when two random vectors are considered. The evaluation is repeated for different values of the correlation η: after the generation, the random vectors are given to the estimators to obtain the mutual information. Furthermore, $\bar{X}_1$ and $\bar{X}_2$ contain 500000 samples.

Figure 2.24 shows the results of the comparison. In particular, the mutual information significantly drops when the correlation is different from 1. Moreover, the estimated curves correspond to the theoretical case, confirming the correct behaviour of the estimators. Since the SKR is a combination of mutual information, the same agreement between the theory and the simulation is expected regarding the SKR. This also prove the correctness of the simulation procedure employed.

2.4.3 Results

Simulations aimed at evaluating the SKR in different channel conditions, i.e. for different values of the Rice factor K, of the DS and of the SNR. For the sake of simplicity, the legitimate and the eavesdropped channels are assumed to share the same Rice factor K and DS, as well as Eve is supposed to have the same correlation towards Alice and Bob indifferently.

Secrecy Key Rate and Rice Factor

Simulations have been run for different values of K and correlation between the wireless channels, but always with the same SNR of 10 dB and with a DS of 30 ns. In addition, the estimation has been done both for 1 filters (narrowband case, Figure 2.25) and for 4 filters (wideband case, Figure 2.26). When Alice and Bob share highly correlated channel observations the SKR lower and upper bound basically coincide: this is not surprising as they come to coincide as soon as Alice and Bob share highly correlated channel observations (as can be understood by looking at (1.17) and (1.18)). Instead, when the correlation is reduced, the two curves become distinguishable. Moreover, it is possible to highlight a decreasing trend of the SKR with the Rice Factor: for larger K, the channels are more stable and the multipath effects are reduced, the channel fluctuations are weaker, hence the overall randomness inside the channel is lower and the SKR is reduced. The reasons of this decreasing evolution of the SKR can be found by looking at Figure 2.27, which reports some PSD for different values of the Rice factor. As K increases, the channel becomes flatter, resulting in a weaker entropy and hence, in a lower SKR.

Reducing the Alice-Bob correlation also impairs the SKR, as it means that the disagreements in the bit sequences harvested from the channel become more probable because of the lower reciprocity level. A further reduction in the SKR is triggered when Eve improves her correlation with respect to Alice/Bob, as she can then better infer some information about the key, thus reducing its overall secrecy. Since the SKR represents the total number of bits that can be extracted after the filterbank method, it is normal to observe higher values when 4 filters are employed (Figure 2.26).

Secrecy Key Rate and SNR

The simulations have been then performed with respect to the SNR experienced by Alice and Bob, whereas the SNR of Eve is always kept to 10 dB, the DS is 30 ns and the Rice factor has been set to 10 dB. Once again, the simulations are repeated for different values of correlation.

Figure 2.28 depicts the SKR as a function of the SNR with 1 filter, while Figure 2.29 shows the situation with 4 filters. In line with the Gaussian case, the SKR increases with the SNR, as a stronger noise between Alice and Bob of course affects the channel reciprocity, thus increasing the probability of disagreement between the key they finally get from the channel observations. The sensitivity to the channels' correlation high-

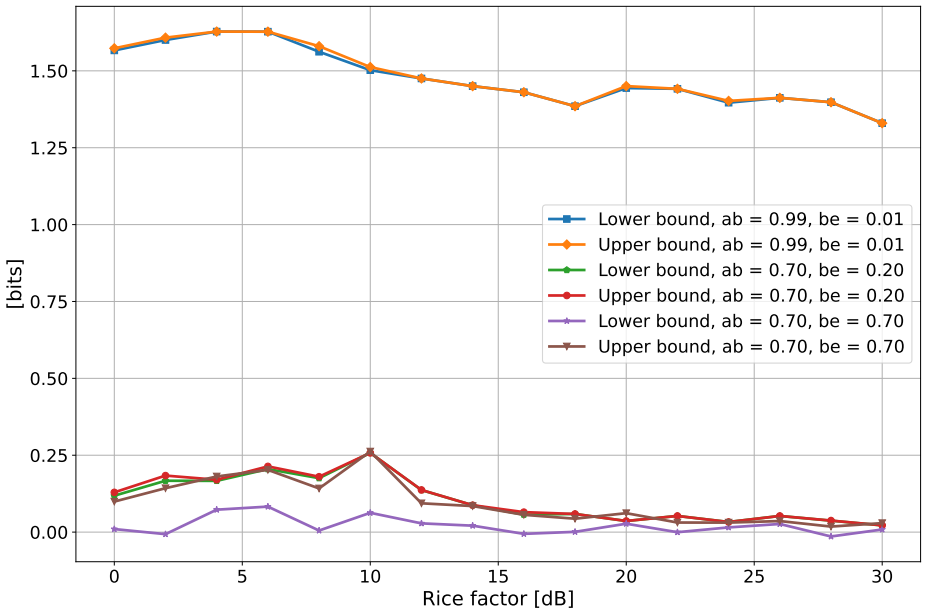


Figure 2.25: Secrecy Key Rate as a function of the Rice Factor K, for different values of the correlation and with 1 filter. In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

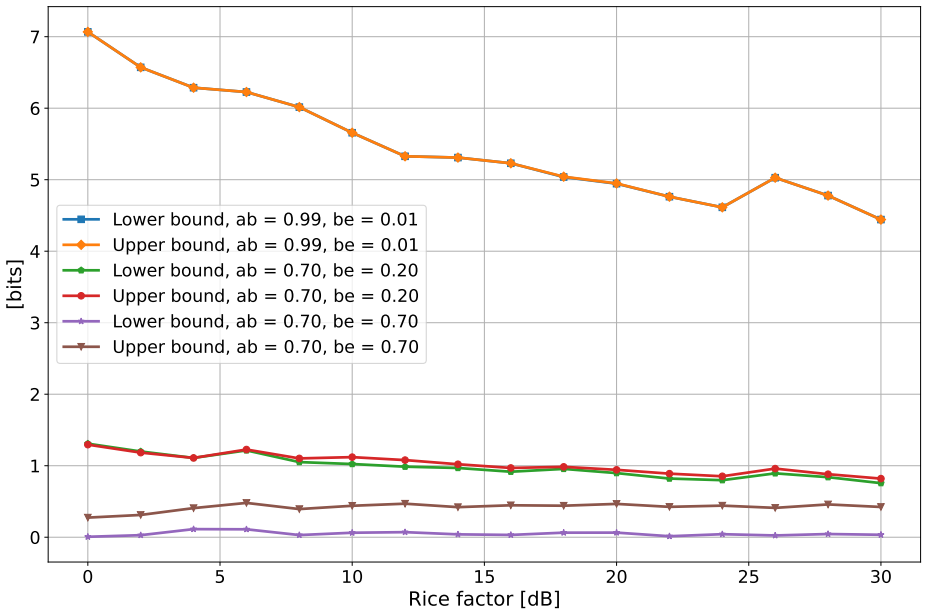


Figure 2.26: Secrecy Key Rate as a function of the Rice Factor K, for different values of the correlation and with 4 filters. In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

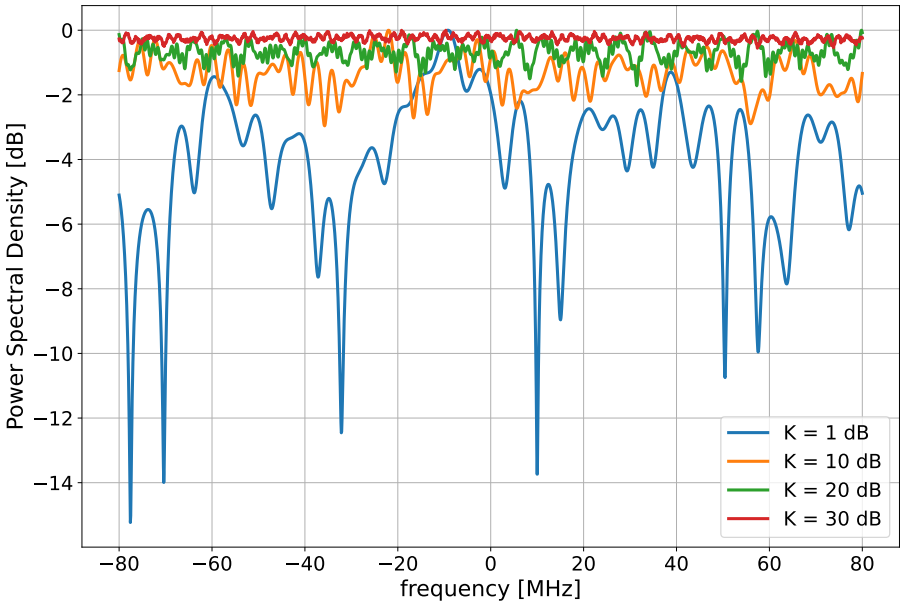


Figure 2.27: Power Spectral Densities with different value of the Rice Factor K. From [74]

lighted in Figure 2.28 and 2.29 is of course the same already discussed with reference to Figure 2.25 and 2.26.

Secrecy Key Rate and Delay Spread

As a last case, the simulations have been performed fixing both the SNR and the Rice factor at 10 dB, but varying the DS of the channel.

As for the case with 1 filter, depicted in Figure 2.30, it is possible to notice that the DS does not seem to have a big impact on the SKR. Conversely, the SKR tends to decrease with increasing DS, when multiple filters are employed (Figure 2.31). This trend is also in line with what has been reported in [70].

The reason for this behaviour can be understood by looking at Figure 2.32 and bearing in mind that the number of paths in the TDL is fixed: when the DS is low, there is higher probability that the different paths cannot be resolved singularly, therefore they might severely interfere and create deep null in the PSD. By contrast, when the DS is larger, the different paths are spread over a wider delay range, and therefore they less frequently add up coherently inside the PSD, thus corresponding to a more oscillating PSD, but without deep fades.

In terms of entropy of the channel, and hence mutual information between Alice and Bob, having deep fades increases the randomness of the channel, translating in a higher SKR. Moreover, the effect of the deep fades is somehow mitigated in case of one single filter, since it blunts the effects due to the presence of deep fades by averaging the

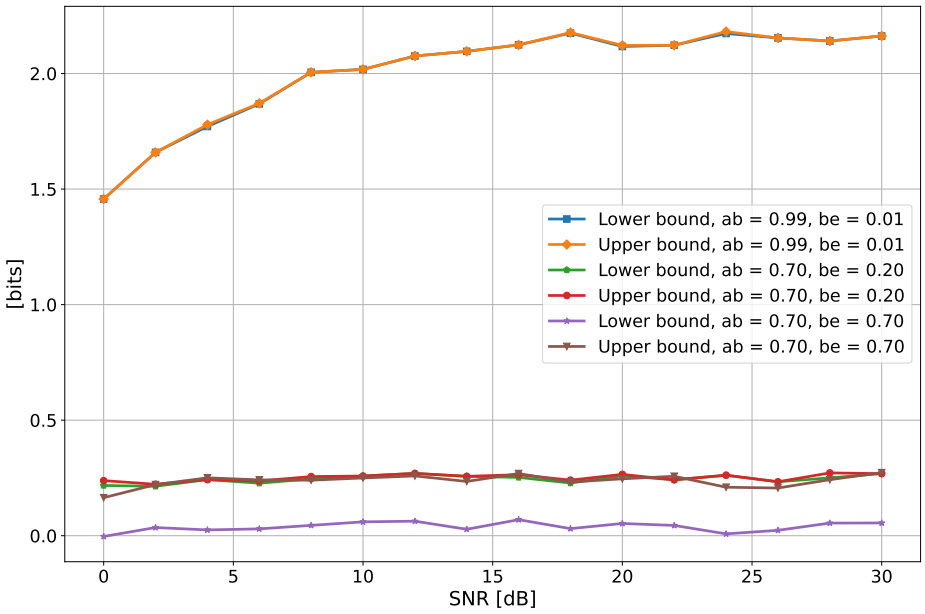


Figure 2.28: Secrecy Key Rate as a function of the SNR of Alice and Bob, for different values of the correlation and with 4 filters. In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

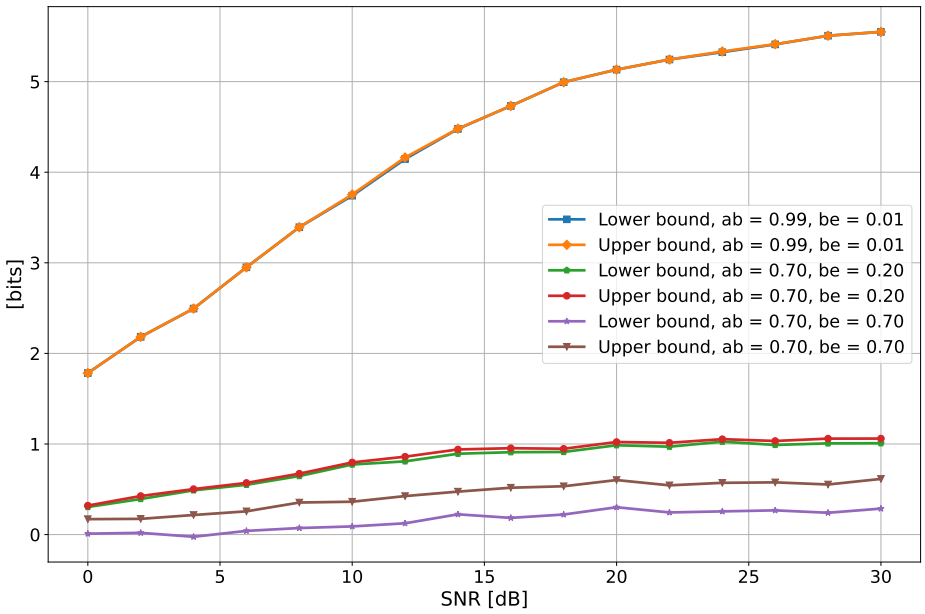


Figure 2.29: Secrecy Key Rate as a function of the SNR of Alice and Bob, for different values of the correlation and with 4 filters. In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

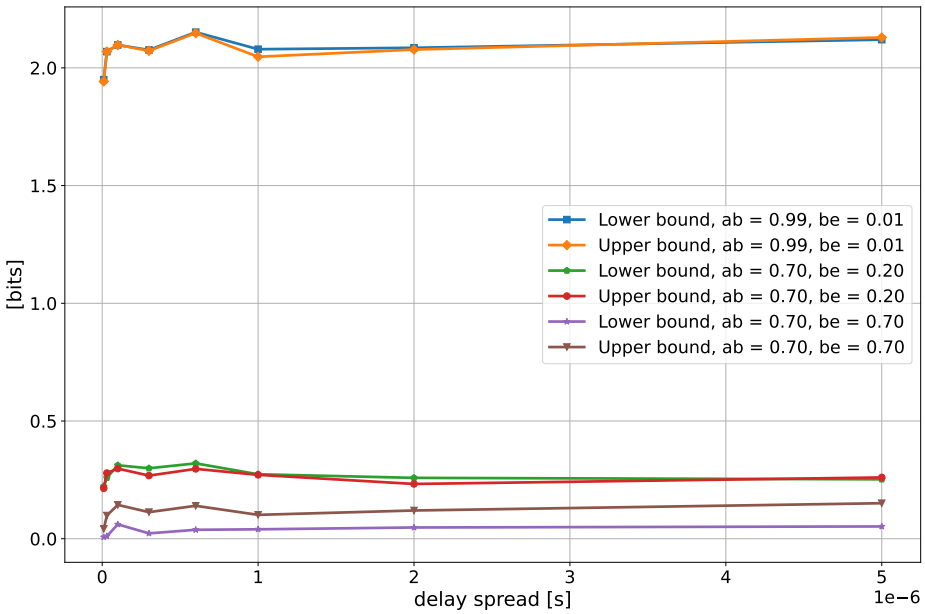


Figure 2.30: Secrecy Key Rate as a function of the Delay Spread of the channel of Alice and Bob, for different values of the correlation and with 1 filter. In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

PSD over the whole signal bandwidth. Instead, when 4 filters are employed, the deep fades in case of low DS creates more variability on the filter outputs, introducing more entropy.

In conclusion, SKR has been computed consider a realistic channel model, highlighting the impact of different channel parameters on the effectiveness of PLKG.

2.5 Final Remarks

In this chapter, an analysis of the spatial correlation properties in wireless channels is provided. In particular, through measurements and mathematical models, it can be shown that classical Jake's-like models are not suitable for all the environments and propagation characteristics. At the same time, a new theoretical model is provided and a first validity assessment is conducted. Moreover, the impact of spatial correlation on PLKG is studied, showing that in presence of an Eavesdropper PLKG should be used carefully, employing solutions that respect the actual SKR of the communication system.

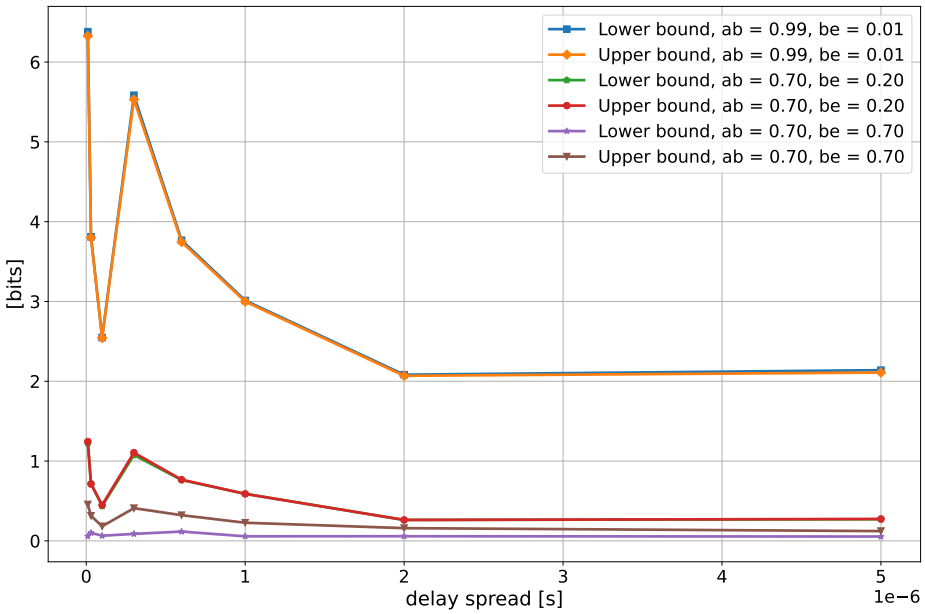


Figure 2.31: Secrecy Key Rate as a function of the Delay Spread of the channel of Alice and Bob, for different values of the correlation and with 1 filters In the legend, "ab" and "be" stand for Alice-Bob correlation and Bob-Eve correlation. From [74].

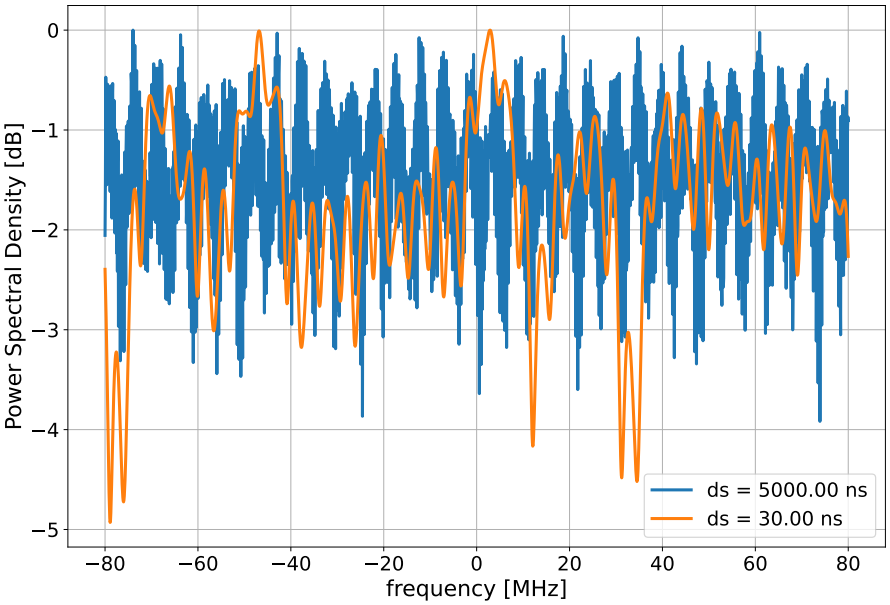


Figure 2.32: A realization of Power Spectral Density with different Delay Spread. From [74].

3

Frequency Diverse Array for Physical Layer Security

In the previous chapters, the concepts of PLS is introduced, and an analysis of PLKG and spatial correlation is provided. However, other techniques can be employed to improve communication security. In this chapter, the usage of FDA is proposed to protect the security. FDA are antenna solutions that employ a small frequency shift among the array elements to produce an angle and range dependant beam pattern, hence confining the power in a limited area of the space. This solution seems interesting from the security point of view, since the field can be received only inside a limited area of the environment. First, a complete introduction of the FDA is provided, with their peculiar characteristics. Then, the concept of *Geofencing* is introduced. Then, a small digression on the challenges of FDA in real scenarios is proposed. In the end, an analysis of the impact of array design parameters on the produced beam pattern is provided, aiming at giving some hints on how to design an FDA for secure communications.

3.1 Introduction to Frequency Diverse Array

A transmitting antenna array is referred to as FDA if the different radiating elements are supplied by feeding signals at different frequencies [79, 80]. Frequency diversity enables "power spatial focusing", i.e. the possibility for the radiated field to peak around some target point(s). Therefore, the field peaks at some specific distance in some specific direction and at some instants of time [79–82]. In principle, this corresponds to a better control of the transmitted power spatial distribution compared to standard phased array, which can only enforce "beam angular steering", i.e. boost the electromagnetic radiation in some privileged, spatial direction(s). Nevertheless, the array solution can increase the field intensity of a single radiating element by a factor always equal to the number of radiating elements at most, regardless of whether the array is frequency diverse or not. Therefore, the real advantage brought by FDA compared to standard arrays is not a further boost of intensity in the target point, but

rather a lower intensity outside the target spot.

FDA techniques have been mainly envisaged for radar and navigation [79, 80, 83–86], and they have been recently proposed for Wireless Power Transfer (WPT) [87, 88]. Moreover, the focus capability of the FDA technologies might suggest its usage for signal Geofencing. In the framework of wireless communication systems, Geofencing refers to the possibility of confining the RF signals to a specified limited area. Signal Geofencing can be employed, for example, in medical observation for pandemic control [89] or elderly patient tracking [90], or in unnamed aerial vehicles' navigation [91] and logistic [92]. Signal Geofencing can be potentially beneficial in a twofold way, i.e. to manage interference issues and to enforce communications secrecy [93–95]. As a matter of fact, limiting the intensity of the transmitted signal outside a spot placed on the target receiver also reduces the interference brought to other users. At the same time, providing a satisfactory SNR ratio only at the target receiver can also limit the access of possible eavesdroppers to the information content exchanged by two legitimate users. In terms of PLS, this technique allows boosting secrecy capacity, since it reduces the eavesdropper channel SNR (as can be understood by looking at (1.3)). Of course, FDA techniques for both secrecy and interference control require information about the users' position, i.e. they belong to the class of *location aware* wireless applications [96, 97]. However, wireless positioning has been gaining increasing interest over the years, to the extent that it is now a common feature of many user equipment. Indoor localization performance might be still imprecise in some cases - mostly because of obstruction and multipath impairments - but technical progress (e.g. based on Machine Learning) is expected to further improve indoor positioning accuracy [98, 99].

3.1.1 Mathematical Description of Frequency Diverse Array

FDA principle consists of modulating the feeding signal with different central frequencies, in order to achieve a range dependent Array Factor (AF). If the array consists of M elements, the feeding signal of the m-th element can be expressed as:

$$\begin{aligned} s_m(t) &= S_m \cos(2\pi f_m t + \delta_m) \\ &= S_m \cos[2\pi(f_0 + \Delta f_m)t + \delta_m], \end{aligned} \tag{3.1}$$

where Δf_m is the frequency increase at the m-th element ($m = 0, 1 \ldots M-1$) with respect to the single, reference element (herein conventionally labelled with $m = 0$). Frequencies are usually deployed over the array according to either a linear or a logarithmic policy [79], i.e.:

$$\Delta f_m = m\Delta f, \tag{3.2}$$

$$\Delta f_m = \log(m+1)\Delta f, \tag{3.3}$$

being Δf a fixed frequency offset. Although the different frequencies are usually assigned to the array elements according to a simple, incremental scheme (i.e. the increase Δf_m applied to the m-th element), solutions based on a random distribution of the

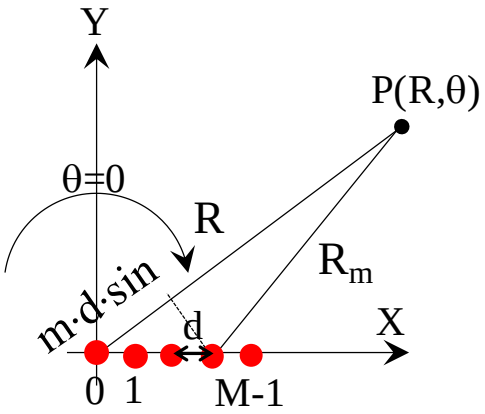


Figure 3.1: Deployment of a Linear FDA. Picture from ©2024 IEEE [101].

frequencies across the array (i.e. the increase Δf_m applied to the m'-th element, with m in general different from m') have been also investigated [100].

The free space, far-field radiated by an FDA can be expressed according to the classical formulation generally adopted for standard array, i.e. as the product between the field generated by the single, reference element (E_0) and a proper AF. Depending on the geometry of the array and the feeding characteristics, the radiated far field assume a different expression, hence a different shape of the beam spot can be achieved.

A general scheme of an FDA is depicted in Figure 3.1, where the array elements are placed linearly. The free space field radiated by the m-th element in $P(R, \theta)$ at time instant t can be written as:

$$e_m(R, \theta, t) = \Re\left\{\left(\frac{E_{0m}}{R_m} e^{j\delta_m} e^{-j\beta_m R_m}\right) e^{j2\pi f_m t}\right\}, \tag{3.4}$$

where E_{0m} is the complex field emitted in the θ direction, $\beta_m = 2\pi/\lambda_m$ and R_m the distance travelled by the m-th signal. In far field conditions, the signals arriving in P from each array element basically experience the same path-loss, i.e.:

$$1/R_m \approx 1/R \tag{3.5}$$

Conversely, the following expression for R_m should be considered in the exponential to account for the phase shift due to propagation:

$$R_m \approx R - md \sin\theta, \tag{3.6}$$

being d the spacing between the elements, and:

$$\frac{1}{\lambda_m} = \frac{f_m}{c} = \frac{f_0}{c} + \frac{\Delta f_m}{c}. \tag{3.7}$$

The field $e_m(R,\theta,t)$ can be then expressed as:

$$\begin{aligned} e_m(R,\theta,t) &= \Re\left\{\left(\frac{E_{0m}}{R}e^{j\delta_m}e^{-j\overbrace{\frac{2\pi f_0}{c}}^{\beta_0}R}e^{j\frac{2\pi m f_0 d\sin\theta}{c}}e^{-j\frac{2\pi\Delta f_m(R-md\sin\theta)}{c}}e^{j2\pi\Delta f_m t}\right)e^{j2\pi f_0 t}\right\} \\ &= \Re\left\{\left(\frac{E_{0m}}{R}e^{-j\beta_0 R}\right)\left(e^{j\delta_m}e^{j\frac{2\pi m f_0 d\sin\theta}{c}}e^{-j\frac{2\pi\Delta f_m(R-md\sin\theta)}{c}}e^{j2\pi\Delta f_m t}\right)e^{j2\pi f_0 t}\right\}. \end{aligned} \tag{3.8}$$

Finally, the total field radiated by the FDA in P at time t can be computed as the sum of the fields from each element, where $E_{0m}\approx E_0$ is here also assumed:

$$\begin{aligned} e(R,\theta,t) &= \sum_{m=0}^{M-1}\Re\left\{\left(\frac{E_0}{R}e^{-j\beta_0 R}\right)\left(e^{j\delta_m}e^{j\frac{2\pi f_0 m d\sin\theta}{c}}e^{-j\frac{2\pi\Delta f_m(R-md\sin\theta)}{c}}e^{j2\pi\Delta f_m t}\right)e^{j2\pi f_0 t}\right\} \\ &= \Re\left\{\left(\underbrace{\frac{E_0}{R}e^{-j\beta_0 R}}_{E_0(P)}\right)\left[\underbrace{\sum_{m=0}^{M-1}e^{j\delta_m}e^{j\frac{2\pi f_0 m d\sin\theta}{c}}e^{-j\frac{2\pi\Delta f_m(R-md\sin\theta)}{c}}e^{j2\pi\Delta f_m t}}_{AF(P,t)}\right]e^{j2\pi f_0 t}\right\}. \end{aligned} \tag{3.9}$$

The total, complex field $e(P,t)$ therefore corresponds to the product of the complex field radiated by the single, reference element ($E_0(P)$ in (3.9)) and a complex array factor $AF(P,t)$ equal to:

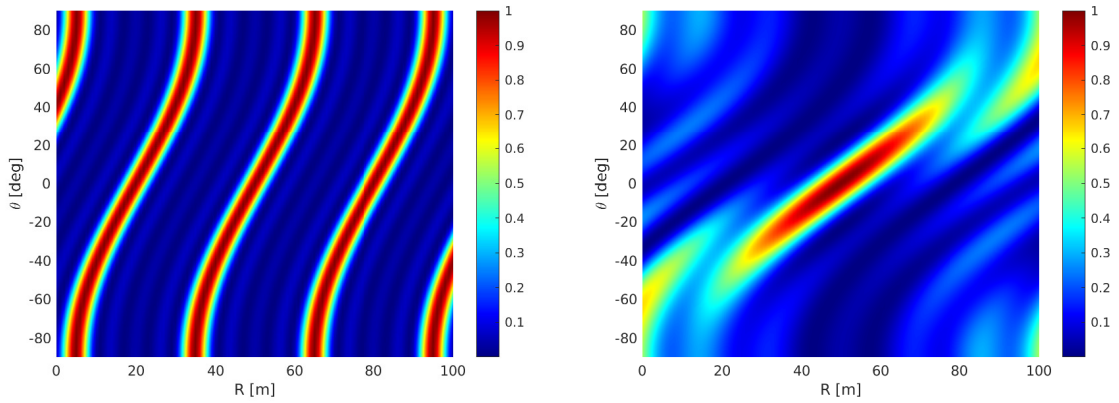
$$AF(R,\theta,t) = \sum_{m=0}^{M-1}e^{j\delta_m}e^{j\frac{2\pi f_0 m d\sin\theta}{c}}e^{-j\frac{2\pi\Delta f_m(R-md\sin\theta)}{c}}e^{j2\pi\Delta f_m t}. \tag{3.10}$$

Therefore, even though FDA allows confining the field in a limited area, the created spot moves in time. In fact, the produced Array Factor depends on distance, angle, but also time, in a periodic way. In addition, based on the employed frequency shift, spatial repetitions of the spot arise, as shown Figure 3.2. Moreover, the frequency shift choice determines the shape of the spot and the period. When a linear increment is employed, the AF assumes an S-shaped spot (Figure 3.2a), while with logarithmic increase it assumes a rounder shape (Figure 3.2b).

If the goal of the FDA is to make the field peaking in a target point, $P_t(R_t,\theta_t)$ the phase δ_m of the signal feeding the $m-th$ element must be set as follows:

$$\delta_m^{peak} = \beta_0 R_t - \frac{2\pi m f_0 d\sin\theta_t}{c} + 2\pi\frac{\Delta f_m}{c}\left[R_t-(m)d\sin\theta_t\right] - 2\pi\Delta f_m t. \tag{3.11}$$

According to (3.11) the phase coefficients should be continuously tuned over time to keep the peak of the field on P_t. In case of static target, the phase values must linearly change over time, thus corresponding to a saw-tooth phase modulation profile.



(a) AF with linear increment. **(b)** AF with logarithmic increment.

Figure 3.2: Example of AF produced by a Linear FDA, with linear and logarithmic increase. Picture from ©2024 IEEE [101].

Conversely, the phase-time relationship turns out much harder in case P_t is moving (i.e. in mobile wireless communications), hence accurate and up-to-date information on the target point position are required to the transmitting FDA. This issue is mitigated in case mobility occurs at somehow constant speed and along the same, specific track, as for instance in railways [102]. In order to reduce the complexity of the phase tuning procedure, the peak condition is often limited to some instant t_0 (usually set as $t_0 = 0$ for the sake of simplicity [79]), i.e.:

$$\delta_m^{peak} = \beta_0 R_t - \frac{2\pi m f_0 d \sin\theta_t}{c} + 2\pi \frac{\Delta f_m}{c} \left[R_t - md \sin\theta_t\right] - 2\pi \Delta f_m t_0. \tag{3.12}$$

In order that two legitimate users can effectively exchange some information through the FDA communications, the field should steadily peak in the target receiving location P_t for a time (much) greater than the symbol length. Of course, this requirement is automatically met if the phases can be set according to (3.11), as the field peak will be then steadily placed on P_t. By contrast, if the condition in (3.12) is instead enforced, the array factor is going to change over time at a rate related to Δf_m (as highlighted in (3.10)), and the following relation should be therefore fulfilled (also in agreement with [79]):

$$\Delta f_m \ll B \ll f_0, \quad \forall m \tag{3.13}$$

Planar Array

With reference to the planar deployment shown in Figure 3.3 let N and M be the number of elements along the X and the Z axis, respectively, whereas d_x and d_z are the corresponding spacings. The feeding frequency does not change along X axis, but only along Z axis: the FDA characteristic (the frequency shift) is applied along the column, while elements in a row share the same operating frequency. The distance

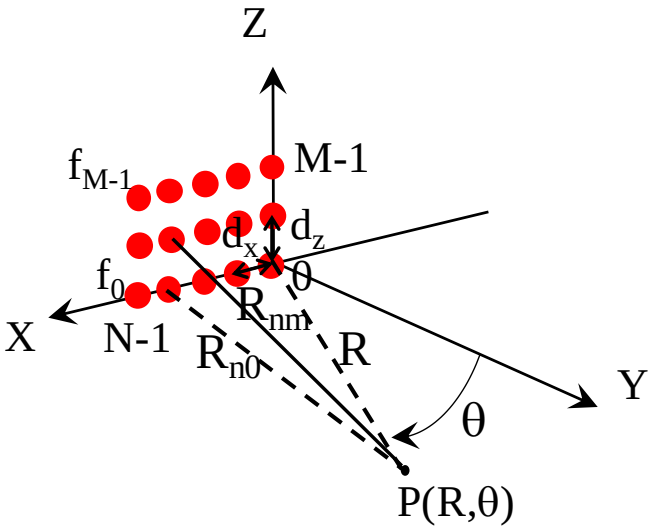


Figure 3.3: Planar deployment of an FDA. Picture from ©2024 IEEE [101].

between the (n, m) element on the grid and the point P can be clearly expressed as:

$$R_{nm} = \sqrt{R_{n0}^2 + (m \cdot d_z)^2}. \tag{3.14}$$

Under far-field conditions, the distance between the element $(n, 0)$ and P can be still computed as in (3.6) by simply replacing m with n and d with d_x. Then:

$$R_{nm} \approx \sqrt{(R - nd_x \sin\theta)^2 + (m \cdot d_z)^2}. \tag{3.15}$$

The array factor can be therefore expressed as:

$$\begin{aligned} AF(R, \theta, t) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} & e^{j\delta_{nm}} e^{j\frac{2\pi f_0}{c}(R_{nm} - R)} \\ & e^{-j\frac{2\pi \Delta f_m R_{nm}}{c}} e^{j2\pi \Delta f_m t}. \end{aligned} \tag{3.16}$$

An example of the |AF| with a linear increment policy is depicted in Figure 3.4.

The phase values required to set the peak in P_t at time instant t_0 can be then written as:

$$\delta_{nm} = \beta_0 R_{nm} + \frac{2\pi \Delta f_m R_{nm}}{c} - 2\pi \Delta f_m t_0. \tag{3.17}$$

Circular Deployment

In addition to the linear and the planar deployment, the circular layout reported in Figure 3.5 is also here considered. Frequency diversity is applied across the M elements over each circle, whereas the N elements on the same spoke share the same

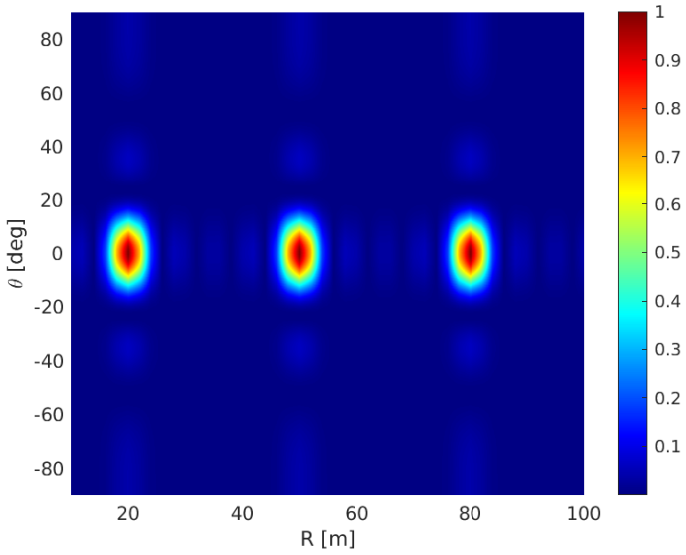


Figure 3.4: Example of the AF produced by a 5x5 Planar Array. Picture from ©2024 IEEE [101].

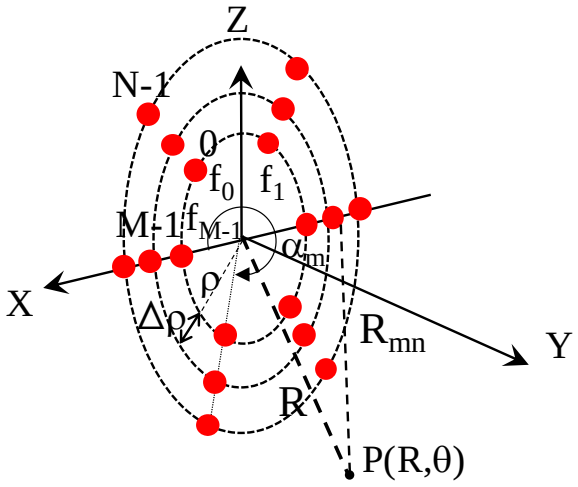
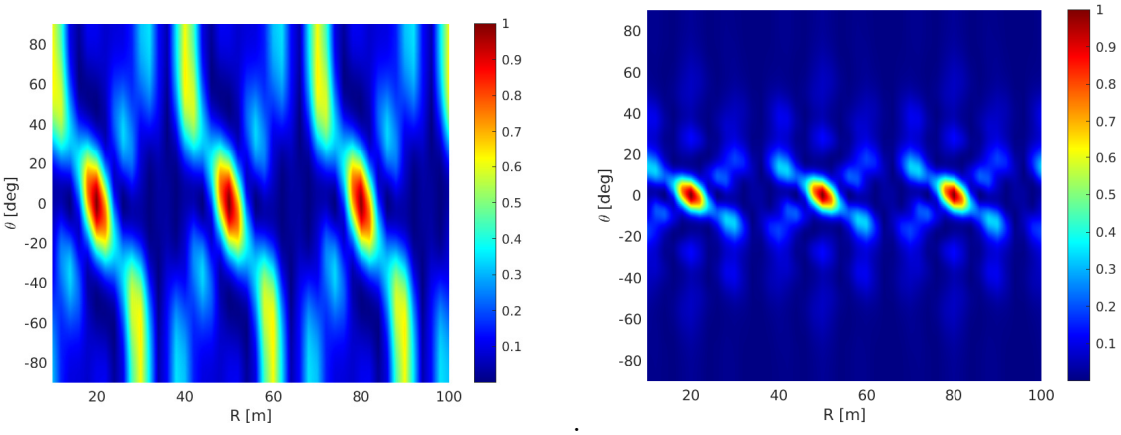


Figure 3.5: Multiple rings circular deployment of an FDA. Picture from ©2024 IEEE [101].



(a) AF with a single ring **(b)** AF with multiple rings.

Figure 3.6: Example of AF produced by a Circular FDA, with a single and multiple rings. Picture from ©2024 IEEE [101].

frequency [103]. Also, the elements are uniformly spaced in both the radial and the angular direction. The far-field approximation for the element-to-point P distance and the corresponding expression of the array factor are reported in (3.18) and (3.19), respectively.

$$R_m \approx R - (\rho + n\Delta\rho)\sin\theta\cos\alpha_m. \tag{3.18}$$

$$\begin{aligned} AF(R,\theta,t) = \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} & e^{j\delta_{mn}} e^{j\frac{2\pi f_0}{c}(\rho+n\Delta\rho)\sin\theta\cos\alpha_m} \\ & e^{-j\frac{2\pi\Delta f_m}{c}(R-(\rho+n\Delta\rho)\sin\theta\cos\alpha_m))} e^{j2\pi\Delta f_m t}. \end{aligned} \tag{3.19}$$

Figure 3.6 shows the AF produced by a circular FDA.

Equation (3.19) easily provides the phase shift δ_{mn} required to set up the field peak in P_t at time instant t_0:

$$\begin{aligned} \delta_{mn} = & \beta_0 R_t + \frac{2\pi\Delta f_m}{c}\left[R_t - (\rho + n\Delta\rho)\sin\theta_t\cos\alpha_m\right] \\ & - \frac{2\pi f_0}{c}(\rho + n\Delta\rho)\sin\theta_t\cos\alpha_m - 2\pi\Delta f_m t_0. \end{aligned} \tag{3.20}$$

As a general consideration, the linear increase policy triggers the spatial repetition of the AF peak, with a spatial period of $c\,/\,\Delta f$. However, the spatial repetition of the spot due to the array factor periodicity is not simply reflected in the field spatial distribution, as the intensity of the spots increasingly fades at larger distance due to the path-loss. Therefore, multiple spots can actually reduce the FDA effectiveness to limit both the interference and the eavesdropping threat, especially in case the eavesdropper

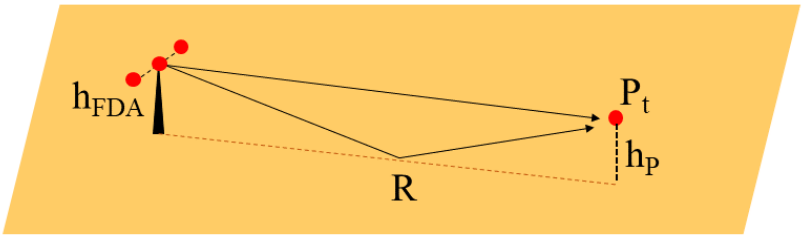


Figure 3.7: FDA propagation in presence of a PEC reflecting surface.

or the interfered user is placed on a beam spot closer to the transmitter than the target user. This occurrence can be limited if the spot spatial period is greater than the target point distance, i.e.:

$$R_t \leq \frac{c}{\Delta f} \tag{3.21}$$

3.1.2 Two-rays model for FDA

In agreement with several previous studies [79, 83, 84, 87], propagation in ideal free space conditions is usually considered in previous studies on FDA. Nevertheless, FDA might also be deployed in complex environments, where shadowing and/or multipath effects may rise up. The impact of multipath on FDA performance is here preliminary addressed in the simple case sketched in Figure 3.7, where the presence of a Perfect Electrical Conductor (PEC) reflecting surface introduces a reflected propagation path in addition to the direct contribution [104]. Compared to [105], where the main focus was not on propagation issues and the ground effect was taken into account through a random fading coefficient, a deterministic approach is here considered, which can more easily highlight the way multipath can affect Geofencing effectiveness. The final, analytical formulation achieved herein is actually rougher than the field expressions proposed in [104], but it is also clearly simpler and more reader-friendly, and therefore more suited to straightforwardly convey the message that multipath effects should be taken into account when FDA are deployed in real propagation scenarios.

Under the assumption $R >> h_{FDA}, h_{P_t}$ (Figure 3.7), the total field received at frequency f_m (E^m_{tot}) can be formally expressed through a correction factor simply applied to the free space field $\left(E^m_{fs}\right)$ [66], i.e.:

$$E^m_{tot} = E^m_{FS} \cdot CF_m = E^m_{FS} \cdot \left(1 + \Gamma_m \cdot e^{-j\beta_m \Delta r}\right), \tag{3.22}$$

where CF_m is the correction factor, Γ_m and β_m are the reflection coefficient and the wave number at frequency f_m, respectively, and $\Delta r \approx 2h_{FDA} \cdot h_{P_t}/R$. Since the reflecting surface is made of PEC, $\Gamma_m = -1$, $\forall m$. Let's also assume for the sake of simplicity that Δf_m is so smaller than f_0 (equation (3.13)) that $\beta_m \approx \beta_0$ in equation (3.22). Then:

$$E_{tot}^{m} \approx E_{FS}^{m} \cdot CF_0 = E_{FS}^{m} \cdot \left(1 - e^{-j\beta_0 \Delta r}\right). \tag{3.23}$$

Under the considered assumptions the signals received at different frequencies in presence of the ground approximately add up as they do in free space, i.e. the FDA array factor can be still leveraged to express the total received free space field, i.e.:

$$|E_{tot}(P,t)| \approx |E_0(P)| \cdot |AF(P,t)| \cdot |CF_0(P)|. \tag{3.24}$$

According to [66], the magnitude of the correction factor can be expressed as:

$$|CF_0| = \left[2\left|\sin\left(\frac{2\pi}{\lambda_0}\frac{h_{FDA} \cdot h_P}{R}\right)\right|\right]. \tag{3.25}$$

At large distance, where $sin\left(\frac{1}{R}\right) \approx \frac{1}{R}$, the interference between the direct and the reflected waves keeps steadily destructive, and the received signal intensity decreases over distance at a rate harsher than free space. At shorter distances, the presence of the PEC reflecting surface introduces fluctuations on the received signal strength in both the frequency and the range domains, depending on whether the interference is constructive or destructive. In case it turns out destructive in P_t, the total received field can be dramatically weak regardless of the array factor. This is clearly highlighted in Figure 3.8, where the same situation already considered in Figure 3.6b under free space conditions is reconsidered taking into account the PEC reflecting surface effect by means of the approximated (3.24).

To what extent FDA-based wireless application can cope with multipath propagation looks like a critical issue, which requires more accurate and specific attentions. In this respect, FDA performance and focus effectiveness in multipath and NLoS scenarios has been also preliminarily investigated in [106] through ray tracing simulations, as further discussed in the following section.

3.2 Frequency Diverse Array Propagation in Multipath Environment

As discussed before, FDA solutions have been envisaged for Radar applications and WPT and introduced as a possibility to enforce signal Geofencing. If radar systems can often benefit from friendly, free space like propagation, wireless sensors networks are often deployed in indoor scenarios, where devices are commonly placed in cluttered environments, or even in hidden and obstructed locations. Hence, multipath propagation occurs, either in LOS or in NLOS. Some studies [107, 108] have already discussed the effect of multipath propagation on FDA, even though they are basically limited to the ground effect. However, an investigation on the effect of multipath is desirable, which should take into account real-like scenarios. A first solution might be to

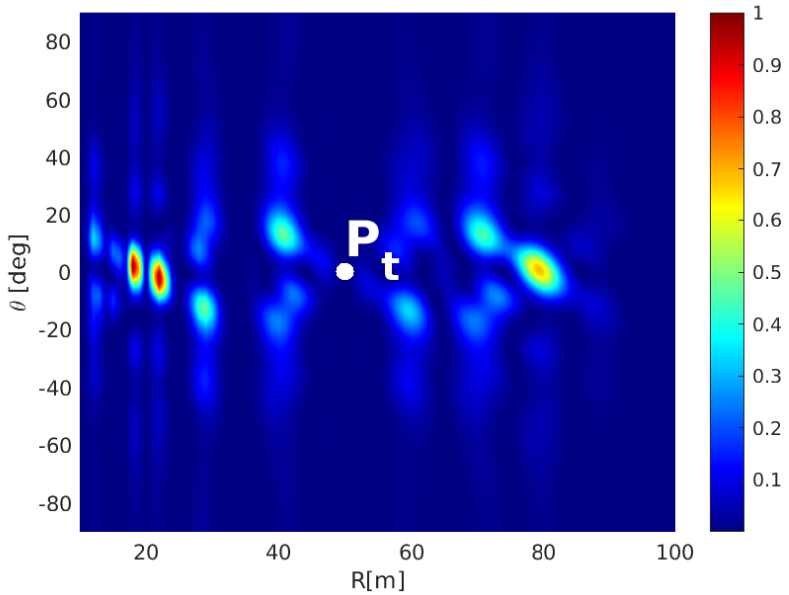
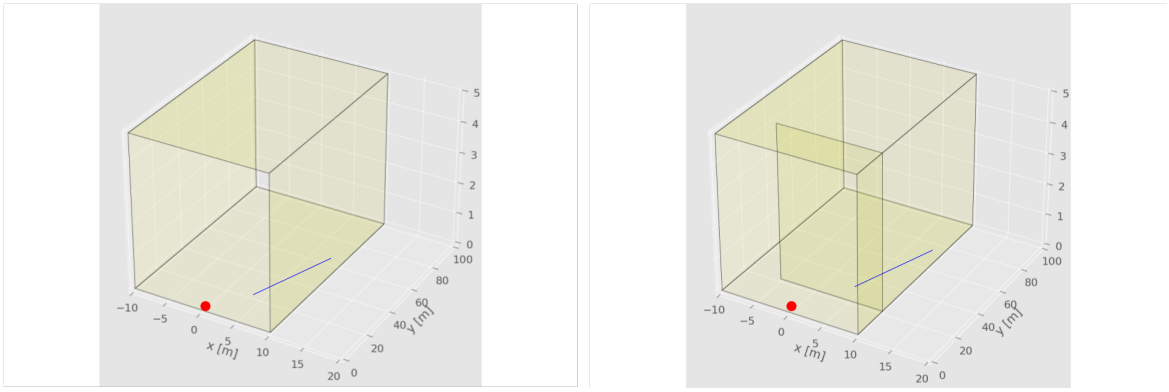


Figure 3.8: Possible effect of a PEC reflecting surface on propagation from a circular FDA with $M = N = 5$, $f_0 = 3.5\,\text{GHz}$, $\Delta f = 10\,\text{MHz}$, target point (highlighted in white in the figure) $P_t\,(50m, 0°)$ and $h_{FDA} = 3\,\text{m}$, $h_P = 1\,\text{m}$. Picture from ©2024 IEEE [101].

perform measurements with an FDA prototype, in real scenarios and in an anechoic chamber. However, this would require a significant effort, in particular to determine the shape of the spot. As a second solution, propagation can be modelled by means of an Ray Tracing (RT) algorithm, which can approximate the actual propagation in a 3-D modelled scenario. This solution has the advantage of being simpler and faster than the real measurements, it allows simulating a 3-D modelled environment and the free space-like propagation [109], then compute the received fields for a set of receiver (usually referred as Coverage Map) to get the shape of the FDA spot.

In case an FDA operates in free space-like propagation, it is possible to express the total received field in a point as the product between the field radiated by the single reference element and a proper AF, which contains the focus effect of the array. However, the AF-based formulation becomes impossible when the environment shows multipath propagation conditions. Therefore, an RT algorithm has been employed to compute the total received field in each receiving point. Inside the RT digital environment, the FDA is described by inserting multiple transmitting point distributed in space as the elements of the array. Each transmitter is treated independently by the simulation, hence mutual coupling effects are not considered. The RT simulation is repeated for each transmitter, every time changing the transmitted frequency based on the frequency shift of the array. For the sake of simplicity, the transmitters are supposed to be isotropic radiators. Simulations compute the complex field from each radiator, then the phase-shifts required to trigger the focus effect in the focus point P_t are applied to each received contribution. In this way, the fields are shifted to obtain the desired focus effect. Then, the overall field is achieved by adding up all the radiated fields.



(a) Corridor-like scenario. **(b)** Corridor-like scenario with the obstacle.

Figure 3.9: Corridor-like scenario. The red dot represents the FDA, the line represents the receiving path. Picture from ©2023 IEEE [106].

The sum is carried out in the time domain, as the received fields do not share the same frequency: therefore, a single reference time instant has been chosen, namely the time instant $t = 0$. If the array is a general $M \times N$ array, the total field in a receiving point is achieved as:

$$E_{tot} = \Re\left\{\sum_m \sum_n E_{mn} e^{2\pi f_{mn} t_0 + \delta_{mn}}\right\}, \tag{3.26}$$

where $\Re\{\cdot\}$ is the real part operator, E_{mn} is the received field from the (m, n) element, f_{mn} its frequency, and δ_{mn} the phase shift. Then, the field is multiplied by the propagation distance r, in order to filter out the effect of the propagation losses and obtain a quantity similar to an AF. Eventually, the field spatial envelope is considered, to get rid of the oscillation of the cosine function in the time field expression, and to highlight only the multipath oscillations of the field.

Inside the simulations, a corridor-like scenario has been employed, considering both LOS and NLOS conditions. As shown in Figure 3.9, the environment is composed by two lateral walls, the roof, and the ground, all supposed to be made of concrete. The corridor is 20 m wide, 100 m long and 5 m high. Moreover, to limit the direct component and enable diffraction effects, an obstacle has been placed 20 m in front of the FDA. In particular, the obstacle is a wall 15 cm thick, made of concrete, and with a length of 15 m.

In the considered scenarios, a 5x5 planar array is studied, with $\Delta f = 10$ MHz, with different focus target points. To study the propagation, a line of receivers is employed (as shown in Figure 3.9), in order to see the radial effect of the multipath and to keep affordable the computation time. In fact, to achieve good results from the RT simulation, the receivers should be very close to each other, in order to correctly sample the field oscillation due to the multipath. Hence, the number of receivers is set to be 22224, which corresponds to a pace of $\lambda/100$. Both the transmitter array and all the

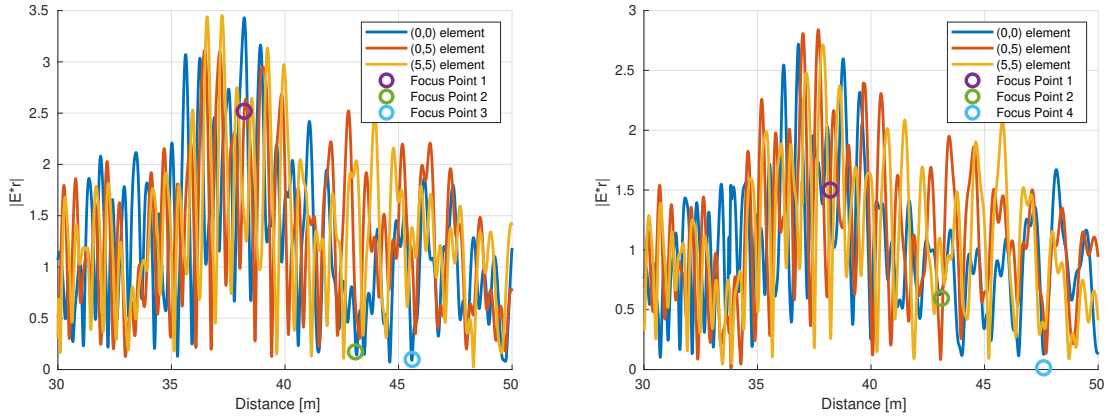
Table 3.1: Simulation parameter summary. Picture from ©2023 IEEE [106].

Parameter	Value
f0	3.5 GHz
Δf	10 MHz
ε_r	5
σ	0.01 S/m
Linear spacing	$\lambda_0/4 = 0.08$
TX and RX height	2 m
Distance simulation range	30 m - 50 m
Pt	$R_t = 38.2, 43.1$
Obstacle thickness	15 cm
Number of receivers	22224
Pace	$\lambda/100$
Focus Point 1 (R, θ)	(38.2 m, 8.59°)
Focus Point 2 (R, θ)	(43.1 m, 8.59°)
Focus Point 3 (R, θ)	(45.6 m, 8.59°)
Focus Point 4 (R, θ)	(47.6 m, 8.59°)

receivers are placed 2 m above the ground. In this case, the simulation for the corridor scenario takes around 20 minutes, while the corridor with the obstacle takes around 30 minutes, on a machine equipped with an Intel i7 12th generation CPU and 16 GB of RAM memory. A summary of the simulation parameters is reported in Table 3.1. The considered array seems to be a perfect trade-off between focus capabilities and simulation time. Simulations have been carried out choosing three focus points for each environment, named P1, P2, P3 for the corridor scenario, and P1, P2, P4 for the corridor with obstacle (Table 3.1). Figure 3.10a reports $|E| \cdot r$ for three single elements of the array in the corridor, named the $(0, 0)$, the $(0, 5)$ and the $(5, 5)$ element: it is possible to see that P1 is a point where the multipath field sums up nearly in phase with the LoS component, hence reaching a value higher than the expected value from the free space simulation. This means that the total AF should experience a peak at that point thanks to the capability to combine the effect of the different elements and gain from the multipath. P2 and P3 are locations where the AF is smaller than free space, since fields do not sum up in phase, which means that the total AF is expected to be lower than the free space one. Figure 3.10b reports the field of the same elements, but now in the corridor with obstacle. P1 and P2 show the same behaviour as before, but now P4 is a position in which the multipath fields probably does not sum up in phase.

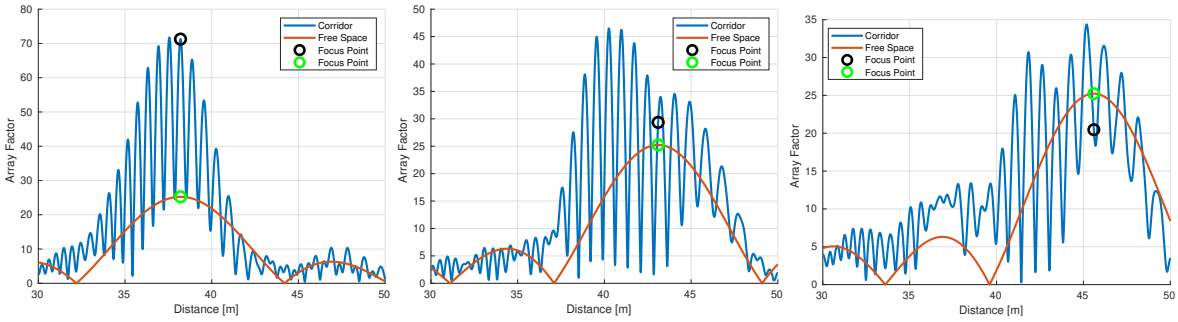
3.2.1 Simulation Results: Corridor Line of Sight

The results for the focusing in P1 are reported in Figure 3.11a: at a first sight it is possible to observe that the free space AF (red line) is a smooth line peaking in the



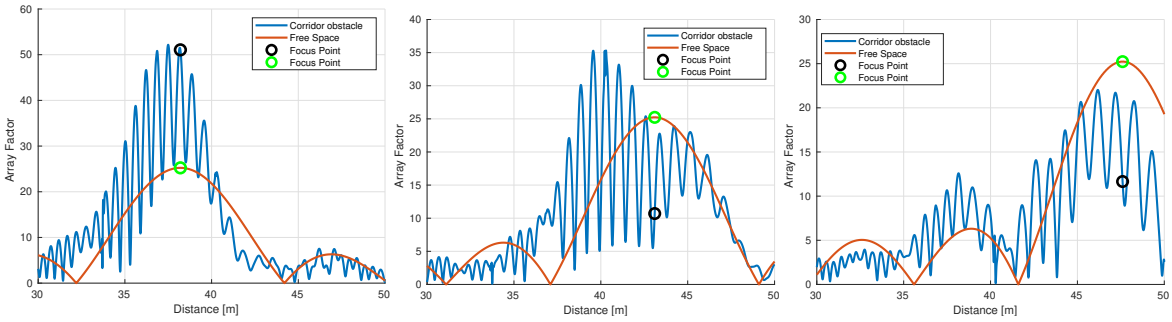
(a) Corridor scenario. **(b)** Corridor scenario with obstacle.

Figure 3.10: Spatial distribution of the normalized field radiated by the (0,0), (0,5) and (5,5) element of array. Picture from ©2023 IEEE [106].



(a) P1 **(b)** P2 **(c)** P3

Figure 3.11: Spatial envelope of the overall, normalized field propagating from the FDA inside the corridor. Picture from ©2023 IEEE [106].



(a) P1 **(b)** P2 **(c)** P4

Figure 3.12: Spatial envelope of the overall, normalized field propagating from the FDA inside the corridor with the obstacle. Picture from ©2023 IEEE [106].

focus point, while the AF in the corridor (blue line) has fast fluctuations due to the presence of the fading in the environment. In addition, the peak of the free space AF reaches the value of 25, which is the maximum achievable, according to the theory (equal to the number of elements of the array). Instead, the AF in the environment reaches a higher value with respect to the free space, mainly due to the multiple components of the field arriving at the receiver and constructively combining, thanks to the advantageous phase values. Moreover, the value of the AF oscillates, but the nulls are almost above the Free Space AF, which means that in general the user will experience a better quality of service. Lastly, the general trend of the AF follows the one of the Free Space.

Differently, in Figure 3.11b results for the focus point in P2 are reported. In this case, the AF still fluctuates, but now the fluctuations reaches values well below the Free Space AF. In addition, the shape of the AF does not fit well the one of Free Space. The same behaviour con be observed when the focus point is set in P3, Figure 3.11c, where all the elements show a low value of the received field. With respect to P1, now the AF reaches lower values in general, still having peaks above the Free Space.

As a general remark, it is possible to say that the multiple elements of the array introduce a sort of spatial and frequency diversity: although multipath interference can turn out destructive at some frequency and for some transmitting elements, it is unlikely that harsh fading occur at each frequency and over the whole array. Therefore, it seems that in many cases at least some received field contributions keep on adding up as they do in free space even when multipath shows up.

3.2.2 Simulation Result: Corridor Non-Line of Sight

Figure 3.12a reports the simulation results for the focus point in P1. This point is a location where the field of each array element still adds constructively, in fact the propagation in the corridor does not differ too much from the Free Space case: the AF peaks in the target location, although still fluctuates, and the general shape is followed. Differently, as shown in Figure 3.12b and Figure 3.12c, if we consider P2 and P4 the

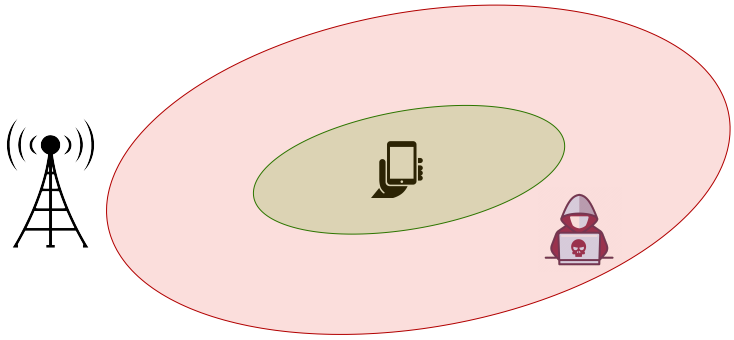


Figure 3.13: Exemplifying scheme of signal Geofencing mechanism. FDA is able to create a zone around the user where the SNR is sufficiently high, while outside the signal is not received due to the interference pattern created by the FDA.

electric field of each array element adds destructively, and the focus capabilities are blurred accordingly. In fact, the AF is first reduced, then it peaks in a different point with respect to the desired one. In addition, the null of the AF falls below the free space.

3.2.3 Final remarks

In conclusion, although FDA seems to be an interesting technology, its efficacy should be better investigated in real like scenarios. In fact, FDA in its original conceived radar applications would work in favourable conditions. Instead, when employed for WPT or possible future communication applications, the propagation might happen in more complex scenario. Although being just preliminary results, this simulative work showed that FDA focus capabilities might be impaired by real scenarios, hence deeper studies should be carried out to assess the real effectiveness of this solution for WPT or for signal Geofencing.

3.3 Geofencing Through Frequency Diverse Array

Once the basic concepts of FDA and signal Geofencing have been introduced, in order that the potential advantages offered by FDA to wireless communications become real opportunities, the size and the shape of the Geofencing area has to be carefully set. In fact, signal Geofencing takes advantage from the low possibility of a malicious user (or device) placed very close to the intended user in a wireless communication: in this way, providing a satisfactory SNR only around user's position further reduces the possibility of eavesdropping the communication. An illustrative example of Geofencing to protect communications is shown Figure 3.13.

In case the focus spot is exceedingly large, mitigation of both interference and eaves-

dropping threat might be naively impaired; conversely, if it is uselessly small, spot's placement on the target receiver could be difficult, unless very precise information about its position is available. Furthermore, it is worth pointing out that signal Geofencing provided by FDA is unavoidably time-dependent, i.e. it can be enforced at the target point at some time intervals, but not forever [81, 93], unless the phase of the feeding signals can be adaptively tuned. Although often neglected in previous studies [95, 110], this represents a crucial aspect that can cast a shadow on the real convenience of FDA for effective signal Geofencing. Nevertheless, FDA can be arranged in order that spatial focusing is periodic over time, thus supplying authorized users with multiple time slots for reliable communications, provided that synchronization is also supported. Moreover, transmission can be interrupted as soon as the array beam spot is no longer fairly placed on the target receiver, thus anyway preventing any eavesdropper from the access to private data [111].

Furthermore, in the framework of resorting to FDA to improve the privacy of communications, transmission of artificial noise to knock down the signal-to-noise ratio of possible eavesdropper has been also proposed [112, 113]. Since artificial noise of course should not be delivered to the legitimate receiver, the array factor should now have a notch in P_t. The phase δ_m of the signal feeding the $m-th$ element must be then set as:

$$\delta_m^{notch} = \delta_m^{peak}, \delta_{m+1}^{notch} = \delta_{m+1}^{peak} + \pi, \quad m = 1, 3, 5.., M-1 \tag{3.27}$$

In case large array size can be afforded, part of the array could be devoted to focus the signal on the target receiver, whereas the remaining elements could be employed to spread artificial noise all around.

Most of the existing studies on FDA for wireless communications mainly deal with effective schemes and algorithms to arrange the signals feeding the radiating elements to limit interference and/or pursue communication privacy, whereas the antenna layout is always and simply limited to the uniform linear case [81, 95, 97, 110, 114, 115]. By contrast, a thorough investigation on the impact of the main antenna array parameters (like the number of elements, their spatial deployment and spacing, the arrangement of the frequencies across them) on the Geofencing effectiveness is desirable.

Moreover, some major relationships so far not fully highlighted between signal Geofencing in the time and in the spatial domain are also addressed. The outcomes of the following investigation can provide useful design guidelines and highlight practical limitations for Geofencing applications.

3.3.1 Time Analysis

FDA array pattern is inherently time-dependant: in spite of some alleged solutions for time invariant FDA that have been proposed in some previous studies, the analysis carried out in [116] has definitively stated that a range-dependent pattern eventually always leads to a time-dependent pattern. Thus, it is impossible to generate a time-invariant range-dependent beam pattern.

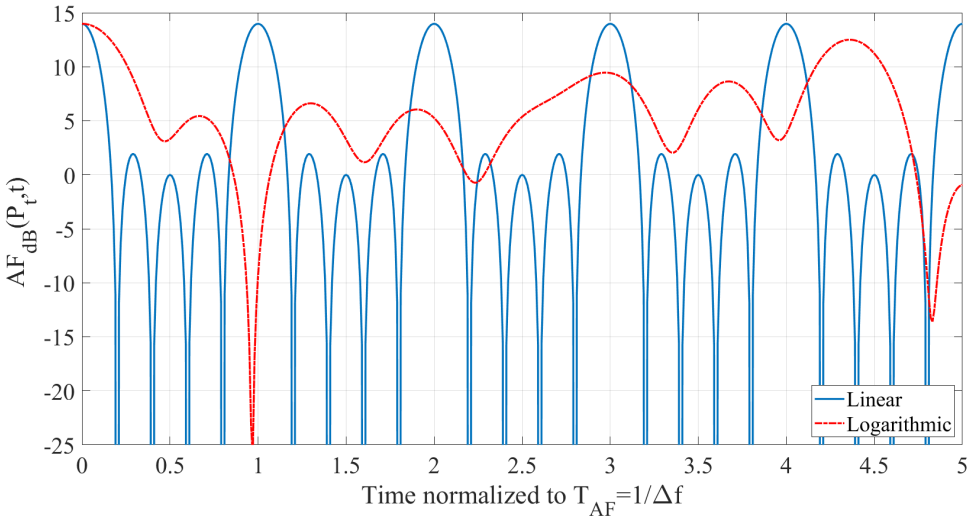


Figure 3.14: Time evolution of the AF from a circular FDA, for different frequency shift policies. Picture from ©2024 IEEE [101].

As shown in Figure 3.14, in case a linear frequency shift policy is employed, the AF is periodic with a period $T_{AF} = 1/\Delta f$. Hence, the beam moves in space with a fixed pattern, periodically peaking in the desired focus point. Conversely, with a logarithmic policy, the periodicity is lost, and the AF hardly rises up again to its maximum. Eventually, a linear policy seems a better solution for communications, since the time evolution of the AF is predictable and the communication can be adapted easily.

A greater number of elements over the ring of course increases the value of the AF at t_0, but also unexpectedly reduces the time AF keeps closer to the maximum (Figure 3.15). For instance, the half-factor time-width, i.e. the time interval where the AF is kept greater than the half of the maximum, drops from about 18% to 3.6% when M is increased from 5 to 25. Interestingly, if the 25 elements are instead spread over 5 rings, corresponding to 5 different feeding frequencies instead of 25, the same increase in peak is achieved, while preserving the half-factor time-width at the same time. This actually represents the main reason why the 2D layout (i.e. the circular and the planar ones) should be conveniently conceived with a number of different frequencies lower than the total number of array elements. Limiting the number of radiated frequencies can also contribute to reducing the overall FDA power consumption, as the generation and the management of the different frequencies might represent an energy demanding process inside the array front-end.

3.3.2 Geofencing sensitivity to Array Parameters

The sensitivity of the Geofencing effect to the FDA parameters is here investigated by means of two specific parameters, namely the *focus area* (A_f) and the *focus efficiency* (ε_f). The focus area is defined as the area around the target point P_t where the

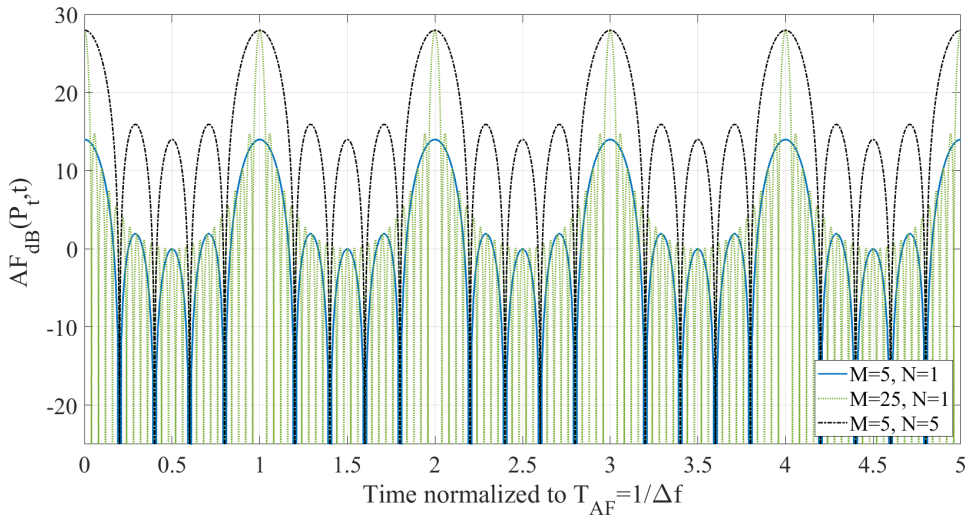


Figure 3.15: Time evolution of the AF from a circular FDA, for different number of elements. Picture from ©2024 IEEE [101].

normalized $|AF|^2_{dB}$ is greater than $-3\,\text{dB}$, whereas the focus efficiency is computed as:

$$\varepsilon_f = \frac{A_f}{\sum_{s=1}^{N_s} A_s \cdot \left(\frac{R_t}{R_s}\right)^2}, \tag{3.28}$$

being R_t the distance of the target point from the transmitting FDA, N_s the number of spots over the service area where $|AF|^2_{dB}$ is greater than $-3\,\text{dB}$, A_s the area of the s-th spot and R_s its distance from the FDA. The focus area accounts for the Geofencing effectiveness on the target point, whereas the focus efficiency accounts for the presence of multiple spots over the service area. Although ideal Geofencing of course corresponds to ε_f equal to 1, an efficiency greater than 0.5 may represent an acceptable target, meaning that the spurious spots are overall smaller than the target spot or, otherwise, that they are further from the transmitting FDA than the target point, and therefore exposed to heavier attenuation. With reference to A_f, it should not exceed some tens of square meters as a fair rule of thumb.

In particular, the spatial average of the focus area and efficiency ($\langle A_f \rangle$ and $\langle \varepsilon_f \rangle$, respectively) is computed herein for different characteristics of the FDA. The statistical assessment is carried out through a Monte Carlo approach. For each considered setting of the FDA (geometrical layout, number of elements and spacing, frequency offset), A_f and ε_f have been computed for $N_t = 1000$ target points uniformly spread over the service area, and the N_t corresponding values have been finally averaged to get the spatial means. The investigation is limited to the linear frequency increase across the elements, which is expected to be more critical in terms of focus efficiency because of the peak spatial repetition. The circular layout is first addressed as a reference deployment, and it is then compared to the planar and the linear solutions.

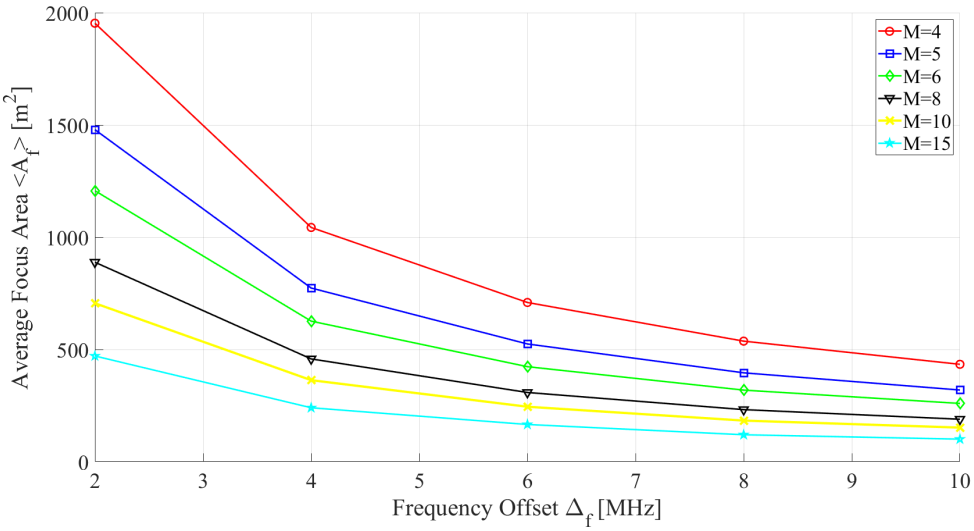


Figure 3.16: Average focus area, single ring circular FDA, R $\leq$ 100 m, f_0=3.5 GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

Circular Layout

The average focus area and efficiency for a single ring circular array are plotted in Figure 3.16 and 3.17 against Δf and for different M values. Increasing the frequency offset leads to smaller focus area, but unfortunately to lower efficiency, as the spots' radial period gets shorter, and therefore (3.21) results unsatisfied over an increasingly larger part of the service area. This increases the occurrence of cases where additional spots closer to the transmitting FDA turn up, to the detriment of the mean focus efficiency. A greater number of radiating elements over the ring turns out beneficial on both $\langle A_f \rangle$ and $\langle \varepsilon_f \rangle$, although it makes harder to meet the condition stated in (3.13). Moreover, the benefit reduces as M increases, especially for the focus efficiency. Numerous elements is also an impairment on the sensitivity of the focus area to the frequency offset (Figure 3.16).

The introduction of multiple rings can further improve both the focus area and efficiency (Figure 3.18), although $\langle \varepsilon_f \rangle$ turns out to be insensitive t the number of rings (Figure 3.19).

These results clearly show that Δf should be limited to few MHz to get a satisfactory efficiency, but this contrasts with the requirement empirically set on the focus area. In fact, according to Figure 3.16 and 3.18, even numerous rings and/or elements over each ring can hardly provide $\langle A_f \rangle$ smaller than some hundreds of square meters for Δf up to few MHz.

Performance can be improved by limiting the extension of the service area, i.e. the maximum distance where the Geofencing effect is enforced. Figure 3.20 and 3.21 compare the average focus area and efficiency in case the maximum range is set to 100 m and 50 m. Of course, the range reduction automatically makes (3.21) more easily satisfied, thus corresponding to higher efficiency (Figure 3.21). Moreover, figures like Figure

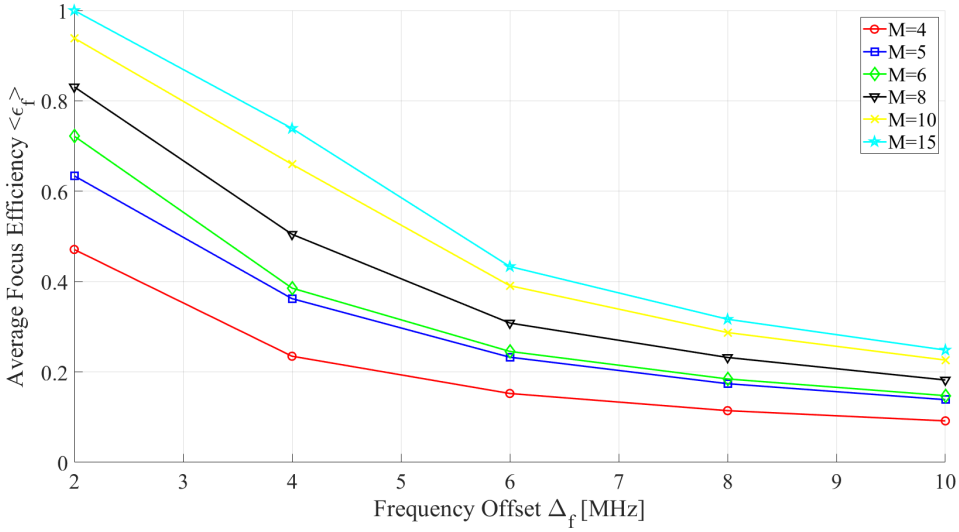


Figure 3.17: Average focus efficiency, single ring circular FDA, R $\leq$ 100 m, f_0=3.5 GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

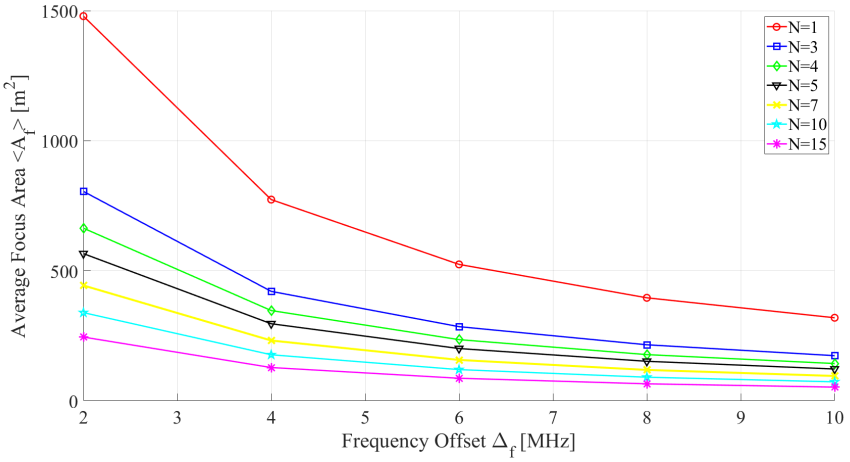


Figure 3.18: Average focus area, multiple rings circular FDA, M=5, $R \leq 100$ m, $f_0 = 3.5$ GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

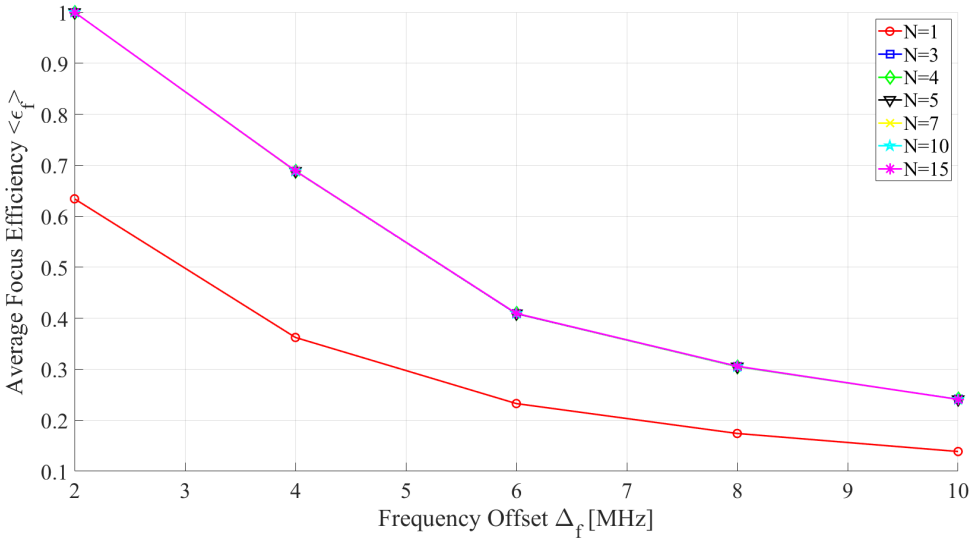


Figure 3.19: Average focus efficiency, multiple rings circular FDA, M=5, R $\leq$ 100 m, $f_0 = 3.5$ GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

3.6b and 3.4 show that radial spots keep their shape in the *polar* plane, i.e. their area grows up with distance. Therefore, limiting the range is also beneficial to $\langle A_f \rangle$ (Figure 3.20).

The impact of the communication frequency and of the spacing between the array elements on the Geofencing effectiveness is finally reported in Figure 3.22 and 3.23. Both $\langle A_f \rangle$ and $\langle \varepsilon_f \rangle$ seem independent of the frequency, whereas increasing the spacing reduces the focus area while keeping the efficiency basically unchanged, unless it is excessively stretched (Figure 3.23). In fact, as a large spacing can boost the side lobes level in standard arrays, it can similarly trigger the appearance of "side spots" in the angular direction, to the disadvantage of the focus efficiency.

In conclusion, many parameters seem to affect the focus area, like the frequency offset, the number of elements and their spacing, whereas the focus efficiency is mainly driven by the frequency offset. Therefore, it can be convenient to choose M, N and the spacing to get a satisfactory (average) focus area, and select Δf in order to meet also the requirement on the (average) focus efficiency. In this general framework, it is worth reminding that limiting the range also turns out to be beneficial, i.e. signal Geofencing through FDA seems a viable solution only for short/mid-range wireless communications, as also previously suggested by (3.21). For instance, setting the maximum range at 50 m, M=N=5, $\Delta f = 4$ MHz and with spacing equal to $3\lambda_0$, then $\langle A_f \rangle \approx 32m^2$ and $\langle \varepsilon_f \rangle = 1$.

3.3.3 Comparison with Planar and Linear Deployment

As shown in Figure 3.24 and 3.25, the performance achieved for the linear and planar layouts follows the same trends already highlighted for the circular case.

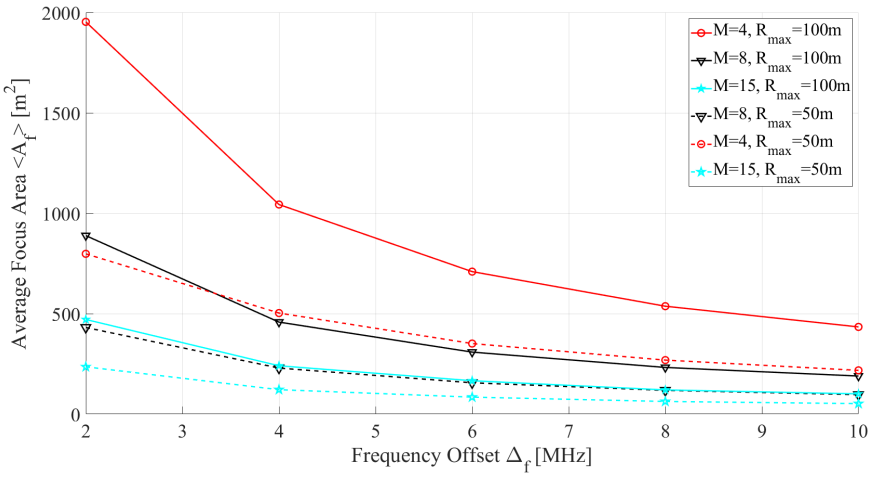


Figure 3.20: Impact of range restriction on the focus area for a single ring circular FDA, f_0=3.5 GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

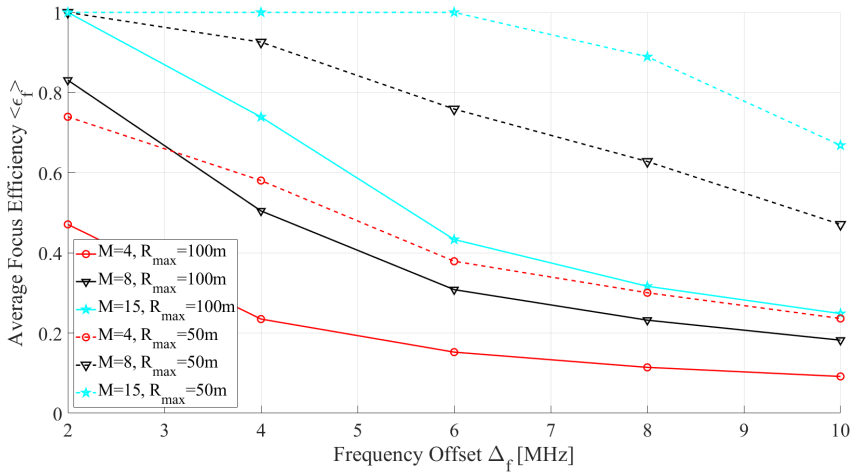


Figure 3.21: Impact of range restriction on the focus efficiency for a single ring circular FDA, f_0=3.5 GHz, spacing=$\lambda_0/2$. Picture from ©2024 IEEE [101].

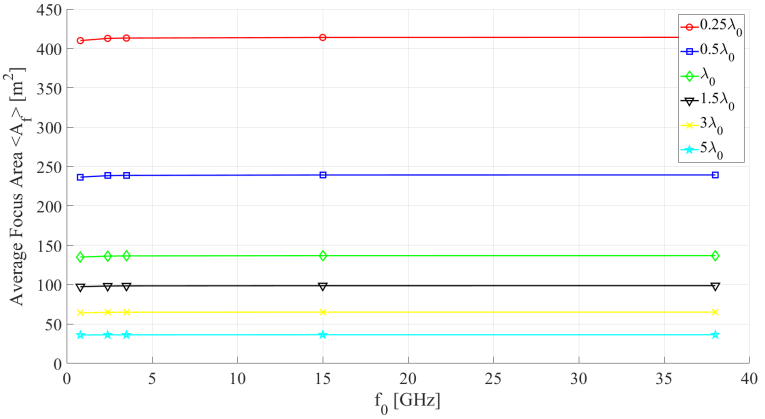


Figure 3.22: Focus area sensitivity to communication frequency and elements spacing for a circular FDA with M=5, N=5, $\Delta_f = 5$ MHz. Picture from ©2024 IEEE [101].

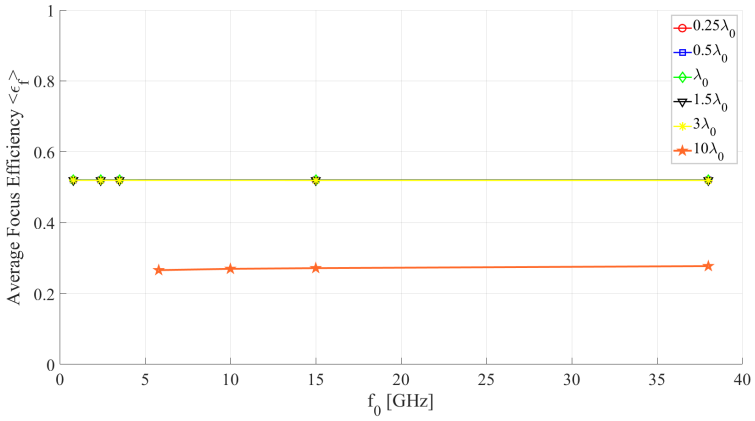


Figure 3.23: Focus efficiency sensitivity to communication frequency and elements spacing for a circular FDA with M=5, N=5, $\Delta_f = 5\,\text{MHz}$. Picture from ©2024 IEEE [101].

For the same array parameters, a planar FDA in general exhibits worse performance than the corresponding circular FDA in terms of both focus area and efficiency. Conversely, a linear FDA (with random-like frequency spreading) can yield a quite limited focus area, in general well smaller compared to a circular or planar array with the same number of elements (Figure 3.24). Unfortunately, the linear deployment turns out to be less efficient than the circular layout with the same number of transmitting antennas (Figure 3.25). It is worth pointing out that the random-like distribution of frequencies aver the array can be done in different ways, corresponding to different realizations of $|AF|$ in the (R, θ) plane. This property can be exploited to make Geofencing more effective. In fact, enforcing a random-like time swap of the frequencies across the array elements may result in a correspondingly frantic change of the spurious spots position around the target spot. This effect can further hamper any possible eavesdropping attack, as well as fairly share interference all over the space rather than keep it affecting few specific locations (in a sort of *interference hopping* effect).

In comparison with the circular deployment, a larger spacing between the elements is less effective in both the linear and the planar case, as it still reduces the size of the focus area (Figure 3.26) but it also affects the focus efficiency to a heavier extent (Figure 3.27).

The major trends and results, are summed up in Table 3.2, which reports the sensitivity of the focus area and efficiency to the main parameters of the FDA.

3.4 Final Remarks

In this chapter, the potential of FDA for enhancing physical layer security, particularly through Geofencing applications, was thoroughly examined. The analysis highlighted the unique capabilities of FDA systems to spatially and temporally focus energy, thereby restricting the communication zone to a specific area. This characteristic makes

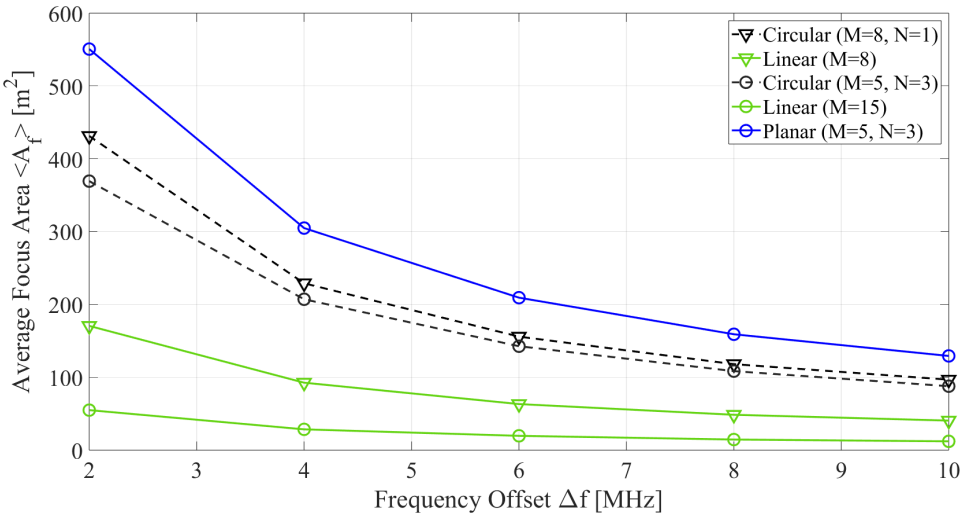


Figure 3.24: Average focus area in the linear and in the planar case, comparison with the circular layout. $f_0 = 3.5\,\text{GHz}$, spacing=$\lambda_0/2$, $R_{max} = 50\,\text{m}$. Picture from ©2024 IEEE [101].

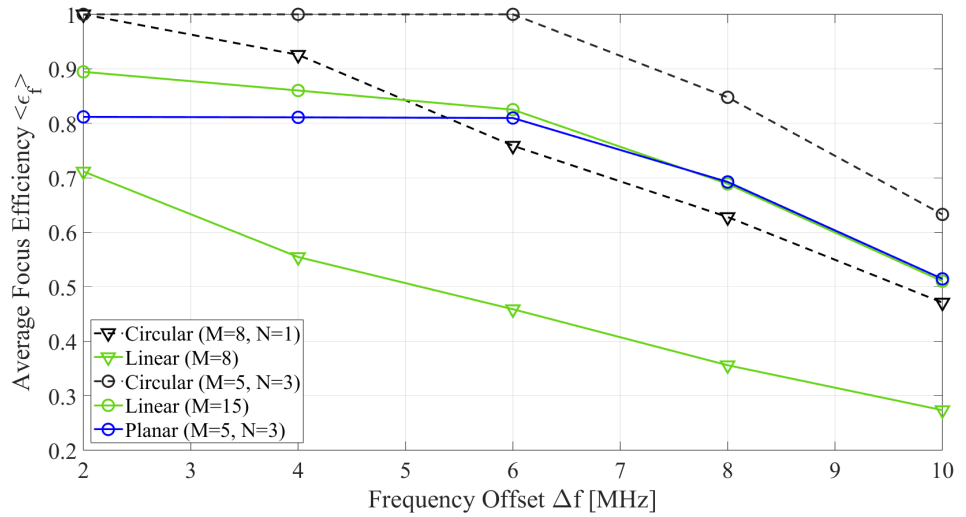


Figure 3.25: Average focus efficiency in the linear and in the planar case, in comparison with the circular layout. $f_0 = 3.5\,\text{GHz}$, spacing=$\lambda_0/2$, $R_{max} = 50\,\text{m}$. Picture from ©2024 IEEE [101].

Table 3.2: Sensitivity of focus area and efficiency to the major array parameters. Picture from ©2024 IEEE [101].

	$\uparrow \Delta f$	↑M	↑N	$\uparrow f_0$	↑Spacing	↑Range
Focus Area	↓	↓	↓	–	↓	↑
Focus Efficiency	↓	↑	– (approx.)	–	– (circular) ↓ (planar/linear)	↓

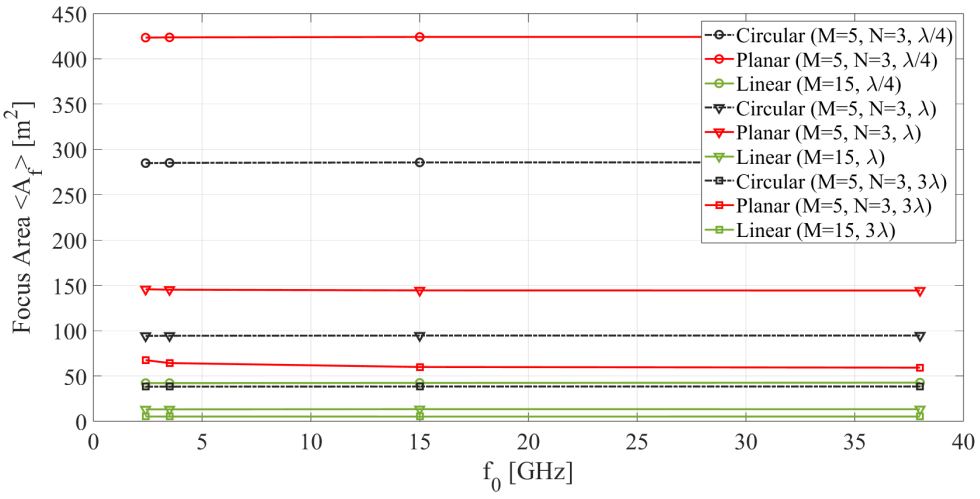


Figure 3.26: Average focus area in the linear and in the planar case, comparison with the circular layout. $\Delta f = 5\,\text{MHz}$, $R_{max} = 50\,\text{m}$. Picture from ©2023 IEEE [106].

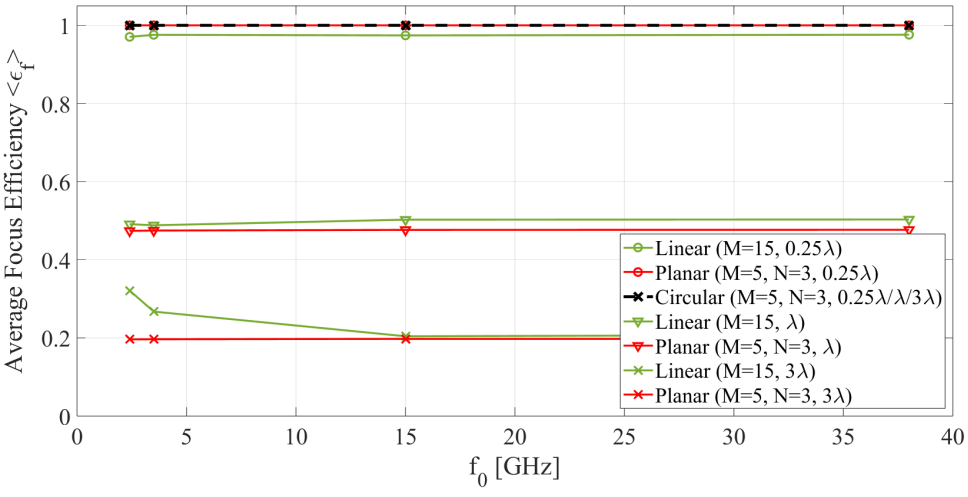


Figure 3.27: Average focus efficiency in the linear and in the planar case, in comparison with the circular layout. $\Delta f = 5\,\text{MHz}$, $R_{max} = 50\,\text{m}$. Picture from ©2023 IEEE [106].

FDA a valuable tool for securing wireless communications against eavesdropping and other security threats.

Through RT simulations, FDA characteristics are explored in multipath environment, aiming at analysing the impact of real environment on FDA beam pattern, which is usually studied only in free space like propagation. Then, the impact of the different design parameters of the array on the beam pattern is highlighted, providing some design rules for using FDA for secure communications. Although being interesting, FDA might be impractical: the feeding mechanism is more complex with respect of classical phased arrays, and the benefits of range dependant beam pattern are somehow limited by the inner time variability of the AF. Nevertheless, FDA could represent an additional layer of security along with all the classical techniques employed, or could work to facilitate and protect vulnerable phases of cryptography. For example, FDA can be employed during the key agreement phase, reinforcing this vulnerable phase, and then switched off since a higher layer security mechanism is employed.

Overall, this work demonstrates the potential of physical layer techniques to enhance the security of wireless communications in a way that is both efficient and scalable. Future research could further refine these models, particularly by exploring the impact of more complex propagation environments and extending the applicability of FDA systems to secure communication.

Conclusions

In this thesis, several critical aspects of physical layer security were explored, focusing on both key generation methods and advanced antenna technologies.

Traditional models based on the Jakes's uniform scattering assumption are not always reliable to model the spatial correlation properties of wireless channels, which have crucial importance for the effectiveness of many PLS solutions. In particular, the importance of spatial correlation in determining the reliability of key generation protocols is emphasized. In order to stress the limit of the Jake's assumption, spatial correlation measurements have been carried out in different real scenarios with different antennas and in different conditions of propagation. Moreover, a correlation model tailored to Rice channels has been developed and discussed, and proved that the presence of a dominant signal can significantly affect the correlation distance.

With reference to antenna solutions aimed at safer, private communications, the use of Frequency Diverse Array (FDA) for geofencing was examined as a viable solution for securing wireless systems. By concentrating the transmitted power within a specific spatial region, FDA technology offers a way to limit the potential for eavesdropping threat. Results indicate that by carefully selecting the frequency offsets and array configuration, it is possible to achieve a good level of security, which might serve as a basis level of security along with other security mechanisms (e.g. encryption).

Overall, this work demonstrates the potential of physical layer techniques to enhance the security of wireless communications in a way that is both efficient and scalable. However, in the future, PLS might not become an alternative to classical cryptography, but rather a complementary solution. Low-end, low-energy, lightweight devices, such as IOT, might benefit from PLS solutions. Other more complex systems, might employ PLS as another security layer to further enhance wireless communications security, along with classical cryptographical approach.

List Of Acronyms

ACF Autocorrelation Function.

AES Advanced Encryption Standard.

AF Array Factor.

AWGN Additive White Gaussian Noise.

BCH Bose-Chaudhuri-Hocquenghem.

CIR Channel Impulse Response.

CSI Channel State Information.

CTF Channel Transfer Function.

DH Diffie-Hellman.

DOA Direction of Arrival.

DS Delay Spread.

FDA Frequency Diverse Array.

FDD Frequency Division Duplexing.

FEC Forward Error Correction.

FFT Fast Fourier Transform.

IOT Internet Of Things.

KDR Key Disagreement Rate.

KGR Key Generation Rate.

LOS Line Of Sight.

MIMO Multiple Input-Multiple Output.

MIMO Single Input-Multiple Output.

NIST National Institute of Standards and Technologies.

NLOS Non-Line Of Sight.

OFDM Orthogonal Frequency Division Modulation.

OTP One Time Pad.

PAP Power Angle Profile.

PEC Perfect Electrical Conductor.

PLKG Physical Layer based-Key generation.

PLS Physical Layer Security.

PSD Power Spectral Density.

RF Radio Frequency.

RSA Rivest-Shamir-Adleman.

RSS Received Signal Strength.

RSSI Radio Signal Strength Indicator.

RT Ray Tracing.

RX Receiver.

SKR Secrecy Key Rate.

SNR Signal to Noise Ratio.

TDD Time Division Duplexing.

TDL Tapped Delay Line.

TX Transmitter.

VNA Vector Network Analyser.

WPT Wireless Power Transfer.

WSSUS Wide Sense Stationary Uniform Scattering.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash. 'Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications'. In: *IEEE Communications Surveys Tutorials* 17.4 (2015), pp. 2347–2376. DOI: 10.1109/COMST.2015.2444095.

[2] *2019 CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS*. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf. Mar. 2020.

[3] J. Zhang, G. Li, A. Marshall, A. Hu and L. Hanzo. 'A New Frontier for IoT Security Emerging From Three Decades of Key Generation Relying on Wireless Channels'. In: *IEEE Access* 8 (2020), pp. 138406–138446. DOI: 10.1109/ACCESS.2020.3012006.

[4] Henk C. a. van Tilborg. *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*. Spinger Nature.

[5] B.Schneier N.Ferguson. *Practical Cryptography*. Wiley Publishing.

[6] Alfred Menezes. 'The Discrete Logarithm Problem'. In: *Elliptic Curve Public Key Cryptosystems*. Boston, MA: Springer US, 1993, pp. 49–59. ISBN: 978-1-4615-3198-2. DOI: 10.1007/978-1-4615-3198-2_4. URL: https://doi.org/10.1007/978-1-4615-3198-2_4.

[7] W. Diffie and M. Hellman. 'New directions in cryptography'. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[8] R. L. Rivest, A. Shamir and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342.

[9] H. Riesel. *Prime Numbers and Computer Methods for Factorization*. Progress in Mathematics. Birkhäuser Boston, 2013. ISBN: 9781475710892. URL: https://books.google.it/books?id=4-TgBwAAQBAJ.

[10] Chi Cheng, Rongxing Lu, Albrecht Petzoldt and Tsuyoshi Takagi. 'Securing the Internet of Things in a Quantum World'. In: *IEEE Communications Magazine* 55.2 (2017), pp. 116–120. DOI: 10.1109/MCOM.2017.1600522CM.

[11] Huanguo Zhang, Zhaoxu Ji, Houzhen Wang and Wanqing Wu. 'Survey on quantum information security'. In: *China Communications* 16.10 (2019), pp. 1–36. DOI: 10.23919/JCC.2019.10.001.

[12] Jialiang Li, Junli Wan, Wei Wang and Shuifa Sun. 'Survey on Quantum Secret Communication'. In: *2011 Symposium on Photonics and Optoelectronics (SOPO)*. 2011, pp. 1–5. DOI: 10.1109/SOPO.2011.5780565.

[13] G. S. Vernam. 'Secret signaling system'. In: *U.S. Patent 1 310 719* (1919).

[14] *Specification for the Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197. Accessed on September the 10th, 2024. 2001. URL: https://web.archive.org/web/20130305143117/http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

[15] *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. Federal Information Processing Standards Publication 197. Accessed on September the 10th, 2024. Nov. 2001. URL: https://web.archive.org/web/20170312045558/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[16] Vaishali Bhatia and K.R. Ramkumar. 'An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm'. In: (2020), pp. 89–94. DOI: 10.1109/ICCCA49541.2020.9250806.

[17] Sandeep Rao, Dindayal Mahto, DILIP YADAV and Danish Khan. 'The AES-256 Cryptosystem Resists Quantum Attacks'. In: *International Journal of Advanced Research in Computer Science* 8 (Apr. 2017), pp. 404–408.

[18] Sourav Purification, Simeon Wuthier, Jinoh Kim, Jonghyun Kim and Sang-Yoon Chang. 'Fake Base Station Detection and Blacklisting'. In: *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*. 2024, pp. 1–9. DOI: 10.1109/ICCCN61486.2024.10637542.

[19] Zixin Wang, Bin Cao, Yao Sun, Chenxi Liu, Zhiguo Wan and Mugen Peng. 'Protecting System Information from False Base Station Attacks: A Blockchain-based Approach'. In: *IEEE Transactions on Wireless Communications* (2024), pp. 1–1. DOI: 10.1109/TWC.2024.3406729.

[20] Halima Sadia, Saima Farhan, Yasin Ul Haq, Rabia Sana, Tariq Mahmood, Saeed Ali Omer Bahaj and Amjad Rehman Khan. 'Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach'. In: *IEEE Access* 12 (2024), pp. 52565–52582. DOI: 10.1109/ACCESS.2024.3380014.

[21] Michele Polese, Leonardo Bonati, Salvatore D'Oro, Stefano Basagni and Tommaso Melodia. 'Understanding O-RAN: Architecture, Interfaces, Algorithms,

Security, and Research Challenges'. In: *IEEE Communications Surveys & Tutorials* 25.2 (2023), pp. 1376–1411. DOI: 10.1109/COMST.2023.3239220.

[22] Aly Sabri Abdalla and Vuk Marojevic. 'End-to-End O-RAN Security Architecture, Threat Surface, Coverage, and the Case of the Open Fronthaul'. In: *IEEE Communications Standards Magazine* 8.1 (2024), pp. 36–43. DOI: 10.1109/MCOMSTD.0001.2200047.

[23] P. Suresh, J. Vijay Daniel, V. Parthasarathy and R. H. Aswathy. 'A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment'. In: *2014 International Conference on Science Engineering and Management Research (ICSEMR)*. 2014, pp. 1–8. DOI: 10.1109/ICSEMR.2014.7043637.

[24] Shams Forruque Ahmed, Md. Sakib Bin Alam, Shaila Afrin, Sabiha Jannat Rafa, Samanta Binte Taher, Maliha Kabir, S. M. Muyeen and Amir H. Gandomi. 'Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities'. In: *IEEE Access* 12 (2024), pp. 13125–13145. DOI: 10.1109/ACCESS.2024.3352508.

[25] Muhammad Adil, Muhammad Khurram Khan, Neeraj Kumar, Muhammad Attique, Ahmed Farouk, Mohsen Guizani and Zhanpeng Jin. 'Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions'. In: *IEEE Internet of Things Journal* 11.11 (2024), pp. 19046–19069. DOI: 10.1109/JIOT.2024.3360289.

[26] C. E. Shannon. 'Communication theory of secrecy systems'. In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[27] Matthieu Bloch and João Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[28] A. D. Wyner. 'The wire-tap channel'. In: *The Bell System Technical Journal* 54.8 (1975), pp. 1355–1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x.

[29] S. Leung-Yan-Cheong and M. Hellman. 'The Gaussian wire-tap channel'. In: *IEEE Transactions on Information Theory* 24.4 (1978), pp. 451–456. DOI: 10.1109/TIT.1978.1055917.

[30] Haohao Qin, Xiang Chen, Yin Sun, Ming Zhao and Jing Wang. 'Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications'. In: (July 2011), pp. 1–5. DOI: 10.1109/iccw.2011.5963524.

[31] Rudolph Ahlswede and Imre Csiszar. 'Common randomness in information theory and cryptography. I. Secret sharing'. In: *Information Theory, IEEE Transactions on* 39 (Aug. 1993), pp. 1121–1132. DOI: 10.1109/18.243431.

[32] U.M. Maurer. 'Secret key agreement by public discussion from common information'. In: *IEEE Transactions on Information Theory* 39.3 (1993), pp. 733–742. DOI: 10.1109/18.256484.

[33] J. Zhang, S. Rajendran, Z. Sun, R. Woods and L. Hanzo. 'Physical Layer Security for the Internet of Things: Authentication and Key Generation'. In: *IEEE Wireless Communications* 26.5 (2019), pp. 92–98. DOI: 10.1109/MWC.2019.1800455.

[34] Junqing Zhang, Trung Q. Duong, Alan Marshall and Roger Woods. 'Key Generation From Wireless Channels: A Review'. In: *IEEE Access* 4 (2016), pp. 614–626. DOI: 10.1109/ACCESS.2016.2521718.

[35] Sana Ben Hamida, Jean-Benoit Pierrot, Benoit Denis, Claude Castelluccia and Bernard Uguen. 'On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks'. In: (Sept. 2012). DOI: 10.1109/VTCFall.2012.6399358.

[36] Ozan Alp Topal, Gunes Karabulut Kurt and Halim Yanikomeroglu. 'Securing the Inter-Spacecraft Links: Physical Layer Key Generation from Doppler Frequency Shift'. In: *IEEE Journal of Radio Frequency Identification* (2021), pp. 1–1. DOI: 10.1109/JRFID.2021.3077756.

[37] Rene Guillaume, Andreas Mueller, Christian T. Zenger, Christof Paar and Andreas Czylwik. 'Fair Comparison and Evaluation of Quantization Schemes for PHY-based Key Generation'. In: *OFDM 2014; 18th International OFDM Workshop 2014 (InOWo'14)*. 2014, pp. 1–5.

[38] Christian Zenger, Jan Zimmer and Christof Paar. 'Security Analysis of Quantization Schemes for Channel-based Key Extraction'. In: *EAI Endorsed Transactions on Security and Safety* 2.6 (Aug. 2015). DOI: 10.4108/eai.22-7-2015.2260194.

[39] Neal Patwari, Jessica Croft, Suman Jana and Sneha K. Kasera. 'High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements'. In: *IEEE Transactions on Mobile Computing* 9.1 (2010), pp. 17–30. DOI: 10.1109/TMC.2009.88.

[40] Hongbo Liu, Yang Wang, Jie Yang and Yingying Chen. 'Fast and practical secret key extraction by exploiting channel response'. In: *2013 Proceedings IEEE INFOCOM*. 2013, pp. 3048–3056. DOI: 10.1109/INFCOM.2013.6567117.

[41] Christopher Huth, René Guillaume, Thomas Strohm, Paul Duplys, Irin Ann Samuel and Tim Güneysu. 'Information reconciliation schemes in physical-layer security: A survey'. In: *Computer Networks* 109 (2016). Special issue on Recent Advances in Physical-Layer Security, pp. 84–104. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2016.06.014. URL: https://www.sciencedirect.com/science/article/pii/S1389128616301864.

[42] Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng and Lajos Hanzo. 'Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook'. In: *IEEE Communications Surveys Tutorials* 21.1 (2019), pp. 881–919. DOI: 10.1109/COMST.2018.2864557.

[43] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari and Srikanth V. Krishnamurthy. 'On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments'. In: *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*. MobiCom '09. Beijing, China: Association for Computing Machinery, 2009, pp. 321–332. ISBN: 9781605587028. DOI: 10.1145/1614320.1614356. URL: https://doi.org/10.1145/1614320.1614356.

[44] Junxing Zhang, Sneha K. Kasera and Neal Patwari. 'Mobility assisted secret key generation using wireless link signatures'. In: *in INFOCOM miniconference*. 2009.

[45] Yunchuan Wei, Kai Zeng and Prasant Mohapatra. 'Adaptive Wireless Channel Probing for Shared Key Generation Based on PID Controller'. In: *IEEE Transactions on Mobile Computing* 12.9 (2013), pp. 1842–1852. DOI: 10.1109/TMC.2012.144.

[46] Ozan Alp Topal, Gunes Karabulut Kurt and Berna Özbek. 'Key Error Rates in Physical Layer Key Generation: Theoretical Analysis and Measurement-Based Verification'. In: *IEEE Wireless Communications Letters* 6.6 (2017), pp. 766–769. DOI: 10.1109/LWC.2017.2740290.

[47] NIST website. Accessed on September the 10$^{\text{th}}$, 2024. URL: www.nist.gov.

[48] Wade Trappe. 'The challenges facing physical layer security'. In: *IEEE Communications Magazine* 53.6 (2015), pp. 16–20. DOI: 10.1109/MCOM.2015.7120011.

[49] Simone Del Prete. *Ray-tracing assessment of the robustness of Physical Layer Security key generation protocol*. Master's Thesis, https://amslaurea.unibo.it/24081/. 2021.

[50] Sohail Payami and Fredrik Tufvesson. 'Channel measurements and analysis for very large array systems at 2.6 GHz'. In: *2012 6th European Conference on Antennas and Propagation (EUCAP)*. 2012, pp. 433–437. DOI: 10.1109/EuCAP.2012.6206345.

[51] Wasim Q. Malik. 'Spatial correlation in ultrawideband channels'. In: *IEEE Transactions on Wireless Communications* 7.2 (2008), pp. 604–610. DOI: 10.1109/TWC.2008.060547.

[52] Padam L. Kafle, Apichart Intarapanich, Abu B. Sesay, John Mcrory and Robert J. Davies. 'Spatial correlation and capacity measurements for wideband MIMO channels in indoor office environment'. In: *IEEE Transactions on Wireless Communications* 7.5 (2008), pp. 1560–1571. DOI: 10.1109/TWC.2008.060170.

[53] Zhenghui Li, Fengyu Luan, Yan Zhang, Limin Xiao, Lianfen Huang, Shidong Zhou, Xibin Xu and Jing Wang. 'Capacity and spatial correlation measurements for wideband distributed MIMO channel in aircraft cabin environment'. In: *2012 IEEE Wireless Communications and Networking Conference (WCNC)*. 2012, pp. 1175–1179. DOI: 10.1109/WCNC.2012.6213954.

[54] D.P. McNamara, M.A. Beach and P.N. Fletcher. 'Spatial correlation in indoor MIMO channels'. In: *The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*. Vol. 1. 2002, 290–294 vol.1. DOI: 10.1109/PIMRC.2002.1046707.

[55] Tao Zhou, Cheng Tao, Sana Salous and Liu Liu. 'Measurements and Analysis of Angular Characteristics and Spatial Correlation for High-Speed Railway Channels'. In: *IEEE Transactions on Intelligent Transportation Systems* 19.2 (2018), pp. 357–367. DOI: 10.1109/TITS.2017.2681112.

[56] Limei Lin, Yang Wang, Jiliang Zhang and Dayong Yan. 'Wideband MIMO channel spatial correlation measurement under different polarization patterns'. In: *2010 IEEE International Conference on Information Theory and Information Security*. 2010, pp. 751–754. DOI: 10.1109/ICITIS.2010.5689680.

[57] *Aronia OmniLOG website*. https://aaronia.com/en/shop/antennas-sensors/biconical-antenna/omnilog-pro. Accessed: 2024-08-08.

[58] *Aronia HyperLOG website*. https://aaronia.com/en/shop/antennas-sensors/logper-antennas/breitband-antenne-hyperlog7060. Accessed: 2024-08-08.

[59] P.D. Teal, T.D. Abhayapala and R.A. Kennedy. 'Spatial correlation for general distributions of scatterers'. In: *IEEE Signal Processing Letters* 9.10 (2002), pp. 305–308. DOI: 10.1109/LSP.2002.804138.

[60] J. Fuhl, A.F. Molisch and Ernst Bonek. 'Unified channel model for mobile radio systems with smart antennas'. In: *Radar, Sonar and Navigation, IEE Proceedings* - 145 (Mar. 1998), pp. 32–41. DOI: 10.1049/ip-rsn:19981750.

[61] G.D. Durgin and T.S. Rappaport. 'Effects of multipath angular spread on the spatial cross-correlation of received voltage envelopes'. In: *1999 IEEE 49th Vehicular Technology Conference (Cat. No.99CH36363)*. Vol. 2. 1999, 996–1000 vol.2. DOI: 10.1109/VETEC.1999.780498.

[62] Davide Dardari and Nicolò Decarli. 'Holographic Communication Using Intelligent Surfaces'. In: *IEEE Communications Magazine* 59.6 (2021), pp. 35–41. DOI: 10.1109/MCOM.001.2001156.

[63] Haiyang Zhang, Nir Shlezinger, Francesco Guidi, Davide Dardari and Yonina C. Eldar. '6G Wireless Communications: From Far-Field Beam Steering to Near-Field Beam Focusing'. In: *IEEE Communications Magazine* 61.4 (2023), pp. 72–77. DOI: 10.1109/MCOM.001.2200259.

[64] Davide Dardari. 'Communicating With Large Intelligent Surfaces: Fundamental Limits and Models'. In: *IEEE Journal on Selected Areas in Communications* 38.11 (2020), pp. 2526–2537. DOI: 10.1109/JSAC.2020.3007036.

[65] Younsun Kim, Youngbum Kim, Jinyoung Oh, Hyoungju Ji, Jeongho Yeo, Seunghoon Choi, Hyunseok Ryu, Hoondong Noh, Taehyoung Kim, Feifei Sun, Yi Wang, Yinan Qi and Juho Lee. 'New Radio (NR) and its Evolution toward 5G-Advanced'. In: *IEEE Wireless Communications* 26.3 (2019), pp. 2–7. DOI: 10.1109/MWC.2019.8752473.

[66] J.D. Parsons. 'Fundamentals of VHF and UHF Propagation'. In: *The Mobile Radio Propagation Channel*. John Wiley & Sons, Ltd. Chap. 2, pp. 15–31. ISBN: 9780470841525. DOI: https://doi.org/10.1002/0470841524.ch2. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/0470841524.ch2. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/0470841524.ch2.

[67] J. Zhou, K. Ishizawa, S Sasaki, S. Muramatsu, H. Kikuchi and Y. Onozato. 'Generalized Spatial Correlation Equations for Antenn Arrays in Wireless Diversity Reception: Exact and Approximate Analyses'. In: *IEICE Trans. Comm.* E87-B (1 Jan. 2004), pp. 204–208.

[68] P-C. Hsieh and F-C. Chen. 'A New Spatial Correlation Formulation of Arbitrary AoA Scenarios'. In: *IEEE Ant. and Wireless Propagat. Letters* 8 (Mar. 2009), pp. 398–401. DOI: 10.1109/LAWP.2009.2019311.

[69] Bruno Clerckx and Claude Oestges. *MIMO Wireless Networks: Channels, Techniques and Standards for Multi-Antenna, Multi-User and Multi-Cell Systems*. 2nd. USA: Academic Press, Inc., 2013. ISBN: 012385055X.

[70] Marco Zoli, Miroslav Mitev, André N. Barreto and Gerhard Fettweis. 'Estimation of the Secret Key Rate in Wideband Wireless Physical-Layer-Security'. In: *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*. 2021, pp. 1–6. DOI: 10.1109/ISWCS49558.2021.9562135.

[71] Kai Zeng. 'Physical layer key generation in wireless networks: challenges and opportunities'. In: *IEEE Communications Magazine* 53.6 (2015), pp. 33–39. DOI: 10.1109/MCOM.2015.7120014.

[72] Haji M. Furqan, Jehad M. Hamamreh and Huseyin Arslan. 'New Physical Layer Key Generation Dimensions: Subcarrier Indices/Positions-Based Key Generation'. In: *IEEE Communications Letters* 25.1 (2021), pp. 59–63. DOI: 10.1109/LCOMM.2020.3025262.

[73] Michal Pilc and Piotr Remlein. 'The impact of LOS component on information disclosed to eavesdroppers in wireless channels with PHY-based secret key generation'. In: *2018 Baltic URSI Symposium (URSI)*. 2018, pp. 65–68. DOI: 10.23919/URSI.2018.8406707.

[74] Simone Del Prete, Franco Fuschini and Marina Barbiroli. 'A Study on Secret Key Rate in Wideband Rice Channel'. In: *MDPI Electronics* 11.17 (2022), p. 2772.

[75] Marco Zoli, Andre Noll Barreto, Stefan Köpsell, Padmanava Sen and Gerhard Fettweis. 'Physical-Layer-Security Box: a concept for time-frequency channel-reciprocity key generation'. In: *EURASIP Journal on Wireless Communications and Networking* 2020 (June 2020). DOI: 10.1186/s13638-020-01712-6.

[76] *3GPP TR 38.901 Version 16.1.0 Release 16: Study on channel model for frequencies from 0.5 to 100 GHz.*

[77] Keli Zhang, Zhefeng Song and Yong Liang Guan. 'Simulation of Nakagami fading channels with arbitrary cross-correlation and fading parameters'. In: *IEEE Transactions on Wireless Communications* 3.5 (2004), pp. 1463–1468. DOI: 10.1109/TWC.2004.833469.

[78] Nikolaos Kouiroukidis and Georgios Evangelidis. 'The Effects of Dimensionality Curse in High Dimensional kNN Search'. In: *2011 15th Panhellenic Conference on Informatics*. 2011, pp. 41–45. DOI: 10.1109/PCI.2011.45.

[79] Wen-Qin Wang, Hing Cheung So and Alfonso Farina. 'An Overview on Time/-Frequency Modulated Array Processing'. In: *IEEE Journal of Selected Topics in Signal Processing* 11.2 (2017), pp. 228–246. DOI: 10.1109/JSTSP.2016.2627182.

[80] P. Antonik and M. C. Wicks. 'Frequency diverse array radars'. In: *IEEE Radar Conf.* 2006, pp. 215–217. DOI: 10.1109/RADAR.2006.1631800.

[81] Wen-Qin Wang. 'Frequency Diverse Array Antenna: New Opportunities'. In: *IEEE Ant. and Propagat. Mag.* 57.2 (2015), pp. 145–152. DOI: 10.1109/MAP.2015.2414692.

[82] S Ke, M He, X Bu and W. Cai. 'A Leakage-Based Directional Modulation Scheme for Frequency Diverse Array in Robot Swarm Networks'. In: *IEEE Access* 8 (2020), pp. 107823–107837. DOI: 10.1109/ACCESS.2020.2998938.

[83] W Khan, M Qureshi and S Saeed. 'Frequency Diverse Array Radar With Logarithmically Increasing Frequency Offset'. In: *IEEE Ant. and Wireless Propagat. Letters* 8 (2014), pp. 499–502. DOI: 10.1109/TSP.2015.2422680.

[84] J Xu, G Liao, S Zhu, L Huang and H.C. So. 'Joint range and angle estimation using MIMO radar with frequency diverse array'. In: *IEEE Trans. Signal Process.* 63.13 (20115), pp. 3396–3410. DOI: 10.1109/TSP.2015.2422680.

[85] W-Q. Wang. 'Overview of frequency diverse array in radar and navigation applications'. In: *IET Radar, Sonar Navigat.* 10.6 (2016), pp. 1001–1012. DOI: 10.1109/TSP.2015.2422680.

[86] C Sammartino, C.J. Baker and H. D. Griffiths. 'Frequency diverse MIMO techniques for radar'. In: *IEEE Trans. Aerosp. Electron. Syst.* 49.1 (2013), pp. 201–222. DOI: 10.1109/TAES.2013.6404099.

[87] E. Fazzini, A. Costanzo and D. Masotti. 'Ad-hoc WPT Exploiting Multi-sine Excitation of Linear Frequency Diverse Arrays'. In: *2022 Wireless Power Week*. 2022. DOI: 10.1109/WPW54272.2022.9853938.

[88] E. Fazzini, M. Shanawani, A. Costanzo and D. Masotti. 'A Logarithmic Frequency-Diverse Array System for Precise Wireless Power Transfer'. In: *2020 50th European Microwave Conference (EuMC)*. 2021, pp. 646–649. DOI: 10.23919/EuMC48046.2021.9338242.

[89] Jiajie Tan, Edmund Sumpena, Weipeng Zhuo, Ziqi Zhao, Mengyun Liu and S.-H. Gary Chan. 'IoT Geofencing for COVID-19 Home Quarantine Enforcement'. In: *IEEE Internet of Things Magazine* 3.3 (2020), pp. 24–29. DOI: 10.1109/IOTM.0001.2000097.

[90] Jad Helmy and Ahmed Helmy. 'The Alzimio App for Dementia, Autism & Alzheimer's: Using Novel Activity Recognition Algorithms and Geofencing'. In: *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*. 2016, pp. 1–6. DOI: 10.1109/SMARTCOMP.2016.7501720.

[91] Elie Hermand, Tam W. Nguyen, Mehdi Hosseinzadeh and Emanuele Garone. 'Constrained Control of UAVs in Geofencing Applications'. In: *2018 26th Mediterranean Conference on Control and Automation (MED)*. 2018, pp. 217–222. DOI: 10.1109/MED.2018.8443035.

[92] Rodrigo R. Oliveira, Ismael M.G. Cardoso, Jorge L.V. Barbosa, Cristiano A. da Costa and Mario P. Prado. 'An intelligent model for logistics management based on geofencing algorithms and RFID technology'. In: *Expert Systems with Applications* 42.15 (2015), pp. 6082–6097. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2015.04.001. URL: https://www.sciencedirect.com/science/article/pii/S0957417415002316.

[93] S. Y. Nusenu. 'Development of Frequency Modulated Array Antennas for Millimeter-Wave Communications'. In: *Wireless Communications and Mobile Computing* (2019). DOI: 10.1155/2019/6940708.

[94] S. Y. Nusenu and A. Basit. 'Frequency Diverse Array Antennas: From Their Origin to Their Application in Wireless Communication Systems'. In: *Journal of Computer Networks and Communications* (2018). DOI: 10.1155/2018/5815678.

[95] Jie Xiong, Yaw Nusenu Shaddrack and Wang Wen-Qin. 'Directional Modulation Using Frequency Diverse Array For Secure Communications'. In: *Wireless Pers. Commun.* 95 (2017), pp. 2679–2689. DOI: 10.1007/s11277-3949-1.

[96] J. M. Hamamreh, H. M. Furqan and H. Arslan. 'Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Sur-

vey'. In: *IEEE Communications, Surveys and Tutorials* 21.2 (2019), pp. 1773–1828. DOI: 10.1109/COMST.2018.2878035.

[97] J. M. Lin, Q. M. Li, J. Yang, H. Shao and W-Q. Wand. 'Physical-Layer Security for Proximal Legitimate User and Eavesdropper: A frequency Diverse Array Beamforming Approach'. In: *IEEE Transactions on Information Forensics and Security* 13.3 (2018), pp. 671–684. DOI: 10.1109/TIFS.2017.2765500.

[98] A. Nessa, B. Adhikari, F. Hussain and X.N. Fernando. 'A Survey of Machine Learning for Indoor Positioning'. In: *IEEE Access* (2020), pp. 214945–214965. DOI: 10.1109/ACCESS.2020.3039271.

[99] P. Meissner and K. Witrisal. 'Multipath-assisted single-anchor indoor localization in an office environment'. In: *19th Int. Conf. on Systems, Signals and Image Processing (IWSSIP)*. 2012. DOI: 10.1109/WPTC51349.2021.9458208.

[100] G. Huang, Y. Ding, S Ouyang and V. Fusco. 'Frequency diverse array with random logarithmically increasing frequency offset'. In: *Microwave and Optical Tech Letters* 62.7 (2020), 2554–2561 . DOI: 10.1002/mop.32337.

[101] Simone Del Prete, Marina Barbiroli and Franco Fuschini. 'Frequency Diverse Array for Signal Geofencing in Wireless Communications: Does It Work?' In: *IEEE Open Journal of Antennas and Propagation* (2024). ©2024 IEEE.

[102] X. Wu, H. Shao, J. Lin, Q. Li and Q. Shi. 'High-Speed User-Centric Beampattern Synthesis via Frequency Diverse Array'. In: *IEEE Trans. on Sig. Proc.* 69 (2021), 1226–1241 . DOI: 10.1109/TSP.2021.3054988.

[103] Enrico Fazzini, A. Baris Gok, Alessandra Costanzo and Diego Masotti. 'Accurate Ranging Exploiting a 32-patch Frequency Diverse Array with Circular Symmetry'. In: *2022 16th European Conference on Antennas and Propagation (EuCAP)*. 2022, pp. 1–5. DOI: 10.23919/EuCAP53622.2022.9768991.

[104] C. Centipete and S. Demir. 'Multipath characteristics of frequency diverse arrays over a ground plane'. In: *IEEE Trans. on Ant. and Propagat.* 62.7 (2014), pp. 3567–3574. DOI: 10.1109/TAP.2014.2316292.

[105] Qian Cheng, Shilian Wang, Vincent Fusco, Fanggang Wang, Jiang Zhu and Chao Gu. 'Physical-Layer Security for Frequency Diverse Array-Based Directional Modulation in Fluctuating Two-Ray Fading Channels'. In: *IEEE Transactions on Wireless Communications* 20.7 (2021), pp. 4190–4204. DOI: 10.1109/TWC.2021.3056521.

[106] Simone Del Prete, Franco Fuschini, Marina Barbiroli and Mohammad Hossein Zadeh. 'A Study on Propagation of Frequency Diverse Array in Multipath Environments'. In: *2023 IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC)*. ©2023 IEEE. IEEE. 2023, pp. 090–094.

[107] Qian Cheng, Vincent Fusco, Shilian Wang and Jiang Zhu. 'A Two-Ray Multipath Model for Frequency Diverse Array-Based Directional Modulation in MISOME Wiretap Channels'. In: *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. 2019, pp. 1–5. DOI: 10.1109/VTCFall.2019.8890978.

[108] Cagri Cetintepe and Simsek Demir. 'Multipath Characteristics of Frequency Diverse Arrays Over a Ground Plane'. In: *IEEE Transactions on Antennas and Propagation* 62.7 (2014), pp. 3567–3574. DOI: 10.1109/TAP.2014.2316292.

[109] Franco Fuschini, Enrico M. Vitucci, Marina Barbiroli, Gabriele Falciasecca and Vittorio Degli-Esposti. 'Ray tracing propagation modeling for future small-cell and indoor applications: A review of current techniques'. In: *Radio Science* 50.6 (2015), pp. 469–485. DOI: 10.1002/2015RS005659.

[110] Jie Xiong, Wang Wen-qin, Shao Huaizong and Chen Hui. 'Frequency Diverse Array Transmit Beampattern Optimization With Genetic Algorithm'. In: *IEEE Wireless Ant. and Wirel. Propagation Letters* 16 (2017), pp. 469–472. DOI: 10.1109/LAWP.2016.2584078.

[111] Enrico Fazzini, Alessandra Costanzo and Diego Masotti. 'Range Selective Power Focusing with Time-controlled Bi-dimensional Frequency Diverse Array'. In: *IEEE Wireless Power Trnsfer Conf.* 2021. DOI: 10.1109/WPTC51349.2021.9458208.

[112] S Goel and R Negi. 'Guaranteeing Secrecy using Artificial Noise'. In: *IEEE Trans. on Wireless Comm.* 7.6 (2008), pp. 2180–2189. DOI: 10.1109/TWC.2008.060848.

[113] S. Ji, W.Q. Wang, H. Chen and Z. Zheng. 'Secrecy capacity analysis of AN-aided FDA communication over Nakagami-m fading channels'. In: *IEEE Wireless Commun. Lett.* 7.6 (2018), pp. 1034–1037. DOI: 10.1109/LWC.2018.2850896.

[114] Yuanquan Hong, Xiaojun Jing, Hui Gao and Yuan He. 'Fixed Region Beamforming Using Frequency Diverse Subarray for Secure mmWave Wireless Communications'. In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 2706–2721. DOI: 10.1109/TIFS.2020.2969576.

[115] W-Q. Wang. 'Range-Angle Dependent Transmit Beampattern Synthesis for Linear Frequency Diverse Arrays'. In: *IEEE Transactions on Ant. and Propagat.* 61.8 (2013), pp. 4073–4081. DOI: 10.1109/TAP.2013.2260515.

[116] K. Chen, S. Yang, Y. Chen and S.-W. Qu. 'Accurate Models of Time-Invariant Beampatterns for Frequency Diverse Arrays'. In: *IEEE Trans. on Ant. and Propagat.* 67.5 (2019), 3022–3029 . DOI: 10.1109/TAP.2019.2896712.