Physical Layer Security in Frequency-Domain Fast-Fading TDD Time-Reversal SISO OFDM Communication

Sidney J. Golstein*†, Trung-Hien Nguyen*, François Rottenberg*, François Horlin*, Philippe De Doncker*, and Julien Sarrazin†

*Wireless Communication Group, Université Libre de Bruxelles, 1050 Brussels, Belgium

†Sorbonne Université, CNRS, Laboratoire de Génie Electrique et Electronique de Paris, 75252, Paris, France
Université Paris-Saclay, CentraleSupélec, CNRS, Laboratoire de Génie Electrique et Electronique de Paris, 91192, Gif-sur-Yvette, France

{sigolste,trung-hien,francois.rottenberg,fhorlin,philippe.dedoncker}@ulb.ac.be
julien.sarrazin@sorbonne-universite.fr

***Abstract*—A frequency domain (FD) fast-fading (FF) time division duplex (TDD) time-reversal (TR) precoder is proposed to perform physical layer security (PLS) in single-input single-output (SISO) system using orthogonal frequency-division multiplexing (OFDM). To maximize the secrecy of the communication, the design of an artificial noise (AN) signal well-suited to the proposed FD TR-based OFDM SISO system is derived. This new scheme guarantees the secrecy of a communication toward a legitimate user when the instantaneous channel state information (CSI) of a potential eavesdropper is not known. The instantaneous CSI of the legitimate receiver is known at the transmitter thanks to channel reciprocity in TDD systems. In particular, we derive an AN signal that does not corrupt the data transmission to the legitimate receiver but degrades the decoding performance of the eavesdropper. We consider three possible decoding structures at the eavesdropper position depending on the handhsake procedure, and we derive closed-form approximations of the AN energy to inject in order to maximize the secrecy rate (SR) of the communication. Furthermore, a waterfilling-like power allocation strategy, keeping into account the AN injection, is presented to further enhance the secrecy of the scheme. Simulation results are presented to demonstrate the security performance of the proposed secure FD TR SISO OFDM system.**

***Index Terms*—Physical layer security, time-reversal, time division duplex, fast-fading, eavesdropper, SISO-OFDM, artificial noise, waterfilling, secrecy rate.**

I. Introduction

THE demand for wireless communication services and the number of interconnected users is increasing day by day. Internet-based services have become indispensable in daily life. Wireless media has become the dominant access for most of these services and is intrisically unsecure due to its broadcast nature. Therefore, several issues have emerged and need to be urgently adressed such as data confidentiality and integrity, [1], [2].

The concept of security started in Shannon's work ~~with cryptography based security~~, [3]. ~~Shannon's security model using cryptographic key based sharing approaches was widely used despite having multiple serious drawbacks~~. First, these techniques are based on the assumption that the eavesdropper (Eve) has limited computational power capabilities. With the fast development in computing power devices, secret keys are nowadays more subject to successful brut-force attacks. Second, the security is enhanced when the key length increases, resulting in more waste of resources. In addition, the key management processes become a real issue with the deployment of large-scale heterogeneous and decentralized networks involving different acces technologies, such as 5G networks. Finally, the emergence of power-limited, delay-sentive and processing-restricted wireless technologies, such as Internet Of Things (IoT), banking, health monitoring, vehicular communications, makes cryptography-based methods naturally unsuitable, [1].

To circumvent the aforementionned issues, physical layer security (PLS) has emerged as an effective way to enhance security of wireless communications, [4]–[7]. PLS classically takes benefit of the characteristics of wireless channels (e.g., multipath fading, noise, dispersion, diversity) to improve security of communications against potential eavesdroppers without relying on computational complexity, i.e., the security will not be affected if Eve has unlimited computing capabilities, [8], [9].

The starting point of PLS was exposed in 1975 by Wyner where it is explained that a communication can be made secure, without sharing a secret key, when the wiretap channel of the eavesdropper is a degraded version, i.e., ~~much~~ noisier, of the legitimate link (Bob), [10]. This work was later extended to the broadcast channel in [11] and to the Gaussian channel in [12].

It is of prime importance to evaluate the effectiveness of a PLS scheme by quantifying the degree of secrecy it can provide with a suitable metric. One of the most studied class of PLS metrics is ~~the signal-to-interference-plus-noise ratio (SINR) based metric where the secrecy channel capacity is commonly used~~. It is defined as the difference in channel capacities between the legitimate receiver and the eavesdropper, and was first formulated in [10]. PLS performances highly

This work was supported by the ANR GEOHYPE project, grant ANR-16-CE25-0003 of the French Agence Nationale de la Recherche and was also carried out in the framework of COST Action CA15104 IRACON.

depend on the availability of ~~the~~ channel state information (CSI) at the communication parties. It is generaly assumed that the transmitter (Alice) knows Bob CSI but does not know or partially knows Eve CSI , since she is considered as passive, [1]. We often assume Eve as an external passive node of the network that tries to eavesdrop the data. We usually consider that Bob and Eve CSI's are spatially independent. PLS can be achieved by increasing the SINR at the intended position and decreasing the SINR at the unintended position by designing a suitable channel-based adaptive transmission scheme and/or by injecting an artificial noise (AN) signal to the data. These techniques can be implemented in the space, time and/or frequency domains, [1], [13], [14].

Channel-based adaptation secrecy schemes were first introduced in [15]–[17]. In these works, it was proven that positive secrecy can be obtained even if, on average, Bob is a degraded version of Eve, by optimizing or adapting at the transmitter side the communication parameters. In doing so, the transmitted signal will be optimal for Bob's channel and not for Eve's one since they experience different fading. The concept of AN addition was first established in [18]–[20]. The idea is to made Eve's channel condition artificially degraded by intentionnaly adding an AN signal at the transmitter side. This AN signal does ~~not have to~~ degrade Bob's channel, therefore leading to a PLS enhancement, [1]

While many works implement these schemes using multiple antennas at the transmitter, via frequency diverse array beamforming [21], [22], directional modulation (DM) [23], antenna subset modulation (ASM) [24], near-field direct antenna modulation (NFDAM) [25], [26], multiple-inputs multiple-outputs (MIMO) diversity [27]–[30],... few ones ~~intend to~~ do it using single-input single-output (SISO) systems [8], [31]–[39].

In [31], a symbol waveform optimization technique in time-domain (TD) is proposed to reach a desired SINR at Bob with AN injection, under power constraint, when eavesdropper's CSI is not known. Another approach to increase the SINR in SISO systems is time reversal (TR) pre-filtering. This has the advantage to be implemented with a simple precoder at the transmitter. TR achieves a focusing gain at the intended receiver position only, thereby naturally offering intrinsic anti-eavesdropping capabilities, [32], [40]. TR is achieved by up/downsampling the signal in the TD. While the impact of the back-off rate (BOR), defined as the up/downsampling rate [41], was studied in [8], [32], very basic decoding capabilities were attributed at Eve. TR can also be equivalently implemented in frequency domain (FD) by replicating and shifting the signal spectrum, [42]. FD implementation has the advantage to be easily performed using orthogonal frequency-division multiplexing (OFDM). In [33], [34] FD OFDM schemes are presented consisting of subcarriers index selection. Only several subcarriers are used for data transmission depending on their channel gains.

To further enhance the secrecy, few works combine TD or FD precoding with AN injection, [35]–[39]. In [35]–[37], TD TR precoders are presented. In these works, the AN is added either on all the channel taps or on a set of selected taps. While the condition for AN generation is given, its derivation is however not detailed. In [38], [39], FD precoders using OFDM and AN injection are presented. The idea is to use several OFDM subcarriers for dummy data transmission, i.e., several subcarriers are used for data obfuscation. However, the encryption information must be shared between the transmitter and the legitimate receiver, leading to more processing needed at the receiver. In addition, the security is enhanced when more subcarriers are used for data obfuscation, at the expense of the data rate. Furthermore, it is assumed that Eve has no knowledge about the legitimate link.

In this article, we present an original and novel FD TR precoder in SISO OFDM systems with AN addition, which establish secure communications. The paper is an extension of the study in [8] where only one decoding capability was considered at the wiretap link. In the following, we investigate three scenarios corresponding to three different eavesdropper knowledges depending on the handshake procedure. Bob's CSI is fully known at Alice, using channel reciprocity inherent from time division duplex (TDD) systems, in a fast fading (FF) environment. An AN signal is designed in the FD to maximize the ergodic SR of the communication in the presence of a passive eavesdropper whose instantaneous CSI is supposed unknown. A power allocation technique, keeping into account the AN injection, is also derived in order to further enhance the communication SR. The proposed scheme uses only frequency diversity inherently present in multipath environments to achieve security. It can therefore be used in SISO systems and is then well-suited for resource-limited nodes such as encountered in IoT or vehicular communications for instance, [8]. In addition, the presented scheme does not suppose any degradation of Eve's channel compared to the legitimate link. Furthermore, the OFDM implementation makes this approach compatible with LTE and 5G networks.

The reminder of this article is organized as follows: the handshake and the communication protocols are exposed in Section II. Section III presents a closed-form approximation of the amount of AN energy to be injected in order to maximize the SR, for the different decoding structures at Eve. A derivation of the required SNR at Bob to target a desired SR is proposed, as a function of the communication parameters. Then, a waterfilling optimization procedure is outlined in order to further increase the communication SR. Theoretical and numerical results are shown in Section IV. Section V concludes the paper.

Notation: the italic lower-case letter denotes a complex number. Greek letter corresponds to a scalar, the bold lower-case letter denotes a column vector. Bold upper-case letter corresponds to a matrix; $\mathbf{I}_N$ is $N \times N$ identity matrix; $(.)^{-1}$, $(.)^*$, $(.)^H$ are respectively the inverse, the complex conjugate and the Hermitian transpose operators; $\mathbb{E}[.]$ is the expectation operator; $|.|$ is the modulus operator (element-wize modulus if we deal with a matrix); $\odot$ is the element-wize (hadamard) product between two vectors of same dimension.

II. System Model

A. Handshake Protocol

Prior to the secure data transmission between Alice and Bob, a handshake protocol must take place. Depending on it,

Eve will obtain different knowledges about the communication parameters which will lead to different decoding capabilities and so, different security performances.

In this paper, we consider a Fast Fading (FF) Time-Division Duplex (TDD) communication. In doing so, we will investigate three different decoding schemes at Eve depending on weither Alice or Bob wants to first initiate the secure communication. The FF hypothesis means that each OFDM block sent by Alice will experience a different channel realization. ICI, donner des ordres de grandeurs. On dit que le fait qu'on soit en FF ne permet pas à Eve de learn des paramètres car à chaque block OFDM le canal change MAIS d'un autre côté, ce le fading n'est pas assez rapide que pour qu'Alice et Bob ait le temps de s'envoyer une request + ACK sans le canal ait changé... The TDD hypothesis implies that channel reciprocity between Alice and Bob or Alice and Eve can be used.

The first two scenarios appear when Bob first requests to Alice for secure communication. In both cases, Bob transmits a pilot to Alice allowing her to know Bob's channel.

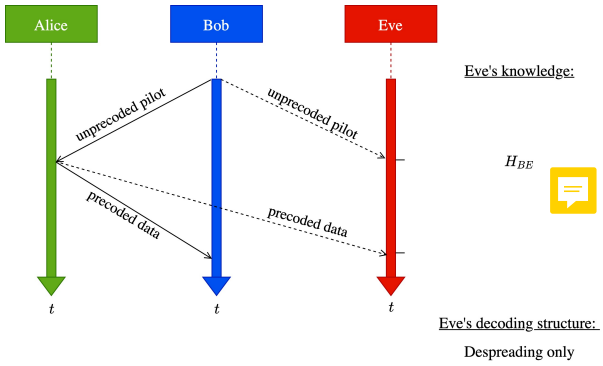

Figure 1. FF TDD, Bob initiates the communication, no pilot sent

If Alice only transmits precoded data to Bob, Eve will not be able to know anything about the communication parameters. In that situation, she will implement the "*same decoding structure as Bob*", i.e., she will only despread the received sequence. This situation is presented in Fig.1.

However, if Alice sends a precoded pilot and precoded data to Bob, Eve will be able to know her equivalent channel $\mathbf{H}_B^* \mathbf{H}_E$ and will implement the "*matched filtering*" decoding structure. This is depicted in Fig.2

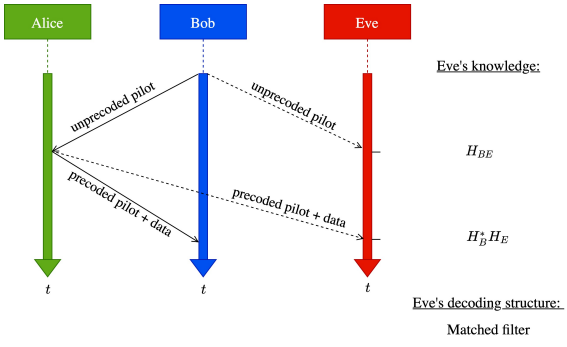

Figure 2. FF TDD, Bob initiates the communication, pilots sent

The third investigated situation arises when Alice asks first to Bob for secure commnication, as depicted in Fig.3. In this configuration, she sends a pilot to Bob allowing Eve to estimate her own channel frequency response (CFR) $\mathbf{H}_E$. From that, Bob acknowledges to Alice without need of sending his channel estimation $\mathbf{H}_B$. This comes from the channel reciprocity property in TDD systems. Finally, Alice will send precoded data without pilot to Bob. From the FF assumption, Eve cannot learn the precoding performed by the transmitter. In this configuration, Eve will implement the *"own channel knowledge"* decoding structure.

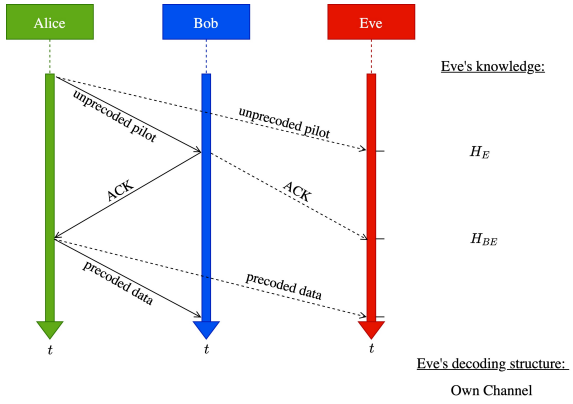

Figure 3. FF TDD, Alice initiates communication

In the following, these three decoding schemes will be investigated and analytic models will be derived.

B. Communication Protocol

When the handshaking procedure between Alice and Bob is established, secure data can be transmitted to Bob. In order to do so, the useful data will be precoded and an AN signal $\mathbf{w}$ will be added to it before transmission, as depicted in Fig.4.

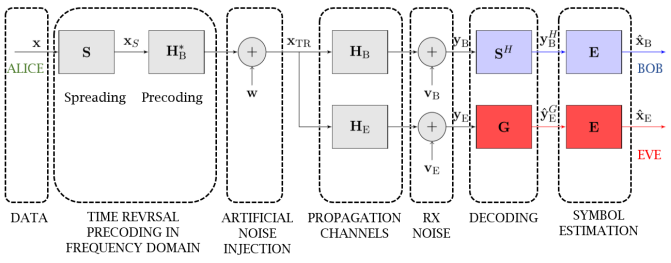

Figure 4. Communication scheme

The system model was already described in [8]. Briefly, it consists ~~to~~ data transmission onto OFDM blocks with Q subcarriers. We consider that only one data block $\mathbf{x}$ is sent and is composed of N symbols x_n (for $n = 0, \ldots, N-1$, with $N \leq Q$). The symbol x_n is a zero-mean random variable (RV) with variance $\mathbb{E}\left[|x_n|^2\right] = \sigma_x^2 = 1$, i.e., a normalized constellation is considered. The block is then spread by a factor $U = Q/N$, called back-off rate (BOR), thanks to the spreading matrix $\mathbf{S}$ of size $Q \times N$. The design of the spreading matrix is such that it allows not to increase the PAPR, as suggested in [43]. The

matrix is expressed in [8]. The signal is spread in the FD by repetiting and shifting its spectrum, [42]. In doing so, each data symbol will be transmitted onto U different subcarriers with a spacing of N subcarriers, introducing frequency diversity. The spread sequence is then precoded with the complex conjugate of Bob's channel $\mathbf{H}_{\mathrm{B}}^{*}$, before addition of the AN signal $\mathbf{w}$ and transmission.

The AN should not have any impact at Bob's position but should be seen as interference everywhere else since Alice does not have any information about Eve's instantaneous CSI, i.e., Eve is a passive node. Furthermore, this signal should not be guessed at the unintended positions to ensure the secure communication. From that, the idea of the AN signal addition is to corrupt the data detection everywhere except at Bob's position. With these considerations, the transmitted sequence becomes:

$$\mathbf{x}_{\mathrm{TR}} = \sqrt{\alpha}\, \mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\, \mathbf{x} + \sqrt{1-\alpha}\, \mathbf{w} \tag{1}$$

where $\alpha \in [0,1]$ defines the ratio of the total energy sent dedicated to the useful signal, knowing that $\mathbb{E}\left[\left|\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}\right|^{2}\right] = \mathbb{E}\left[|\mathbf{w}|^{2}\right] = 1/U$. Whatever the value of α, the total transmitted power remains constant, i.e., $1/U$.

In order to precod the data, Alice needs to have the knowledge of Bob CFR. We consider that Alice can perfectly estimate Bob CFR. The channels between Alice and Bob ($\mathbf{H}_{\mathrm{B}}$) and between Alice and Eve ($\mathbf{H}_{\mathrm{E}}$) are assumed to be static during the transmission of one OFDM symbol. However, the CFRs differ between two subsequent OFDM blocks thanks to the FF hypothesis. $\mathbf{H}_{\mathrm{B}}$ and $\mathbf{H}_{\mathrm{E}}$ are $Q \times Q$ diagonal matrices whose elements are $h_{\mathrm{B},q}$ and $h_{\mathrm{E},q}$ (for $q = 0,...,Q-1$) and follow a zero-mean unit-variance complex normal distribution, i.e., their modulus follow a Rayleigh distribution. We also consider that the overall channel energies are normalized to unity for each channel realization. The precoding matrix $\mathbf{H}_{\mathrm{B}}^{*}$ is also a diagonal matrix with elements $h_{\mathrm{B},q}^{*}$. At Bob, a despreading operation is performed by applying $\mathbf{S}^{H}$. We consider that Bob and Eve know the spreading sequence. Bob will then apply a ZF equalization. As stated in section II-A, three decoding structures $\mathbf{G}$ will be investigated at Eve. These different schemes will lead to different level of security performances. After decoding, Eve also perfoms a ZF equalization. A perfect synchronization is finally assumed at Bob and Eve positions.

1) Artificial noise Design: In order not to have any impact at the intended position, the AN signal must satisfy the following condition:

$$\mathbf{A}\mathbf{w} = \mathbf{0} \tag{2}$$

where $\mathbf{A} = \mathbf{S}^{H}\mathbf{H}_{\mathrm{B}} \in \mathbb{C}^{N\times Q}$. Condition (2) ensures that $\mathbf{w}$ lies in the right null space of $\mathbf{A}$. If we perform a singular value decomposition (SVD) of $\mathbf{A}$, we obtain:

$$\mathbf{A} = \mathbf{U}\left(\mathbf{\Sigma}\ \mathbf{0}_{Q-N\times Q}\right)\begin{pmatrix}\mathbf{V}_1^{H}\\ \mathbf{V}_2^{H}\end{pmatrix} \tag{3}$$

where $\mathbf{U} \in \mathbb{C}^{N\times N}$ contains left singular vectors, $\mathbf{\Sigma} \in \mathbb{C}^{N\times N}$ is a diagonal matrix containing singular values, $\mathbf{V}_1 \in \mathbb{C}^{Q\times N}$ contains right singular vectors associated to non-zero singular values, and $\mathbf{V}_2 \in \mathbb{C}^{Q\times Q-N}$ contains right singular vectors that span the right null space of $\mathbf{A}$. Therefore, the AN signal can be expressed as:

$$\mathbf{w} = \beta\mathbf{V}_2\tilde{\mathbf{w}} \tag{4}$$

which ensures that (2) is satisfied for any arbitrary vector $\tilde{\mathbf{w}} \in \mathbb{C}^{Q-N\times 1}$. Since $Q = NU$, as soon as $U \geq 2$, there is a set of infinite possibilities to generate $\tilde{\mathbf{w}}$ and therefore the AN signal. In the following, we assume that $\tilde{\mathbf{w}}$ is a zero-mean circularly symmetric white complex Gaussian noise with covariance matrix $\mathbb{E}\left[\tilde{\mathbf{w}}(\tilde{\mathbf{w}})^{H}\right] = \mathbf{I}_{Q-N}$. The AN signal is then generated thanks to (4) with a weighting coefficient β to have an energy of 1/U.

2) Received sequence at the intended position: After despreading, the received sequence at Bob is:

$$\mathbf{y}_{\mathrm{B}}^{H} = \sqrt{\alpha}\, \mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\mathbf{x} \ + \ \mathbf{S}^{H}\mathbf{v}_{\mathrm{B}} \tag{5}$$

where $\mathbf{v}_{\mathrm{B}}$ is the FD complex AWGN. The noise's auto-correlation is $\mathbb{E}\left[|v_{\mathrm{B},n}|^{2}\right] = \sigma_{\mathrm{V,B}}^{2}$ and the covariance matrix is $\mathbb{E}\left[(\mathbf{S}^{H}\mathbf{v}_{\mathrm{B}}).(\mathbf{S}^{H}\mathbf{v}_{\mathrm{B}})^{H}\right] = \sigma_{\mathrm{V,B}}^{2}.\mathbf{I}_{N}$. We also assume that the data and noise symbols, x_n and $v_{\mathrm{B,n}}$ respectively, are independent of each other. In (5), each transmitted symbol is affected by a real gain at the position of the legitimate receiver. This results from the data precoding at Alice leading to the product $\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{B}}^{*}$ in the received sequence at Bob, which is a real diagonal matrix. The gains differ between each symbol in the OFDM block but increases with an increase of the BOR value as each symbol would be sent on more subcarriers and would benefit from a larger frequency diversity gain. If we consider a fixed bandwidth, the TR focusing effect is enhanced for higher BOR's at the expense of the data rate. We also observe that no AN contribution is present in (5) since (2) is respected. A ZF equalization is performed at the receiver leading to:

$$\begin{aligned}\hat{\mathbf{x}}_{\mathrm{B}} &= \left(\sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\mathbf{x} + \mathbf{S}^{H}\mathbf{v}_{\mathrm{B}}\right)\\ &= \mathbf{x} + \left(\sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\right)^{-1}\mathbf{S}^{H}\mathbf{v}_{\mathrm{B}}\end{aligned} \tag{6}$$

From (6), a perfect data recovery is possible in high SNR scenarios.

3) Received sequence at the unintended position: The received sequence at the eavesdropper position is given by:

$$\mathbf{y}_{\mathrm{E}}^{G} = \sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{G}\mathbf{v}_{\mathrm{E}} \tag{7}$$

where $\mathbf{G}$ is a $N \times Q$ filter matrix performed by Eve, $\mathbf{v}_{\mathrm{E}}$ is the complex AWGN. The noise auto-correlation is $\mathbb{E}\left[|v_{\mathrm{E,n}}|^{2}\right] = \sigma_{\mathrm{V,E}}^{2}$. In (7), $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}$ is a complex diagonal matrix. Therefore, since the transmitted data is precoded to reach Bob, each received symbol component will be affected by a random coefficient. This coefficient can be real or complex depending on the decoding structure $\mathbf{G}$. If it is complex, its magnitude does not depend on the BOR value. It results in an absence of TR gain at the unintended position. As a consequence, worse decoding performance will be expected at Eve than at the intended position. In addition, we observe in (7) a term depending on the AN signal. It results from the precoding at Alice since $\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w} \neq \mathbf{0}$ in general. This term introduces an

interference at Eve and thus ~~scrambles~~ the received constellation even in a noiseless environment. After ZF equalization, the estimated symbols are:

$$\begin{aligned}\hat{\mathbf{x}}_{\mathrm{E}} &= \left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}+\sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}+\mathbf{G}\mathbf{v}_{\mathrm{E}}\right)\\ &= \sqrt{\alpha}\mathbf{x}+\sqrt{1-\alpha}\left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}+\left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{v}_{\mathrm{E}}\end{aligned} \tag{8}$$

Equation (8) shows that the addition of AN in the FD TR SISO OFDM communication can secure the data transmission. ~~In fact~~, a term depending on the AN signal still remains after equalization even in high SNR scenarios. It is to be noted that, since $\mathbf{w}$ is generated from an infinite set of possibilities, even if Eve knows its equivalent channel $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}$ and the spreading sequence, she cannot estimate the AN signal to try retrieving the data. The degree of security will depend on the investigated scenario, i.e., decoding structure $\mathbf{G}$ at Eve, and the amount of data energy (via α) that is injected into the communication, as it will be explained in Section III.

III. Performance Assessments

The classical metric used to evaluate the degree of secrecy in a communication in the PLS field is the secrecy capacity channel, or secrecy rate (SR). The SR is defined as the maximum transmission rate that can be supported by the legitimate receiver's channel while ensuring the impossibility for the eavesdropper to retrieve the data, [44]. In the ergodic sense, it can be expressed as:

$$\begin{aligned}C_S &= \left[\mathbb{E}\left[\log_2\left(1+\gamma_B\right)-\log_2\left(1+\gamma_E\right)\right]\right]^{+}\\ &\approx \left[\log_2\left(1+\mathbb{E}\left[\gamma_B\right]\right)-\log_2\left(1+\mathbb{E}\left[\gamma_E\right]\right)\right]^{+}\end{aligned} \tag{9}$$

where $[x]^{+}$ ~~is equal to x if $x \geq 0$, or 0 if $x \leq 0$~~, γ_B and γ_E being respectively the SINR at Bob and Eve's positions. To estimate the SR of the communication, we observe from (9) that an analytic expression of Bob and Eve ergodic SINR must be derived.

A. Hypothesis

In order to obtain the analytic models, we consider the following assumptions:

- Q subcarriers, back off rate = U, $N = Q/U$ symbols sent per OFDM block
- $\mathbf{H}_{\mathrm{B}} = \mathbf{H}_{\mathrm{B},x} + j\mathbf{H}_{\mathrm{B},y} \sim \mathcal{CN}(0,1) \sim \mathcal{N}(0,\frac{1}{2}) + j\mathcal{N}(0,\frac{1}{2})$
- $\mathbf{H}_{\mathrm{E}} = \mathbf{H}_{\mathrm{E},x} + j\mathbf{H}_{\mathrm{E},y} \sim \mathcal{CN}(0,1) \sim \mathcal{N}(0,\frac{1}{2}) + j\mathcal{N}(0,\frac{1}{2})$
- $h_{B,i} \perp\!\!\!\perp h_{B,j}, \forall i \neq j$, i.e., no frequency correlation between Bob's channel subcarriers
- $h_{E,i} \perp\!\!\!\perp h_{E,j}, \forall i \neq j$, i.e., no frequency correlation between Eve's channel subcarriers[1].
- $h_{B,i} \perp\!\!\!\perp h_{E,j}, \forall i, j$, i.e., Bob and Eve are sufficiently spaced leading to no spatial correlation between them.

[1]Thanks to the design of the spreading matrix, the U subcarriers composing one symbol are spaced by $N = Q/U$ subcarriers. If this distance is larger than the coherence bandwidth of the channel, the assumption holds. This usually occurs in rich multipath environments and for sufficiently large bandwidths and moderate BOR values.

B. SINR determination

In this section, we derive the ergodic SINR for the transmitted symbols n, $n = 0, \ldots, N-1$ at Bob and Eve positions depending on the investigated scenario, i.e., on the handshake procedure.

1) At the intended position: At Bob, a simple despreading operation is performed. As a reminder, due to the precoding at the transmitter side, every transmitted data symbol will be affected by a real gain, as expressed in (5). The ergodic SINR for the transmitted symbols n is given by:

$$\begin{aligned}\mathbb{E}\left[\gamma_{B,n}\right] &= \mathbb{E}\left[\frac{\left|\sqrt{\alpha}A_{1,n}x_n\right|^2}{\left|A_{2,n}\right|^2}\right] = \alpha\mathbb{E}\left[\left|A_{1,n}x_n\right|^2\right]\mathbb{E}\left[\frac{1}{\left|A_{2,n}\right|^2}\right]\\ &\geq \frac{\alpha\mathbb{E}\left[\left|A_{1,n}x_n\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]} = \frac{\alpha\mathbb{E}\left[\left|A_{1,n}\right|^2\right]\mathbb{E}\left[\left|x_n\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]}\end{aligned} \tag{10}$$

where $A_{1,n} = \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2$, x_n is the n^{th} data symbol, and $A_{2,n} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}\left|v_{\mathrm{B},n+iN}\right|$ is the n^{th} noise symbol component and where it is observed that $A_{1,n} \perp\!\!\!\perp x_n \perp\!\!\!\perp A_{2,n}$.
For the term $A_{1,n}$, we have (see A-A1):

$$\mathbb{E}\left[\left|A_{1,n}\right|^2\right] = \frac{\alpha(U+1)}{U} \tag{11}$$

The mean energy per noise symbol, $A_{2,n}$, can be derived as follow (see A-A2):

$$\mathbb{E}\left[\left|A_{2,n}\right|^2\right] = \sigma_{\mathrm{V,B}}^2 \tag{12}$$

From (10), (11) and (12), the ergodic SINR for particular symbols n at the intended position is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \geq \frac{\alpha\,(U+1)}{U\,\sigma_{\mathrm{V,B}}^2} \tag{13}$$

It was observed in simulations than the lower-bound (13) is tight enough to be used as an approximation of the averaged SINR at the intended position.

2) At the unintended position: At the unintended position, the received signal before ZF equalization is given by (7). Let's introduce $\mathbf{A}_1 = \sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}$, $\mathbf{A}_2 = \mathbf{G}\mathbf{v}_{\mathrm{E}}$ and $\mathbf{A}_3 = \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}$ being respectively the data component, the noise component and the AN component of the received signal for a particular decoding structure $\mathbf{G}$. Using the Jensen's inequality, an approximation of a lower-bound of the averaged SINR of the symbols n at the unintended position can be derived as[2]:

$$\begin{aligned}\mathbb{E}\left[\gamma_{E,n}\right] &= \mathbb{E}\left[\frac{\left|A_{1,n}\right|^2}{\left|A_{2,n}+A_{3,n}\right|^2}\right] \approx \mathbb{E}\left[\left|A_{1,n}\right|^2\right]\mathbb{E}\left[\frac{1}{\left|A_{2,n}+A_{3,n}\right|^2}\right]\\ &\gtrapprox \frac{\mathbb{E}\left[\left|A_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}+A_{3,n}\right|^2\right]} = \frac{\mathbb{E}\left[\left|A_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]+\mathbb{E}\left[\left|A_{3,n}\right|^2\right]}\end{aligned} \tag{14}$$

[2]Neglecting the covariance between $\left|A_{1,n}\right|^2$ and $\left|A_{2,n}+A_{3,n}\right|^2$, as done in the first line of (14), makes the nature of the bound, i.e., lower or upper, obtained for $\mathbb{E}\left[\gamma_{E,n}\right]$ uncertain. However, we have observed by simulations that it remains a lower one for all considered scenarios.

where $A_{1,n}$, $A_{2,n}$ and $A_{3,n}$ being respectively the data, noise and AN n^{th} symbol components of the received signal. The expression of the SINR at Eve will depend on the receiving structure $\mathbf{G}$ and we will investigate three of them.

a) Same decoding strucure as Bob: This scenario corresponds to the situation presented in Fig.1. The decoding structure at Eve is therefore $\mathbf{G} = \mathbf{S}^H$. In that case, the received sequence becomes:

$$\mathbf{y}_{\text{E}}^G = \sqrt{\alpha}\mathbf{S}^H\mathbf{H}_{\text{E}}\mathbf{H}_{\text{B}}^*\mathbf{S}\,\mathbf{x} + \sqrt{1-\alpha}\,\mathbf{S}^H\mathbf{H}_{\text{E}}\mathbf{w} + \mathbf{S}^H\mathbf{v}_{\text{E}} \quad (15)$$

We define:

$$\begin{aligned} A_{1,n} &= \sqrt{\alpha}\frac{1}{U}\sum_{i=0}^{U-1} h_{\text{E},n+iN}\; h_{\text{B},n+iN}^* \\ A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\text{E},n+iN} \\ A_{3,n} &= \sqrt{1-\alpha}\frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\text{E},n+iN}\; w_{n+iN} \end{aligned} \quad (16)$$

For the data component, we have (see A-B1a):

$$\mathbb{E}\left[|A_{1,n}|^2\right] = \frac{\alpha}{U} \quad (17)$$

For the noise component, we obtain (see A-B1b):

$$\mathbb{E}\left[|A_{2,n}|^2\right] = \sigma_{\text{V,E}}^2 \quad (18)$$

The AN term is given by (see A-B1c):

$$\mathbb{E}\left[|A_{3,n}|^2\right] = \frac{1-\alpha}{U} \quad (19)$$

From (14), (17), (18) and (19), the ergodic SINR for particular symbols n when Eve has the same capabilities as Bob is given by:

$$\mathbb{E}\left[\gamma_{E,n}\right] \gtrapprox \frac{\frac{\alpha}{U}}{\sigma_{\text{V,E}}^2 + \frac{1-\alpha}{U}} \quad (20)$$

Low performances at Eve are expected with this decoding structure since the despreading operation will not coherently add the received symbol components. No frequency diversiy will be obtained, leading to suboptimal decoding performances, and therefore to high SR values.

b) Matched filtering: The scenario is depicted in Fig.2. Eve implements a matched filtering decoding structure $\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\text{B}}\mathbf{H}_{\text{E}}^*$. The received signal is given by:

$$\mathbf{y}_{\text{E}}^G = \sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_{\text{E}}\right|^2\left|\mathbf{H}_{\text{B}}\right|^2\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_{\text{B}}\left|\mathbf{H}_{\text{E}}\right|^2\mathbf{w} + \mathbf{S}^H\mathbf{H}_E^*\mathbf{H}_B\mathbf{v}_{\text{E}} \quad (21)$$

We define:

$$\begin{aligned} A_{1,n} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\text{E},n+iN}\right|^2\left|h_{\text{B},n+iN}\right|^2 \\ A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\text{E},n+iN}^*\; h_{\text{B},n+iN}\; v_{\text{E},n+iN} \\ A_{3,n} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathbf{B},n+iN}\left|h_{\text{E},n+iN}\right|^2\; w_{n+iN} \end{aligned} \quad (22)$$

The data component can be derived as (see A-B2a):

$$\mathbb{E}\left[|A_{1,n}|^2\right] = \frac{\alpha(U+3)}{U} \quad (23)$$

The additve white noise component is determined as follow (see A-B2b):

$$\mathbb{E}\left[|A_{2,n}|^2\right] = \sigma_{\text{V,E}}^2 \quad (24)$$

The AN term is given by (see A-B2c):

$$\mathbb{E}\left[|A_{3,n}|^2\right] = \frac{1-\alpha}{U+1} \quad (25)$$

From (14), (23), (24) and (25), the ergodic SINR for particular symbols n when Eve matched filters the received sequence is given by:

$$\mathbb{E}\left[\gamma_{E,n}\right] \gtrapprox \frac{\alpha\frac{U+3}{U}}{\sigma_{\text{V,E}}^2 + \frac{1-\alpha}{U+1}} \quad (26)$$

c) Own channel knowledge: This situation is shown in Fig.3. Eve will decode the data thanks to $\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\text{E}}^*$. The received sequence is:

$$\mathbf{y}_{\text{E}}^G = \sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_{\text{E}}\right|^2\mathbf{H}_{\text{B}}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\text{E}}\right|^2\mathbf{w} + \mathbf{S}^H\mathbf{H}_E^*\mathbf{v}_{\text{E}} \quad (27)$$

We define:

$$\begin{aligned} A_{1,n} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\text{E},n+iN}\right|^2 h_{\text{B},n+iN}^* \\ A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\text{E},n+iN}^* v_{\text{E},n+iN} \\ A_{3,n} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1}\left|h_{\text{E},n+iN}\right|^2 w_{n+iN} \end{aligned} \quad (28)$$

The first term is determined as, see A-B3a:

$$\mathbb{E}\left[|A_{1,n}|^2\right] = \frac{2\alpha}{U} \quad (29)$$

The AWGN term is derived as follow, see A-B3b:

$$\mathbb{E}\left[|A_{2,n}|^2\right] = \sigma_{\text{V,E}}^2 \quad (30)$$

Finally, the AN term is given by, see A-B3c:

$$\mathbb{E}\left[|A_{3,n}|^2\right] = \frac{2(1-\alpha)}{U} \quad (31)$$

From (14), (29), (30) and (31), the ergodic SINR for particular symbols n when Eve knows her own channel is given by:

$$\mathbb{E}\left[\gamma_{E,n}\right] \gtrapprox \frac{\frac{\alpha}{U}}{\frac{\sigma_{\text{V,E}}^2}{2} + \frac{1-\alpha}{U}} \quad (32)$$

One can observe that (32) is very similar to (20) such that high SR values are expected. In particular, (32) leads to slightly higher SINR values at Eve than (20), i.e., slightly lower SR values, especially at high $\sigma_{\text{V,E}}^2$ and high α.

C. Optimal amount of data energy to inject

For each handshake scenario, we derived a closed form approximation of the SINR for the transmitted symbols n at Bob and Eve positions, respectively given by (20), (26) and (32). We can then obtain the analytic expressions of the SR thanks to (9). These expressions can finally be optimized as a function of α to determine the amount of data energy to inject in the communication in order to maximize the ergodic SR.

1) Same decoding strucure as Bob: With (9), (13) and (20), the SR becomes:

$$C_s \approx \log_2\left(1+\frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}}\right)-\log_2\left(1+\frac{\frac{\alpha}{U}}{\sigma^2_{\mathrm{V,E}}+\frac{1-\alpha}{U}}\right) \tag{33}$$

If we introduce $T_1 = -(U+1)$, $T_2 = (U+1)U\sigma^2_{\mathrm{V,E}}+U+1-U\sigma^2_{\mathrm{V,B}}$ and $T_3 = U\sigma^2_{\mathrm{V,B}}(U\sigma^2_{\mathrm{V,E}}+1)$, it is easy to show that the SR is maximized for:

$$\alpha_{\mathrm{opt}} = \frac{-T_2}{2T_1} \tag{34}$$

2) Matched filtering: With (9), (13) and (26), the SR is expressed as:

$$C_s \approx \log_2\left(1+\frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}}\right)-\log_2\left(1+\frac{\alpha\frac{U+3}{U}}{\sigma^2_{\mathrm{V,E}}+\frac{1-\alpha}{U+1}}\right) \tag{35}$$

If we introduce $T_1 = U+1$, $T_2 = (U+1)^2\sigma^2_{\mathrm{V,E}}+(U+1)-U\sigma^2_{\mathrm{V,B}}$, $T_3 = U(U+1)\sigma^2_{\mathrm{V,B}}\sigma^2_{\mathrm{E}}+U\sigma^2_{\mathrm{V,B}}$, and $T_4 = (U+1)(U+3)\sigma^2_{\mathrm{V,B}}-U\sigma^2_{\mathrm{V,B}}$, the optimal amount of data energy to transmit is:

$$\alpha_{\mathrm{opt}} = \frac{\pm\sqrt{T_1^2T_3^2\ +\ T_1T_2T_3T_4\ -\ T_1T_3T_4^2}\ -\ T_1T_3}{T_1T_4} \tag{36}$$

where only the positive root is solution since $\alpha \in [0,1]$.

3) Own channel knowledge: With (9), (13) and (32), we obtain a SR expression given by:

$$C_s \approx \log_2\left(1+\frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}}\right)-\log_2\left(1+\frac{\frac{\alpha}{U}}{\frac{\sigma^2_{\mathrm{V,E}}}{2}+\frac{1-\alpha}{U}}\right) \tag{37}$$

By introducing $T_1 = -2(U+1)$, $T_2 = (U+1)(2+U\sigma^2_{\mathrm{V,E}})-2U\sigma^2_{\mathrm{V,B}}$ and $T_3 = U\sigma^2_{\mathrm{V,B}}(U\sigma^2_{\mathrm{V,E}}+2)$, we maximize the SR for:

$$\alpha_{\mathrm{opt}} = \frac{-T_2}{2T_1} \tag{38}$$

D. Required SNR at Bob for a targetted SR

With the closed-form approximations of the SR (33), (35) and (37), it is possible to determine what should be the SNR at Bob and the amount of data energy to transmit α, in order to target a given SR, for different Eve SNR and BOR values. One can study under which conditions it is possible to guarantee a desired level of secrecy using the investigated FD TR SISO schemes. We introduce x being the targetted SR in bit per channel use, $\delta_{B,1}, \delta_{B,2}$ and $\delta_{B,3}$ being respectively Bob's SNR for the first, second and third investigated handshake procedure. Remembering that $\sigma^2_{\mathrm{V,B}} = \frac{1}{U\delta_{B,i}}$, $i = 1,2,3$, we can show that:

$$\delta_{B,i} = \frac{2^x T_{i,1} - T_{i,2}}{T_{i,3}}\ i = 1,2,3 \tag{39}$$

where we define:

$$\begin{aligned}
T_{1,1} &= U\sigma^2_{\mathrm{V,E}}+1\\
T_{1,2} &= U\sigma^2_{\mathrm{V,E}}+1-\alpha\\
T_{1,3} &= \alpha(U+1)(U\sigma^2_{\mathrm{V,E}}+1-\alpha)\\
T_{2,1} &= U(U+1)\sigma^2_{\mathrm{V,E}}+\alpha(U+1)(U+3)+U(1-\alpha)\\
T_{2,2} &= U(U+1)\sigma^2_{\mathrm{V,E}}+U(1-\alpha)\\
T_{2,3} &= \alpha U(U+1)\left[(U+1)\sigma^2_{\mathrm{V,E}}+(1-\alpha)\right]\\
T_{3,1} &= U\sigma^2_{\mathrm{V,E}}+2\\
T_{3,2} &= U\sigma^2_{\mathrm{V,E}}+2-2\alpha\\
T_{3,3} &= \alpha(U+1)(U\sigma^2_{\mathrm{V,E}}+2-2\alpha)
\end{aligned} \tag{40}$$

Eq.(39) gives the required SNR at Bob to target a SR x as a function of the BOR U and the noise level at Eve $\sigma^2_{\mathrm{V,E}}$, for the three investigated decoding structures.

E. Secrecy rate optimization via waterfilling

From section III-C, the optimal amount of transmitted data energy is derived. The analytic expressions (34), (36) and (38) lead to the coefficients α_{opt} that maximize the ergodic SR of the communication depending on the investigated scenarios. In particular, we observe that α_{opt} is an unique coefficient weighting the Q components of the useful data. That is, each subcarrier will be affected by the same coefficient. However, we know that the channel capacity at one subcarrier is proportional to the subcarrier energy. Therefore, subcarriers with higher gains will contribute more to the total channel capacity than subcarriers with lower gains. We also consider throughout this paper that Alice can instantaneously estimate Bob's channel but does not have any information about Eve instantaneous CSI. From that, we can compute the instantaneous capacity at Bob but we only have access to the ergodic capacity at Eve. Therefore, we can tune the amount of transmitted data energy at each subcarrier, i.e., we can apply a different weight at each subcarrier, in such a way that we enhance the instantaneous capacity at Bob while keeping the average transmitted data energy constant. As a conclusion, at each channel realization, we determine a new set of coefficients, denoted by $\boldsymbol{\alpha}_{\mathrm{w}} = [\alpha_{\mathrm{w},0},...,\alpha_{\mathrm{w},Q-1}]^T$, that enhances the instantaneous capacity at Bob while ensuring that:

1. The total radiated energy remains constant:
$$\left|\sqrt{\alpha_{\mathrm{opt}}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}+\sqrt{1-\alpha_{\mathrm{opt}}}\mathbf{w}\right|^2 = \left|\sqrt{\boldsymbol{\alpha}_{\mathrm{w}}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}+\sqrt{1-\boldsymbol{\alpha}_{\mathrm{w}}}\odot\mathbf{w}\right|^2 \tag{41}$$
2. The energy radiated dedicated to the AN signal remains constant:
$$\left|\sqrt{1-\alpha_{\mathrm{opt}}}\mathbf{w}\right|^2 = \left|\sqrt{1-\boldsymbol{\alpha}_{\mathrm{w}}}\odot\mathbf{w}\right|^2 \tag{42}$$
3. The AN signal still lies in the null space of Bob after optimization:
$$\forall\epsilon>0\,,\ \exists\,\boldsymbol{\alpha}_{\mathrm{w}}\ :\ \left|\mathbf{S}^H\mathbf{H}_{\mathrm{B}}\sqrt{1-\boldsymbol{\alpha}_{\mathrm{w}}}\odot\mathbf{w}\right|^2<\epsilon \tag{43}$$

Since we consider that Bob and Eve channels are independent, optimizing the energy coefficients that weight each data

subcarrier to enhance the capacity at Bob will not modify the ergodic capacity at Eve. Consequently, the communication SR will increase with this waterfilling optimization procedure. However it is worth to note that this approach is computationally expensive since new weights have to be determined at each channel realization and since a FF environment is considered.

F. Performance summary

	Same decoding structure as Bob	**Matched filtering**	**Own channel knowledge**
Handshaking protocol	Bob initiates the communication. Alice sends precoded without pilot.	Bob initiates the communication. Alice sends precoded with pilot.	Alice initiates the communication. Bob ACK and Alice sends precoded data.
Decoding structure at Eve	$\mathbf{G} = \mathbf{S}^H$	$\mathbf{G} = \mathbf{S}^H \mathbf{H}_\mathrm{B} \mathbf{H}_\mathrm{E}^*$	$\mathbf{G} = \mathbf{S}^H \mathbf{H}_\mathrm{E}^*$
SR expression	Eq.(33)	Eq.(35)	Eq.(37)
Performance	High SR values since very poor decoding performance at Eve.	Low SR values since matched filtering at Eve, leading to good decoding performances.	Very similar performances than the first model. However, slightly lower SR values for high AWGN energy at Eve, and high α.

Table I
PERFORMANCE SUMMARY FOR THE THREE INVESTIGATED MODELS

IV. Simulation Results

In this section, we present some simulation results that were performed on MATLAB. A bit stream is modulated, the AN signal is generated. The transmitted signal goes through Bob and Eve Rayleigh channels. At the receiver the SINRs are computed in order to obtain the capacities and so, the secrecy rates. We consider one thousand runs and the SR is stored in a matrix at each iteration. The ergodic SR is obtained by averaging over the experiments the values contained in the matrix.

A. Model performances

Fig.5 shows the secrecy performances for the three investigated scenarios, i.e., Eve implementing a simple despreading (circle markers), Eve implementing a matched filter (square markers), and Eve knowing her own channel (diamond markers), in terms of the SR evolution as a function of α. The figure also outlines a comparaison between the simulation curves (continuous lines) and the analytic ones (dotted lines).

First, it can be seen that the analytic models given by (33), (35), and (37) approximate well the simulation curves and remain tight upper bounds for all scenarios. In addition, one can notice the importance of the AN addition to increase the SR. In fact, we observe a SR enhancement with the addition

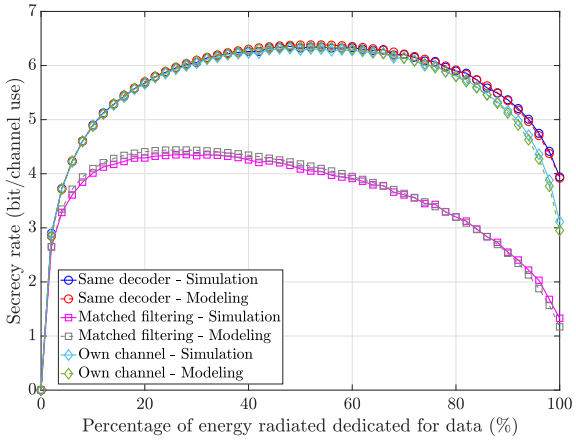

Figure 5. Models vs simulations, E_b/N_0 = 15dB at Bob, E_b/N_0 = 10dB at Eve, BOR = 4

of AN except for very high percentages of AN sent, i.e., when $\alpha \to 0$, or for very high percentages of data sent, i.e., $\alpha \to 1$. Furthermore, for all three models, no more secrecy is obtained when $\alpha \to 0$ since the SINR's at Bob and Eve drop to zero. As anticipated from sections III-B2a and III-B2c, high SR values are obtained, i.e., low decoding performances at Eve, when she has the same capabilities than Bob, and when she knows her own channel. We also observe that these two scenarios exhibit very similar behaviours except when $\alpha \to 1$, as explained in section III-B2c. Finally, we observe low SR values when Eve implements a matched filtering decoding structure. This can be understood from (21) where we notice that each transmitted data symbol will be afffected by a real gain at Eve. From that, each transmitted symbol will benefit from frequency diversity, leading to high decoding performances for the wiretap link, and so, low SR values.

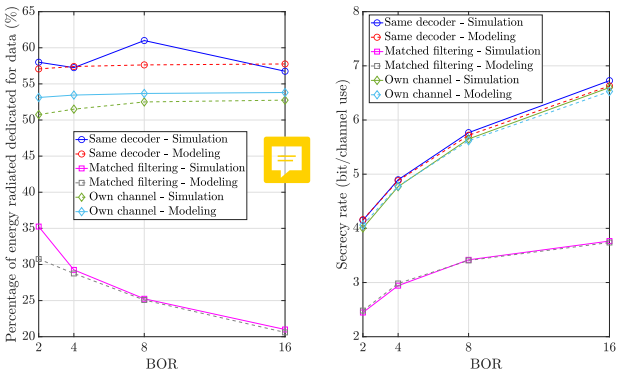

Figure 6. Optimal of AN energy to inject, E_b/N_0 = 10dB at Bob, E_b/N_0 = 5dB at Eve

The left part of Fig.6 illustrates the values of α_{opt} given by (34), (36) and (38) that maximize the ergodic SR determined from the closed-form approximations (33), (35), and (37), as well as obtained from the numerical simulations, as a function of the BOR. The analytic estimations of the optimal amount of data energy to inject are not perfect but, the resulting simulated

SR are very close to the maximal SR obtained numerically, as it can be observed on right part of Fig.6. The reason can be observed in Fig.5 where the SR curves vary very slowly about their maxima when α changes, for all models. So, for a given BOR value, Alice can make a rough determination of α_{opt} depending on Eve decoding structure, and therefore the available SR, if E_b/N_0 is known. One can also note that much lower values of α_{opt} should be injected to maximize the SR when Eve matched filters the received signal compared to the two other scenarios.

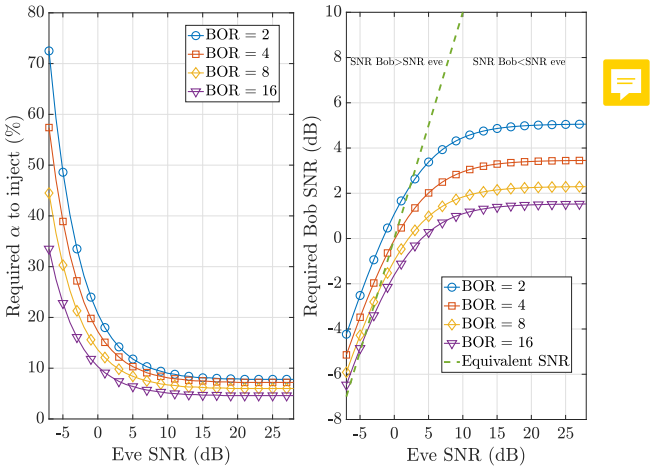

Figure 7. Targetted SR = 0 bit/channel use, matched filtering at Eve

Fig.7 illustrates the discussion from section III-D, only for the scenario where Eve implements a matched filter. A targetted SR of 0 bit per channel use was simulated in order to investigated under which conditions a positive secrecy can be ensured with the proposed FD TR SISO OFDM precoder scheme.

The left part of Fig.7 shows the required amount of data energy to inject to target the SR, as a function of Eve's SNR for different BOR values. One can observe that more AN energy must be injected when Eve SNR increases, which highlights once again the importance of the AN addition. In addition, we observe that higher values of α are needed for lower BOR values, which could have been anticipated from Fig.6

The right part of Fig.7 represents the required SNR values at Bob. First, one observes that, except for low Eve SNRs, i.e., high AWGN energies, lower SNR values at Bob than at Eve are required in order to achieve a positive SR. We see that Bob SNR curves lay in the right side of the green dotted curve as soon as Eve's SNR is higher than 3dB, for all BOR values. The green dotted curve represents the set of points where Bob and Eve SNRs are identical, i.e., where Bob and Eve channels are equivalently degraded. In particular, for high SNR values at Eve, typically higher than 15dB, we note a saturation of Bob required SNR, for all BOR values. This highlights that positive secrecy can be obtained with our FD TR SISO OFDM precoder even if Bob's channel is a degraded version of the wiretap link. Finally, higher Bob SNR values are required when the BOR decreases. This is explained by the fact that the frequency diversity gain decreases with a decrease of the BOR value. Consequently, a better channel condition is needed to target the same SR

B. Waterfilling optimization performances

ATTENTION: REFAIRE SIMU + LONGUE AU LABO

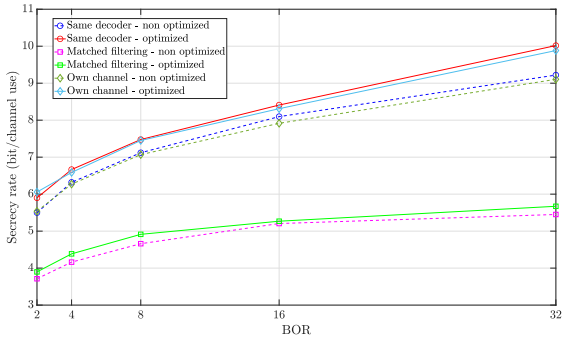

Figure 8. Waterfilling optimization, E_b/N_0 = 15dB at Bob and Eve, BOR = 4

Fig. 8 presents the maximal values of the SR for the three decoding structures, before (dotted lines) and after (continuous lines) waterfilling optimization. As a reminder, before and after optimization, the mean energy radiated dedicated to the useful data remains unchanged, and the AN signal always remains in Bob's null space. The optimal amount of data energy to inject is computed thanks to (34), (36) and (38) in order to ensure a maximal ergodic SR. The SR is then further increased via the waterfilling optimization procedure, as described in section III-E. As we can see, there is an increase of the SR for all three models and all BOR values thanks to the waterfilling.

V. Conclusions

In this paper, the problem of securing the FD TR SISO OFDM wireless transmission, in a FF environment, from a transmitter to a legitimate receiver in the presence of a passive eavesdropper is considered. A novel and original approach based on the addition of an AN signal onto OFDM blocks that improves the PLS is proposed. This approach can be easily integrated into existing standards based on OFDM. It only requires a single transmit antenna and is therefore well suited for devices with limited capabilities. Three different decoding structures for the passive eavesdropper are considered, resulting from the handshake procedure between Alice and Bob. Analytic and simulation results show that the novel approach significantly improves the security of the communication and so considerably jeopardizes any attempt of an eavesdropper to retrieve the data.

APPENDIX A
SINR DERIVATION

A. At the intended position

1) Data term:

$$\begin{aligned}
\mathbb{E}\left[|A_1|^2\right] =& \mathbb{E}\left[\left|\sqrt{\alpha}\,\mathbf{S}^H\left|\mathbf{H}_\mathrm{B}\right|^2\mathbf{S}\right|^2\right] \\
\mathbb{E}\left[|A_{1,n}|^2\right] =& \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right|^2\right] \\
=& \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right)\left(\sum_{j=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\right)^H\right] \\
=& \frac{\alpha}{U^2}\Bigg(\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^4\right] + \\
& \mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right]\mathbb{E}\left[\sum_{\substack{j=0\\ j\neq i}}^{U-1}\left|h^*_{\mathrm{B},n+jN}\right|^2\right]\Bigg) \\
=& \frac{\alpha}{U^2}\left(2U+U(U-1)\right) = \frac{\alpha(U+1)}{U}
\end{aligned} \tag{44}$$

where we used the fact that $\mathbb{E}\left[\left|h_{\mathrm{B},n+iN}\right|^2\right] = 1$ and $\mathbb{E}\left[\left|h_{\mathrm{B},n+iN}\right|^4\right] = 2$ since $\mathbf{H}_\mathrm{B} \sim \mathcal{CN}(0,1)$.

2) AWGN term:

$$\begin{aligned}
\mathbb{E}\left[|A_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{B}\right|^2\right] \\
&= \mathbb{E}\left[\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)^H\right] \\
&= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{B}\mathbf{v}_\mathrm{B}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|v_{\mathrm{B},n+iN}\right|^2\right] = \sigma^2_{\mathrm{V,B}}
\end{aligned} \tag{45}$$

B. At the unintended position

1) Same decoding structure as Bob:

a) Data term:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_1|^2\right] &= \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right|^2\right] \\
\mathbb{E}\left[|A_{1,n}|^2\right] &= \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|h^*_{\mathrm{B},n+iN}\right|^2\right] \\
&= \frac{\alpha}{U}
\end{aligned} \tag{46}$$

b) AWGN term:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{E}\right|^2\right] \\
&= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{E}\mathbf{v}_\mathrm{E}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|v_{\mathrm{E},n+iN}\right|^2\right] = \sigma^2_{\mathrm{V,E}}
\end{aligned} \tag{47}$$

c) AN term:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_3|^2\right] &= \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{w}\right|^2\right] \\
&= (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*\mathbf{w}\mathbf{w}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{3,n}|^2\right] &= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}w_{n+iN}\right|^2\right] = \frac{1-\alpha}{U}
\end{aligned} \tag{48}$$

2) Matched filtering:

a) Data term:

$$\begin{aligned}
\mathbb{E}\left[|A_{1,n}|^2\right] &= \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] \\
&= \frac{\alpha}{U^2}\mathbb{E}\Bigg[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^4\left|h_{\mathrm{E},n+iN}\right|^4 \\
&+ \sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^2\left|h^*_{\mathrm{B},n+iN}\right|^2\left|h^*_{\mathrm{E},n+jN}\right|^2\Bigg] \\
&= \frac{\alpha}{U^2}\left(U.2.2 + U(U-1)\right) = \frac{\alpha(U+3)}{U}
\end{aligned} \tag{49}$$

where we used the fact that $\mathbb{E}\left[\left|h_{\mathrm{E},n+iN}\right|^2\right] = 1$ and $\mathbb{E}\left[\left|h_{\mathrm{E},n+iN}\right|^4\right] = 2$ since $\mathbf{H}_\mathrm{E} \sim \mathcal{CN}(0,1)$.

b) AWGN term:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_\mathrm{E}^*\mathbf{H}_\mathrm{B}\mathbf{v}_\mathrm{E}\right|^2\right] \\
&= \mathbb{E}\left[\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*\mathbf{H}_\mathrm{B}\mathbf{H}_\mathrm{B}^*\mathbf{v}_\mathrm{E}\mathbf{v}_\mathrm{E}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|h_{\mathrm{B},n+iN}\right|^2\left|v_{\mathrm{E},n+iN}\right|^2\right] = \sigma^2_{\mathrm{V,E}}
\end{aligned} \tag{50}$$

c) AN term: The component $\mathbf{A}_{3,n}$ depends on $\mathbf{w}$ and $\mathbf{H}_\mathrm{B}$ which are correlated via the AN design (2). The expectation is therefore more difficult to compute. After some mathematical operations, we find: JUSQU'A QUEL POINT METTRE LES DERIVATIONS ICI ? CA PREND 3 PAGES DANS LE RAPPORT

$$\mathbb{E}\left[|A_{3,n}|^2\right] = \frac{1-\alpha}{U+1} \tag{51}$$

3) Own channel knowledge:

a) Data term:

$$\begin{aligned}
\mathbb{E}\left[|A_{1,n}|^2\right] &= \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}h^*_{\mathrm{B},n+iN}\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] \\
&= \frac{\alpha}{U^2}\mathbb{E}\Bigg[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^4 \\
&+ \sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}h_{\mathrm{B},n+jN}h^*_{\mathrm{B},n+iN}\left|h_{\mathrm{E},n+jN}\right|^2\left|h^*_{\mathrm{E},n+iN}\right|^2\Bigg] \\
&= \frac{\alpha}{U^2}\left(U.2.1 + U(U-1).1.1.0\right) = \frac{2\alpha}{U}
\end{aligned} \tag{52}$$

b) AWGN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{A}_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*\mathbf{v}_{\mathrm{E}}\right|^2\right] \\ &= \mathbb{E}\left[\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\left|\mathbf{v}_{\mathrm{E}}\right|^2\mathbf{S}\right] \\ \mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2\end{aligned} \tag{53}$$

c) AN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{A}_3|^2\right] &= \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w}\right|^2\right] \\ &= (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w}\mathbf{w}^*\left|\mathbf{H}_{\mathrm{E}}^*\right|^2\mathbf{S}\right] \\ \mathbb{E}\left[|A_{3,n}|^2\right] &= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^4|w_{n+iN}|^2\right] = \frac{2(1-\alpha)}{U}\end{aligned} \tag{54}$$

REFERENCES

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[2] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019.

[3] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

[5] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of tas/mrc with antenna correlation," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 254–259, 2012.

[6] D.-D. Tran, D.-B. Ha, V. Tran-Ha, and E.-K. Hong, "Secrecy analysis with mrc/sc-based eavesdropper over heterogeneous channels," *IETE Journal of Research*, vol. 61, no. 4, pp. 363–371, 2015.

[7] Y. Gao, S. Hu, W. Tang, Y. Li, Y. Sun, D. Huang, S. Cheng, and X. Li, "Physical layer security in 5g based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26 350–26 357, 2018.

[8] S. Golstein, T. Nguyen, F. Horlin, P. D. Doncker, and J. Sarrazin, "Physical layer security in frequency-domain time-reversal siso ofdm communication," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, 2020, pp. 222–227.

[9] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5g wireless networks," 2020.

[10] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[12] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[13] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[14] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on ofdm physical layer security," *Physical Communication*, vol. 32, pp. 1 – 30, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490718302817

[15] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[16] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[17] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[18] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, vol. 3, 2005, pp. 1906–1910.

[19] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, 2005, pp. 1501–1506 Vol. 3.

[20] ——, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[21] *Frequency Diverse Array Beamforming for Physical- Layer Security with Directionally-Aligned Legitimate User and Eavesdropper*. Zenodo, Jan. 2018. [Online]. Available: https://doi.org/10.5281/zenodo.1159254

[22] J. Lin, Q. Li, J. Yang, H. Shao, and W. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 671–684, 2018.

[23] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 9, pp. 2633–2640, 2009.

[24] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.

[25] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, 2008.

[26] ——, "A near-field modulation technique using antenna reflector switching," in *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, 2008, pp. 188–605.

[27] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect csi," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[28] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154–1170, 2015.

[29] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9747–9760, 2019.

[30] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Communications Letters*, vol. 15, no. 5, pp. 509–511, 2011.

[31] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure siso transmissions and multicasting," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1864–1874, 2013.

[32] W. Lei, M. Yang, L. Yao, and H. Lei, "Physical layer security performance analysis of the time reversal transmission system," *IET Communications*, vol. 14, no. 4, pp. 635–645, 2020.

[33] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure index and data symbol modulation for ofdm-im," *IEEE Access*, vol. 5, pp. 24 959–24 974, 2017.

[34] J. M. Hamamreh, E. Basar, and H. Arslan, "Ofdm-subcarrier index selection for enhancing security and reliability of 5g urllc services," *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[35] Q. Xu, P. Ren, Q. Du, and L. Sun, "Security-aware waveform and artificial noise design for time-reversal-based transmission," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5486–5490, 2018.

[36] S. Li, N. Li, X. Tao, Z. Liu, H. Wang, and J. Xu, "Artificial noise inserted secure communication in time-reversal systems," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[37] S. Li, N. Li, Z. Liu, H. Wang, J. Xu, and X. Tao, "Artificial noise aided path selection for secure tr communications," in *2017 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2017, pp. 1–6.

[38] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2114–2127, 2017.

[39] K. Umebayashi, F. Nakabayashi, and Y. Suzuki, "A study on secure pilot signal design for ofdm systems," in *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific*, 2014, pp. 1–5.

[40] C. Oestges, A. D. Kim, G. Papanicolaou, and A. J. Paulraj, "Characterization of space-time focusing in time-reversed random fields," *IEEE transactions on antennas and propagation*, vol. 53, no. 1, pp. 283–293, 2005.

[41] T. Dubois, M. Crussiere, and M. Helard, "On the use of time reversal for digital communications with non-impulsive waveforms," in *2010 4th International Conference on Signal Processing and Communication Systems*. IEEE, 2010, pp. 1–6.
[42] T. Nguyen, S. Monfared, J. Determe, J. Louveaux, P. De Doncker, and F. Horlin, "Performance analysis of frequency domain precoding time-reversal miso ofdm systems," *IEEE Communications Letters*, vol. 24, no. 1, pp. 48–51, 2020.
[43] S. Ahmed, T. Noguchi, and M. Kawai, "Selection of spreading codes for reduced papr in mc-cdma systems," in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1–5.
[44] H. Tran, H. Tran, G. Kaddoum, D. Tran, and D. Ha, "Effective secrecy-sinr analysis of time reversal-employed systems over correlated multi-path channel," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 527–532.