Physical Layer Security in a SISO Communication using Frequency-Domain Time-Reversal OFDM Precoding and Artificial Noise Injection

Sidney J. Golstein[*†], 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

[‡] ICTEAM, Université catholique de Louvain, 1348 Louvain-la-Neuve, Belgium

{sigolste,fhorlin,philippe.dedoncker}@ulb.ac.be

francois.rottenberg@uclouvain.be

julien.sarrazin@sorbonne-universite.fr

Abstract

A frequency domain (FD) time-reversal (TR) precoder is proposed to perform physical layer security (PLS) in single-input single-output (SISO) systems using orthogonal frequency-division multiplexing (OFDM) and artificial noise (AN) signal injection. The AN signal does not corrupt the data transmission to the legitimate receiver but degrades the decoding performance of the eavesdropper. This

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.

scheme guarantees the secrecy of a communication towards a legitimate user when the transmitter knows the instantaneous channel state information (CSI) of the legitimate link thanks to the channel reciprocity in time division duplex (TDD) systems, but does not know the instantaneous CSI of a potential eavesdropper. Three optimal decoding structures at the eavesdropper are considered in a fast fading (FF) environment depending on the handshake procedure between Alice and Bob. Closed-form approximations of the AN energy to inject in order to maximize the SR of the communication are derived. In addition, the required conditions at the legitimate receiver's end to guarantee a given SR are determined when Eve's signal-to-noise ratio (SNR) is infinite. Furthermore, a waterfilling power allocation strategy is presented to further enhance the secrecy of the scheme. Simulation results are presented to demonstrate the security performance of the proposed secure system.

Index Terms

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

I. Introduction

Internet-based services have become ubiquitous in daily life. Wireless communication has become the dominant access for most of these services but it is intrisically unsecure due to its unbounded nature. Therefore, several issues have emerged and need to be urgently adressed such as data confidentiality and integrity. The amount of leaked information is also an important feature that needs to be considered and minimized in order to guarantee secrecy of wireless transmissions, [1]–[3].

The concept of security started with Shannon's work, [4]. 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 that were secure decades ago are nowadays more subject to successful brut-force attacks. 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, [5]–[8]. PLS classically takes benefit from unpredictable wireless channel characteristics (e.g., multipath fading, noise, dispersion, diversity) to improve security of communications against potential eavesdroppers without relying on computational complexity, i.e., the security is not affected if Eve has unlimited computing capabilities, [9], [10].

The starting point of PLS was exposed in 1975 by Wyner where he 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., noisier, of the legitimate link (Bob), [11]. This work was later extended to the broadcast channel in [12], and to the Gaussian channel in [13].

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 secrecy capacity. The information-theoretic secrecy-capacity is defined as the number of bits per channel use that can be reliably transmitted from a legitimate transmitter (Alice) to a legitimate receiver (Bob) while guaranteeing a negligible information leakage to the eavesdropper, [14].

PLS can be achieved by increasing the signal-plus-interference to noise ratio (SINR) at Bob and decreasing the SINR at Eve. This can be done 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], [15], [16].

Channel-based adaptation secrecy schemes were first introduced in [17]–[19]. In these works, it was proven that positive secrecy rate (SR) can be obtained even if, on average, the channel between Alice and Bob is a degraded version of the one between Alice and Eve, by optimizing or adapting at the transmitter side the communication parameters. In doing so, the precoded signal is optimal for Bob's channel but not for Eve's one since they experience different fading. The concept of AN addition was first established in [20]–[22]. The idea is to make Eve's channel condition artificially degraded by intentionnaly adding an AN signal to the transmitter data. This AN signal is designed in such a way not to degrade Bob's channel, therefore leading to a PLS enhancement, [1].

While many works implement these schemes with multiple antennas at the transmitter, using for instance frequency diverse array beamforming [23], [24], directional modulation (DM) [25],

antenna subset modulation (ASM) [26], near-field direct antenna modulation (NFDAM) [27], [28], spatial diversity [29]–[32], or waveform design [33], only few works perfom PLS using single-input single-output (SISO) systems [9], [34]–[42]. SISO systems are indeed more suitable to resource-limited devices such as in IoT-type applications. In [34], 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, [35], [43]. 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 [44], was studied in [9], [35], limited non-optimal decoding capabilities were attributed to Eve. Another approach to provide security at the physical layer is the use of orthogonal frequency-division multiplexing (OFDM) scheme which can be implemented in time or frequency domain (FD). In [36], [37] FD OFDM schemes are presented consisting of subcarriers index selection. Only several subcarriers are used for data transmission depending on their channel gains. In [33], the information-theoretic secrecy capacity of an Offset-QAM-based filterbank multicarrier (FBMC-OQAM) communication over a wiretap frequency selective channel is studied. The authors compare the secrecy capacity of the FMBC-OQAM modulation with a cyclic prefix-orthogonal frequency-division multiplexing (CP-OFDM) modulation.

To further enhance the secrecy, few works combine TD or FD precoding with AN injection, [9], [38]–[42]. In [38]–[40], 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 [9], [41], [42], FD precoders using OFDM and AN injection are presented. In [9], the AN is injected in the null space of Bob but only limited decoding capacilities were attributed to Eve. In [41], [42], 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 paper, an original and novel FD TR precoder in SISO OFDM systems with AN addition

is introduced to secure wireless communications. Indeed, TR can be equivalently implemented in FD by replicating and shifting the signal spectrum, [45]. FD implementation has the advantage to be easily performed using OFDM. First results of this scheme were presented in [9] where limited decoding capabilities were considered at Eve. In the following, three scenarios are investigated corresponding to the amount of channel's information Eve can obtain, which in turn depends on the handshake procedure. In all the scenarios, Bob's CSI is fully known at Alice, using channel reciprocity in time division duplex (TDD) systems. An AN signal is designed in the FD in the presence of a passive eavesdropper whose instantaneous CSI is supposed unknown. The ergodic SR performance is derived with analytic models for the three investigated scenarios and compared to simulation results. It allows to determine the optimal amount of AN energy to inject in order to maximize the ergodic SR. Furthermore, it is proven that the investigated scheme can guarantee a desired SR for an infinite signal-to-noise ratio (SNR) at Eve. In addition, a power allocation technique, keeping into account the AN injection, is also derived in order to further enhance the 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, [9]. Finally, the OFDM implementation makes this approach compatible with LTE and 5G networks.

The reminder of this article is organized as follows: the communication and hanshake protocols are respectively exposed in Sections II-A and II-B. 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. The required SNR at Bob to guarantee a desired SR is derived, as a function of the communication parameters. Then, a waterfilling optimization procedure is assessed 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 the $N \times N$ 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 matrix); $\odot$ is the element-wize (hadamard) product between two vectors of same dimension; $\mathbf{0}$ and $\mathbf{1}$ are respectively all-zero and all-one column vector of the right dimension.

II. System Model

A. Communication Protocol

In order to transmit secure data between Alice and Bob, the useful data is precoded and an AN signal **w** is added before transmission, as depicted in Fig.1.

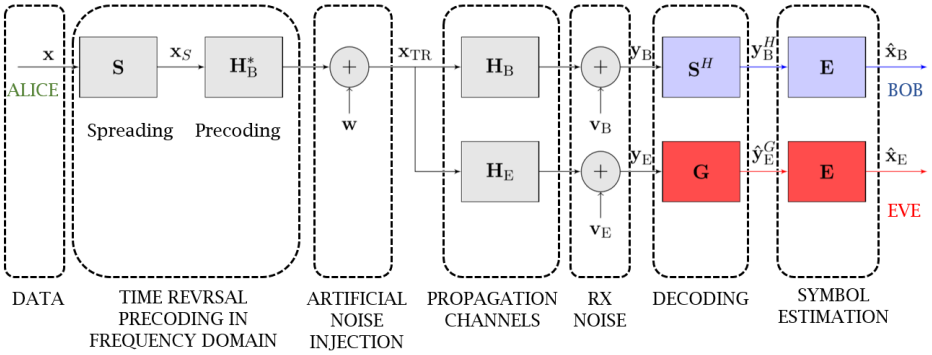

Figure 1. Communication scheme

The scheme consists in data transmission onto OFDM blocks with Q subcarriers. Without loss of generality, it is considered that only one data block $\mathbf{x}$ is sent and is composed of N symbols x_n (for $n = 0, ..., N-1$, 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 in the FD by a factor $U = Q/N$, called back-off rate (BOR), thanks to the spreading matrix $\mathbf{S}$ of size $Q \times N$. $\mathbf{S}$ is designed in such a way not to increase the PAPR, as suggested in [46].

$$\mathbf{S} = \frac{1}{\sqrt{U}} \begin{pmatrix} \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \\ & \vdots & \vdots & \\ \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \end{pmatrix} \tag{1}$$

In doing so, each data symbol is 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 corrupt the data 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. With these considerations, the transmitted sequence becomes:

$$\mathbf{x}_{\mathrm{TR}} = \sqrt{\alpha}\ \mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\ \mathbf{x} + \sqrt{1-\alpha}\ \mathbf{w} \tag{2}$$

where $\alpha \in [0,1]$ defines the ratio of the total power sent dedicated to the useful signal, while ensuring that the total transmitted power remains constant, and equals to 1 per transmitted symbol for any value of α.

The channels between Alice and Bob ($\mathbf{H}_{\mathrm{B}}$) and between Alice and Eve ($\mathbf{H}_{\mathrm{E}}$) 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. The overall channel energies are normalized to unity for each channel realization, i.e., $\mathbb{E}\left[\left|h_{\mathrm{B},q}\right|^2\right] = \mathbb{E}\left[\left|h_{\mathrm{E},q}\right|^2\right] = 1,\ q = 0,...,Q-1$. 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 $\mathbf{S}^{H}$. It is assumed that Bob and Eve know the spreading sequence. Bob then applies a zero forcing (ZF) equalization, while Eve uses the best decoding structure $\mathbf{G}$ she can, depending on the scenario, before applying a ZF equalization too, as explained in section II-B. 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:

$$\mathbf{A}\mathbf{w} = \mathbf{0} \tag{3}$$

where $\mathbf{A} = \mathbf{S}^{H}\mathbf{H}_{\mathrm{B}} \in \mathbb{C}^{N\times Q}$. Condition (3) ensures that $\mathbf{w}$ lies in the right null space of $\mathbf{A}$. A singular value decomposition (SVD) of $\mathbf{A}$ is performed, leading to:

$$\mathbf{A} = \mathbf{U}\left(\Sigma\ \mathbf{0}_{Q-N\times Q}\right)\begin{pmatrix}\mathbf{V}_1^{H}\\ \mathbf{V}_2^{H}\end{pmatrix} \tag{4}$$

where $\mathbf{U} \in \mathbb{C}^{N\times N}$ contains left singular vectors, $\Sigma \in \mathbb{C}^{N\times N}$ 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:

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{U|\mathbf{V_2}|^2}}\tilde{\mathbf{w}} \tag{5}$$

which ensures that (3) 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, it is assumed 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 (5) with a normalization factor ensuring a total energy per symbol of 1.

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

$$\mathbf{y}_{\mathrm{B}}^H = \sqrt{\alpha}\ \mathbf{S}^H\ |\mathbf{H}_{\mathrm{B}}|^2\ \mathbf{S}\mathbf{x}\ +\ \mathbf{S}^H\mathbf{v}_{\mathrm{B}} \tag{6}$$

where $\mathbf{v}_{\mathrm{B}}$ is the FD complex Additive White Gaussian Noise (AWGN) with noise's variance $\mathbb{E}\left[|v_{\mathrm{B},n}|^2\right] = \sigma^2_{\mathrm{V,B}}$ and covariance matrix $\mathbb{E}\left[(\mathbf{S}^H\mathbf{v}_{\mathrm{B}})(\mathbf{S}^H\mathbf{v}_{\mathrm{B}})^H\right] = \sigma^2_{\mathrm{V,B}}\mathbf{I}_N$. In (6), each transmitted data symbol is affected by a real gain $\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2$ at the position of the legitimate receiver. This frequency diversity gain consequently increases the received useful signal power at Bob in fading environments and increases with the BOR value. Considering a fixed bandwidth, the TR focusing effect is enhanced for higher BOR's at the expense of the data rate. It is also observed that no AN contribution is present in (6) since (3) is respected. A ZF equalization is performed at the receiver leading to:

$$\hat{\mathbf{x}}_{\mathrm{B}} = \left(\sqrt{\alpha}\mathbf{S}^H\ |\mathbf{H}_{\mathrm{B}}|^2\ \mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{S}^H\ |\mathbf{H}_{\mathrm{B}}|^2\ \mathbf{S}\mathbf{x} + \mathbf{S}^H\mathbf{v}_{\mathrm{B}}\right) = \mathbf{x} + \left(\sqrt{\alpha}\mathbf{S}^H\ |\mathbf{H}_{\mathrm{B}}|^2\ \mathbf{S}\right)^{-1}\mathbf{S}^H\mathbf{v}_{\mathrm{B}} \tag{7}$$

From (7), 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:

$$\mathbf{y}_{\mathrm{E}}^G = \sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{G}\mathbf{v}_{\mathrm{E}} \tag{8}$$

where $\mathbf{G}$ is a $N \times Q$ decoding matrix performed by Eve and $\mathbf{v}_{\mathrm{E}}$ is a complex AWGN. The nature of the decoding matrix is determined by the considered scenarios, which are presented in the next Section II-B. The noise variance is $\mathbb{E}\left[|v_{\mathrm{E,n}}|^2\right] = \sigma^2_{\mathrm{V,E}}$. The gain of the data component in (8) depends on $\mathbf{G}$ and does not necessarily provide a SNR enhancement due to a TR effect. Similarly,

the AN component does not necessarily cancel out, depending on $\mathbf{G}$. After ZF equalization, the estimated symbols are:

$$\begin{aligned}\hat{\mathbf{x}}_{\mathrm{E}} &= \left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}+\sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}+\mathbf{G}\mathbf{v}_{\mathrm{E}}\right)\\ &=\sqrt{\alpha}\mathbf{x}+\sqrt{1-\alpha}\left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}+\left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{v}_{\mathrm{E}}\end{aligned} \tag{9}$$

Equation (9) shows that the addition of AN in the FD TR SISO OFDM communication can secure the data transmission. The degree of security depends on $\mathbf{G}$ and the amount of data energy, α, that is injected into the communication, with respect to the amount of AN energy injected (via $1-\alpha$), as explained in Section III. 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.

B. Handshake Protocol and related assumptions

Prior to the secure data transmission between Alice and Bob, a handshake protocol must take place. Depending on it, Eve may obtain different degrees of information regarding the channels, which leads to different decoding capabilities and so, different security performance. PLS performance highly depends on the availability of CSI at the communication parties. It is assumed that Alice knows Bob CSI but does not know Eve CSI who is assumed to be an external passive node of the network that tries to eavesdrop the data. Furthermore, Bob and Eve CSI's are considered spatially independent.

In this paper, a Fast Fading (FF) TDD communication is considered. In doing so, three different decoding schemes are investigated at Eve depending on weither Alice or Bob first initiates the secure communication. The FF hypothesis means that each OFDM block sent by Alice experiences a different channel realization. It results in an impossibility for Eve to learn some parameters from the communication, such as the AN variance, since Bob's channel varies too rapidly and has to be frequently re-estimate by Alice.

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

If Alice only transmits precoded data to Bob, Eve is not able to know anything but $\mathbf{H}_{BE}$, the channel between Bob and Eve. In that situation, she cannot do better but to implement the same decoding structure as Bob, denoted by the abbreviation *SDS*. In that scenario, Eve only despreads the received sequence. This situation is presented in Fig.2.

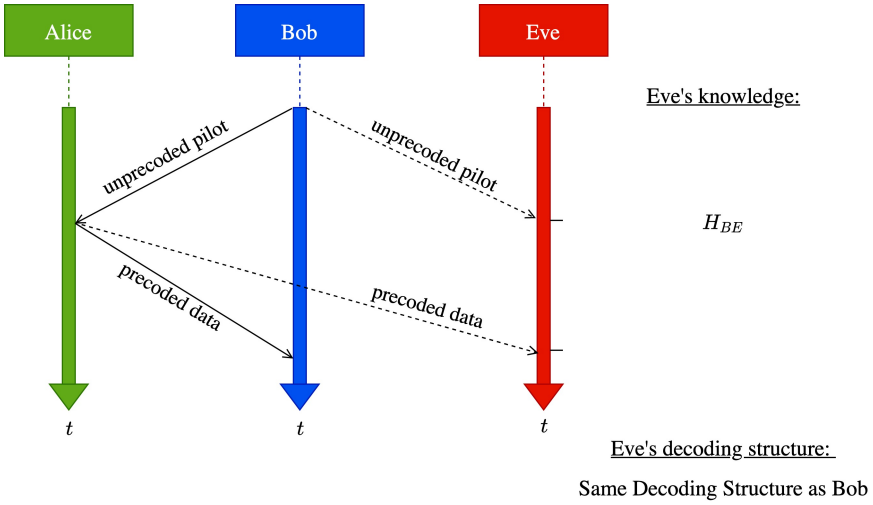

Figure 2. FF TDD, Bob initiates the communication, no pilot sent

However, if Alice sends a precoded pilot in addition to the precoded data to Bob, Eve is then able to evaluate her equivalent channel $\mathbf{H}_{\mathrm{B}}^{*}\mathbf{H}_{\mathrm{E}}$, and therefore to implement a matched filtering decoding structure, denoted by *MF*. This is depicted in Fig.3

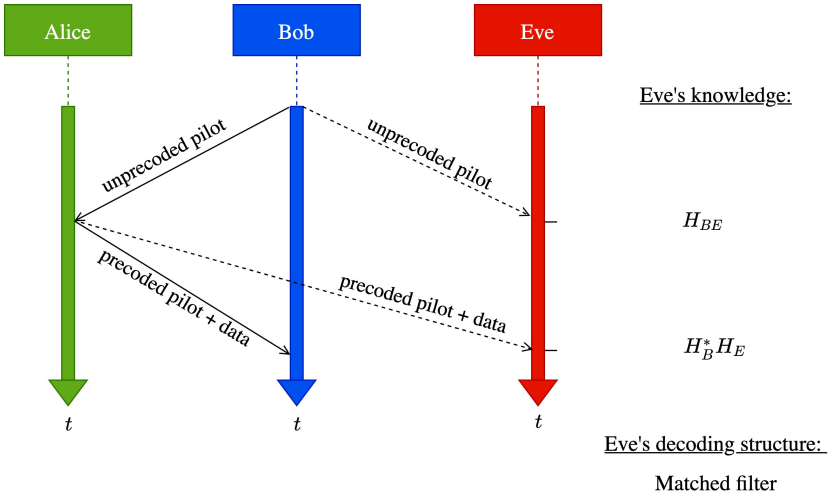

Figure 3. FF TDD, Bob initiates the communication, pilots sent

The third investigated situation arises when Alice asks first to Bob for secure commnication, as depicted in Fig.4. In this configuration, she sends a pilot to Bob allowing Eve to estimate her own channel frequency response (CFR) $\mathbf{H}_{\mathrm{E}}$. From that, Bob acknowledges to Alice without needing to send his own channel estimate $\mathbf{H}_{\mathrm{B}}$, thanks to the channel reciprocity property in

TDD systems. Here, Alice estimates $\mathbf{H}_B$ thanks to an a prirori known ACK. Finally, Alice sends precoded data without pilot to Bob. From the FF assumption, Eve cannot learn the precoding performed by the transmitter. In this configuration, Eve implements a decoding structure that takes benefit of her own channel knowledge, denoted by *OC*.

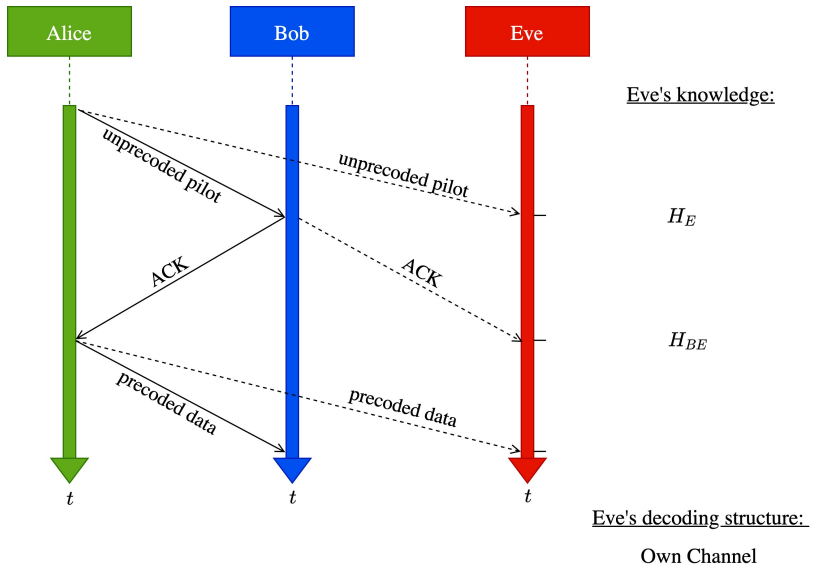

Figure 4. FF TDD, Alice initiates communication

In the following section, the three decoding schemes are studied. Analytical models of their performance are derived and discussed.

III. Performance Assessments

The classical metric used to evaluate the degree of secrecy in a communication in the PLS field is the secrecy channel capacity (SC). The SC 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, [47]. In the ergodic sense, it can be expressed as:

$$C_S = \mathbb{E}\left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]^+ \tag{10}$$

where $[x]^+ = \max(x, 0)$, γ_B and γ_E being respectively the SINR at Bob and Eve's positions. It was shown in [48], Lemma 1, that an achievable ergodic secrecy rate (SR), i.e., a positive rate smaller than or equal to the SC, is given by:

$$R_S = \left[\mathbb{E}\left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]\right]^+ \approx \left[\log_2(1+\mathbb{E}[\gamma_B]) - \log_2(1+\mathbb{E}[\gamma_E])\right]^+ \tag{11}$$

As it is observed in simulations, the bound (11) is tight, leading to an accurate approximation. To estimate the SR of the communication, the analytical expressions of Bob and Eve ergodic SINR's are derived in the following sections.

A. Hypothesis

In order to obtain the analytical models, the following assumptions are considered:

- The data and noise are independent of each other.
- $h_{B,i} \perp\!\!\!\perp h_{B,j}, \forall i \neq j$, 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.

B. SINR determination

In this section, the ergodic SINR for transmitted symbol n, $n = 0, ..., N-1$ at Bob and Eve positions are derived, depending on the investigated scenario, i.e., on the handshake procedure.

1) At the intended position: At Bob, a simple despreading operation is performed. Thanks to the precoding at the transmitter side, every received data symbol is affected by a real gain, as expressed in (6). The ergodic SINR for transmitted symbol n is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] = \mathbb{E}\left[\frac{\left|\sqrt{\alpha}B_{1,n}x_n\right|^2}{\left|B_{2,n}\right|^2}\right] = \alpha\mathbb{E}\left[\left|B_{1,n}x_n\right|^2\right]\mathbb{E}\left[\frac{1}{\left|B_{2,n}\right|^2}\right] \geq \frac{\alpha\mathbb{E}\left[\left|B_{1,n}x_n\right|^2\right]}{\mathbb{E}\left[\left|B_{2,n}\right|^2\right]} = \frac{\alpha\mathbb{E}\left[\left|B_{1,n}\right|^2\right]\mathbb{E}\left[|x_n|^2\right]}{\mathbb{E}\left[\left|B_{2,n}\right|^2\right]} \tag{12}$$

where $B_{1,n} = \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2$, x_n is the n^{th} data symbol at Bob, and $B_{2,n} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}\left|v_{\mathrm{B},n+iN}\right|$ is the n^{th} noise symbol component at Bob and where it is observed that $B_{1,n} \perp\!\!\!\perp x_n \perp\!\!\!\perp B_{2,n}$.
As detailed in A-A and A-B, the components can respectively be derived as:

$$\mathbb{E}\left[|B_{1,n}|^2\right] = \frac{\alpha(U+1)}{U} \tag{13}$$

$$\mathbb{E}\left[|B_{2,n}|^2\right] = \sigma^2_{\mathrm{V,B}} \tag{14}$$

[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.

From (12), (13) and (14), the ergodic SINR for particular symbol n at the intended position is thus given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \geq \frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}} \tag{15}$$

As a reminder, the transmitted energy per symbol is equal to 1. It has been observed in simulations than the lower-bound (15) is tight enough to be used as an approximation for 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 (8). Let's introduce $\mathbf{E}_1^G = \sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x}$, $\mathbf{E}_2^G = \mathbf{G}\mathbf{v}_{\mathrm{E}}$ and $\mathbf{E}_3^G = \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}$ being respectively the data component, the noise component, and the AN component of the received signal at Eve 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]:

$$\begin{aligned}\mathbb{E}\left[\gamma_{E,n}^G\right] &= \mathbb{E}\left[\frac{\left|E_{1,n}^G\right|^2}{\left|E_{2,n}^G + E_{3,n}^G\right|^2}\right] \approx \mathbb{E}\left[\left|E_{1,n}^G\right|^2\right]\mathbb{E}\left[\frac{1}{\left|E_{2,n}^G + E_{3,n}^G\right|^2}\right] \\ &\gtrapprox \frac{\mathbb{E}\left[\left|E_{1,n}^G\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^G + E_{3,n}^G\right|^2\right]} = \frac{\mathbb{E}\left[\left|E_{1,n}^G\right|^2\right]}{\mathbb{E}\left[\left|E_{2,n}^G\right|^2\right] + \mathbb{E}\left[\left|E_{3,n}^G\right|^2\right]}\end{aligned} \tag{16}$$

where $E_{1,n}^G$, $E_{2,n}^G$ and $E_{3,n}^G$ are respectively the data, noise and AN n^{th} symbol components of the received signal at Eve's position, for a particular decoding structure $\mathbf{G}$. The expression of the SINR at Eve depends on the receiving structure $\mathbf{G}$ whose design depends on the amount of knowledge Eve can obtain. The expression (16) is therefore derived for the three considered scenarios.

a) SDS Decoder: This scenario corresponds to the situation presented in Fig.2 where Eve can only obtain the knowledge of $\mathbf{H}_{\mathrm{BE}}$, which is of no help. The optimal decoding structure at Eve is therefore $\mathbf{G} = \mathbf{S}^H$. In that case, the received sequence becomes:

$$\mathbf{y}_{\mathrm{E}}^{SDS} = \sqrt{\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{S}^H\mathbf{v}_{\mathrm{E}} \tag{17}$$

[2]Neglecting the covariance between $\left|E_{1,n}^G\right|^2$ and $\left|E_{2,n}^G + E_{3,n}^G\right|^2$, as done in the first line of (16), makes the nature of the bound, i.e., lower or upper, obtained for $\mathbb{E}\left[\gamma_{E,n}^G\right]$ uncertain. However, it has been observed by simulations that it remains very tight and a lower one for all considered scenarios.

The symbol components can be written as:

$$\begin{aligned} E_{1,n}^{SDS} &= \sqrt{\alpha}\frac{1}{U}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN} h_{\mathrm{B},n+iN}^{*} \\ E_{2,n}^{SDS} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\mathrm{E},n+iN} \\ E_{3,n}^{SDS} &= \sqrt{1-\alpha}\frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN} w_{n+iN} \end{aligned} \tag{18}$$

As detailed in B-A1, B-A2, and B-A3, the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{SDS}|^2\right] = \frac{\alpha}{U} \tag{19}$$

$$\mathbb{E}\left[|E_{2,n}^{SDS}|^2\right] = \sigma_{\mathrm{V,E}}^2 \tag{20}$$

$$\mathbb{E}\left[|E_{3,n}^{SDS}|^2\right] = \frac{1-\alpha}{U} \tag{21}$$

From (16), (19), (20), and (21), the ergodic SINR for particular symbol n when Eve has the same capabilities as Bob is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{SDS}\right] \gtrapprox \frac{\frac{\alpha}{U}}{\sigma_{\mathrm{V,E}}^2 + \frac{1-\alpha}{U}} \tag{22}$$

Relatively low performances at Eve are expected with this decoding structure since the de-spreading operation does not coherently sum up the received symbol components. No frequency diversity gain is consequently achieved, leading to suboptimal decoding performances.

b) MF Decoder: In this scenario, depicted in Fig.3, Eve obtains the knowledge of $\mathbf{H}_{\mathrm{B}}^{*}\mathbf{H}_{\mathrm{E}}$, which allows her to implement a matched filtering decoding structure $\mathbf{G} = \mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^{*}$. The received signal is therefore given by:

$$\mathbf{y}_{\mathrm{E}}^{MF} = \sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{E}}\right|^2\left|\mathbf{H}_{\mathrm{B}}\right|^2\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w} + \mathbf{S}^{H}\mathbf{H}_{E}^{*}\mathbf{H}_{B}\mathbf{v}_{\mathrm{E}} \tag{23}$$

In this scenario, the symbol components become:

$$\begin{aligned} E_{1,n}^{MF} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|h_{\mathrm{B},n+iN}\right|^2 \\ E_{2,n}^{MF} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}^{*} h_{\mathrm{B},n+iN} v_{\mathrm{E},n+iN} \\ E_{3,n}^{MF} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{B},n+iN}\left|h_{\mathrm{E},n+iN}\right|^2 w_{n+iN} \end{aligned} \tag{24}$$

As detailed in B-B1, B-B2, and B-B3, the components can respectively be derived as:

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

$$\mathbb{E}\left[|E_{2,n}^{MF}|^2\right] = \sigma_{\mathrm{V,E}}^2 \tag{26}$$

$$\mathbb{E}\left[|E_{3,n}^{MF}|^2\right] = \frac{1-\alpha}{U+1} \tag{27}$$

From (16), (25), (26), and (27), the ergodic SINR for particular symbol n when Eve matched filters the received sequence is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{MF}\right] \gtrapprox \frac{\alpha\frac{U+3}{U}}{\sigma_{\mathrm{V,E}}^2 + \frac{1-\alpha}{U+1}} \tag{28}$$

The numerator in (28) is about U times larger than in (22) thanks to a frequency diversity gain.

c) OC Decoder: This situation is shown in Fig.4 where Eve can decode the data thanks to $\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*$. The received sequence is:

$$\mathbf{y}_{\mathrm{E}}^{OC} = \sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w} + \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*\mathbf{v}_{\mathrm{E}} \tag{29}$$

With this decoding structure, the received symbol components are defined as:

$$\begin{aligned} E_{1,n}^{OC} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2 h_{\mathrm{B},n+iN}^* \\ E_{2,n}^{OC} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}^* v_{\mathrm{E},n+iN} \\ E_{3,n}^{OC} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2 w_{n+iN} \end{aligned} \tag{30}$$

As detailed in B-C1, B-C2, and B-C3, the components can respectively be expressed as:

$$\mathbb{E}\left[|E_{1,n}^{OC}|^2\right] = \frac{2\alpha}{U} \tag{31}$$

$$\mathbb{E}\left[|E_{2,n}^{OC}|^2\right] = \sigma_{\mathrm{V,E}}^2 \tag{32}$$

$$\mathbb{E}\left[|E_{3,n}^{OC}|^2\right] = \frac{2(1-\alpha)}{U} \tag{33}$$

From (16), (31), (32), and (33), the ergodic SINR for particular symbol n when Eve knows her own channel is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{OC}\right] \gtrapprox \frac{\frac{\alpha}{U}}{\frac{\sigma_{\mathrm{V,E}}^2}{2} + \frac{1-\alpha}{U}} \tag{34}$$

One can observe that (34) is very similar to (22). In particular, (34) leads to slightly higher SINR values at Eve than (22), especially at high $\sigma_{\mathrm{V,E}}^2$ and high α.

C. Optimal amount of data energy to inject

It has to be pointed out that lower bounds of the SINR at Bob and Eve were determined for the three investigated scenarios. From simulations, the closed form approximated SINR lower bounds, derived in (15), (22), (28), and (34), are observed to be very tight and are therefore used in the remaining as an approximation. By doing so, an analytical expression of the SR can be determined using (11) as a function of α. It is therefore straightforward to determine the amount of data energy to inject in the communication, with respect to AN, in order to maximize the ergodic SR.

1) SDS Decoder: With (10), (15), and (22), the SR becomes:

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

It can be shown that the SR is maximized for:

$$\alpha_{\mathrm{opt}}^{SDS}=\frac{(U+1)(U\sigma^2_{\mathrm{V,E}}+1)-U\sigma^2_{\mathrm{V,B}}}{2(U+1)} \tag{36}$$

2) MF Decoder: With (10), (15), and (28), the SR is expressed as:

$$R_s^{MF} \approx \log_2\left(1+\frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}}\right)-\log_2\left(1+\frac{\alpha\frac{U+3}{U}}{\sigma^2_{\mathrm{V,E}}+\frac{1-\alpha}{U+1}}\right) \tag{37}$$

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

$$\alpha_{\mathrm{opt}}^{MF}=\frac{\pm\sqrt{T_1^2T_3^2\;+\;T_1T_2T_3T_4\;-\;T_1T_3T_4^2}\;-\;T_1T_3}{T_1T_4} \tag{38}$$

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

3) OC Decoder: With (10), (15) and (34), the SR expression is given by:

$$R_s^{OC} \approx \log_2\left(1+\frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}}\right)-\log_2\left(1+\frac{\frac{\alpha}{U}}{\frac{\sigma^2_{\mathrm{V,E}}}{2}+\frac{1-\alpha}{U}}\right) \tag{39}$$

Therefore, the optimal amount of data energy to inject is given by:

$$\alpha_{\mathrm{opt}}^{OC}=\frac{(U+1)(2+U\sigma^2_{\mathrm{V,E}})-2U\sigma^2_{\mathrm{V,B}}}{4(U+1)} \tag{40}$$

D. Required SNR at Bob to guarantee a desired SR

With the closed-form approximations of the SR (35), (37), and (39), it is possible to determine the SNR at Bob and the amount of data energy α that guarantees a given SR, as a function of the communication parameters. Let's introduce Δ being the targetted SR in bit per channel use, $\delta_B^{SDS}, \delta_B^{MF}$, and δ_B^{OC} being respectively Bob's required SNR for the first, second and third investigated scenario. Remembering that $\sigma^2_{\mathrm{V,B}} = \frac{1}{U\delta_B}$, the SNR can be found as:

$$\delta_B^{SDS} = \frac{2^{\Delta}(U\sigma^2_{\mathrm{V,E}} + 1) - (U\sigma^2_{\mathrm{V,E}} + 1 - \alpha)}{\alpha(U+1)(U\sigma^2_{\mathrm{V,E}} + 1 - \alpha)} \tag{41}$$

$$\delta_B^{MF} = \frac{2^{\Delta}\left[U(U+1)\sigma^2_{\mathrm{V,E}} + \alpha(U+1)(U+3) + U(1-\alpha)\right] - \left[U(U+1)\sigma^2_{\mathrm{V,E}} + U(1-\alpha)\right]}{\alpha U(U+1)\left[(U+1)\sigma^2_{\mathrm{V,E}} + (1-\alpha)\right]} \tag{42}$$

$$\delta_B^{OC} = \frac{2^{\Delta}(U\sigma^2_{\mathrm{V,E}} + 2) - (U\sigma^2_{\mathrm{V,E}} + 2 - 2\alpha)}{\alpha(U+1)(U\sigma^2_{\mathrm{V,E}} + 2 - 2\alpha)} \tag{43}$$

Equations (41), (42), and (43) give the required SNR at Bob to target SR = Δ, as a function of the BOR U and the noise level at Eve $\sigma^2_{\mathrm{V,E}}$.

To be able to guarantee SR = Δ, one has to consider Eve's SNR = ∞ in equations (41), (42), and (43) as Eve's SNR is not known to Alice.

Let's introduce δ_E as Eve's SNR. One finds $\sigma^2_{\mathrm{V,E}} = \frac{1}{U\delta_E} = 0$. Introducing $\sigma^2_{\mathrm{V,E}} = 0$ in (41), (42), and (43), and denoting $\delta_{B,\infty}^{SDS}, \delta_{B,\infty}^{MF}$, and $\delta_{B,\infty}^{OC}$ respectively as Bob's required SNR to guarantee SR = Δ for the first, second, and third investigated scenario when $\delta_E = \infty$, it comes:

$$\delta_{B,\infty}^{SDS} = \frac{\alpha + 2^{\Delta} - 1}{(-\alpha^2 + \alpha)(U+1)} \tag{44}$$

$$\delta_{B,\infty}^{MF} = \frac{\alpha\left[2^{\Delta}(U+1)(U+3) - U(2^{\Delta}-1)\right] + U(2^{\Delta}-1)}{(-\alpha^2 + \alpha)U(U+1)} \tag{45}$$

$$\delta_{B,\infty}^{OC} = \frac{\alpha + 2^{\Delta} - 1}{(-\alpha^2 + \alpha)(U+1)} = \delta_{B,\infty}^{SDS} \tag{46}$$

Equations (44), (45), and (46) are convex expressions that can be minimized as a function of α. Let's denote $\alpha_{\infty}^{SDS}, \alpha_{\infty}^{MF}$, and α_{∞}^{OC} as the amount of data energy to inject, with respect to AN, in

order to guarantee a desired communication SR when $\delta_E = \infty$, respectively for the first, second and third scenario. It can be shown that:

$$\alpha_{\infty}^{SDS} = \sqrt{(2^{\Delta}-1)^2 + (2^{\Delta}-1)} - (2^{\Delta}-1) \tag{47}$$

$$\alpha_{\infty}^{MF} = \frac{-2A_2 + \sqrt{4A_1A_2 + 4A_2^2}}{2A_1} \tag{48}$$

$$\alpha_{\infty}^{OC} = \sqrt{(2^{\Delta}-1)^2 + (2^{\Delta}-1)} - (2^{\Delta}-1) = \alpha_{\infty}^{SDS} \tag{49}$$

where $A_1 = 2^{\Delta}(U+1)(U+3) - U(2^{\Delta}-1)$, $A_2 = U(2^{\Delta}-1)$.
By replacing the values of α in (44), (45), and (46) respectively by (47), (48), and (49), the expressions of Bob's SNR to ensure SR = Δ are found.

E. Secrecy rate optimization via waterfilling

From section III-C, the optimal amount of transmitted data energy is derived thanks to eq.(36), (38), and (40). It leads to the coefficient α_{opt}^{G} that maximizes the ergodic SR of the communication depending on $\mathbf{G}$. It is a unique power coefficient weighting the Q components of the useful transmitted data. Since the channel capacity is proportionnal to the subcarrier energy, and since Alice has access only to the instantaneous channel capacity at Bob, she can tune the amount of transmitted data energy at each subcarrier, i.e., she can apply a different weight at each subcarrier, to enhance the instantaneous capacity at Bob. In doing so, at each channel realization, she determines a new set of coefficients, denoted $\boldsymbol{\alpha}_{\text{w}}^{G} = [\alpha_{\text{w},0}^{G}, ..., \alpha_{\text{w},Q-1}^{G}]^T$, that enhances the instantaneous capacity at Bob. Because Bob and Eve channels are independent, enhancing the channel capacity at Bob does not change the ergodic capacity at Eve. This power allocation strategy is described below.

If $\boldsymbol{\alpha}_{w}^{G} = [\alpha_{w,0}^{G}, ..., \alpha_{w,Q-1}^{G}]^T$ is the variable to optimize, the objective function to maximize is:

$$\underset{\alpha_w^G}{\arg\max}\, f(\boldsymbol{\alpha}_{w}^{G}) = \left| \mathbf{S}^H \mathbf{H}_{\text{B}}^{*} \sqrt{\boldsymbol{\alpha}_{w}^{G}} \mathbf{H}_{\text{B}} \mathbf{S} \right|^2 \tag{50}$$

Eq.(50) corresponds to the numerator of Bob's SINR. The constraints are:

$$0 \leq \alpha_{w,i}^{G} \leq 1, \ \forall\, i = 0, ..., Q-1 \tag{51}$$

- The received AN still lies in Bob's null space after optimization

$$\left| \mathbf{S}^H \mathbf{H}_{\text{B}}^{*} \sqrt{\mathbf{1} - \boldsymbol{\alpha}_{w}^{G}} \mathbf{w} \right|^2 - \left| \mathbf{S}^H \mathbf{H}_{\text{B}}^{*} \sqrt{\mathbf{1} - \alpha_{\text{opt}}^{G}} \mathbf{w} \right|^2 \leq \epsilon \tag{52}$$

- The total transmitted energy remains unchanged after optimization

$$\left|\sqrt{\boldsymbol{\alpha}_w^G}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x}+\sqrt{\mathbf{1}-\boldsymbol{\alpha}_w^G}\mathbf{w}\right|^2-\left|\sqrt{\alpha_{\mathrm{opt}}^G}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\mathbf{x}+\sqrt{1-\alpha_{\mathrm{opt}}^G}\mathbf{w}\right|^2\leq\epsilon \tag{53}$$

- The transmitted AN energy remains unchanged after optimization

$$\left|\sqrt{\mathbf{1}-\boldsymbol{\alpha}_w^G}\mathbf{w}\right|^2-\left|\sqrt{\mathbf{1}-\alpha_{\mathrm{opt}}^G}\mathbf{w}\right|^2\leq\epsilon \tag{54}$$

where $\epsilon = 1e^{-6}$ is the constraint tolerance. A maximum of 2500 iterations is allowed to carry out the optimization, with a step tolerance of $1e^{-6}$. The optimization is performed thanks to the interior-point algorithm.

The initial vector, depending on the investigated scenario $\mathbf{G}$, is:

$$\boldsymbol{\alpha}_w^{G,0}=\left[\alpha_{\mathrm{opt}}^G,...,\alpha_{\mathrm{opt}}^G\right]^T\in\mathbb{R}^{Q\times 1} \tag{55}$$

It is worth nothing that this approach is computationally expensive since new weights have to be determined at each channel realization because of the FF environment.

F. Performance summary

Table I summarizes the main characterstics and performances for the three investigated decoding structures at Eve:

Table I

PERFORMANCE SUMMARY FOR THE THREE INVESTIGATED MODELS

	SDS Decoder	**MF Decoder**	**OC Decoder**
Eve's knowledge	Despreading matrix: $\mathbf{S}^H$	Despreading matrix: $\mathbf{S}^H$ Equivalent channel: $\mathbf{H}_{\mathrm{B}}^*\mathbf{H}_{\mathrm{E}}$	Despreading matrix: $\mathbf{S}^H$ Own channel: $\mathbf{H}_{\mathrm{E}}$
Optimal 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.(35)	Eq.(37)	Eq.(39)
Performance	Highest SR values since very poor decoding performance at Eve.	Lowest SR values since matched filtering at Eve, leading to a frequency diversity gain. SINR about U times bigger compared to the two other models.	Very similar performances than for the SDS decoder. However, slightly lower SR values for high AWGN energy at Eve, and high α. Exact same SNR required at Bob to guarantee a desired SR than for the SDS decoder.

IV. Simulation Results

In this section, simulation results obtained with MATLAB are presented. A bit stream is QAM-modulated and the AN signal is generated. The transmitted signal goes through Bob and Eve Rayleigh-fading channels. At the receiver, the SINRs are computed in order to obtain the capacities and thus, the secrecy rates. A Monte Carlo simulation is conducted with 1000 realizations. At each iteration, the channel is updated (i.e., FF assumption) and the SR is calculated. The ergodic SR is obtained by averaging over these 1000 realizations.

A. Model performances

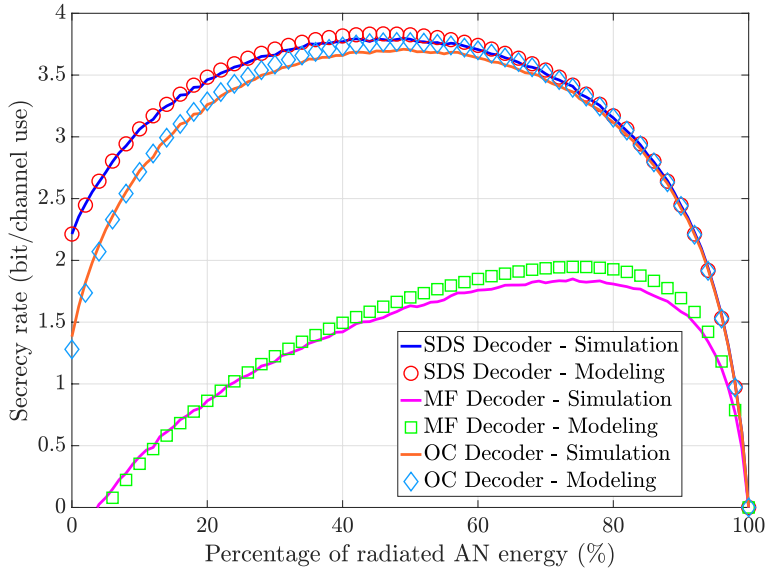

Figure 5. Models vs simulations, δ_B = 10dB, δ_E = 10dB, BOR = 4

Fig.5 shows the secrecy performances as a function of $1-\alpha$, i.e., the AN energy injected, for the three investigated scenarios: Eve implementing a simple despreading (SDS Decoder), Eve implementing a matched filter (MF Decoder), and Eve knowing her own channel (OC Decoder). Fig.5 also outlines a comparaison between the simulation curves (lines) and the analytic ones (markers).

First, it can be seen that the analytical models given by (35), (37), and (39) well approximate the simulation curves and remain tight upper bounds for all scenarios. In addition, one can notice the importance of the AN addition on the SR. In fact, one can observe a SR enhancement with

the addition of AN except for very high percentages of AN sent, i.e., when $1-\alpha \rightarrow 1$, or for very low percentages of AN sent, i.e., $1-\alpha \rightarrow 0$. Furthermore, for all three models, SR$\rightarrow 0$ when $1-\alpha \rightarrow 1$ since the SINR at Bob and Eve drops to zero. As anticipated from sections III-B2a and III-B2c, high SR values are obtained, i.e., low decoding performance at Eve, when she has the same capabilities as Bob, and when she only knows her own channel. It is also observed that these two scenarios exhibit very similar behaviours except when $1-\alpha \rightarrow 0$, as explained in section III-B2c. Finally, one can observe lower SR values when Eve implements a matched filtering decoding structure. This can be understood from (23) where it is noticed that each transmitted data symbol is afffected by a real gain at Eve such that it benefits from a frequency diversity gain, leading to higher decoding performances at Eve, and so, lower SR values. In fact, Eve SINR is about U times larger with the MF decoder compared to the SDS and the OC decoders.

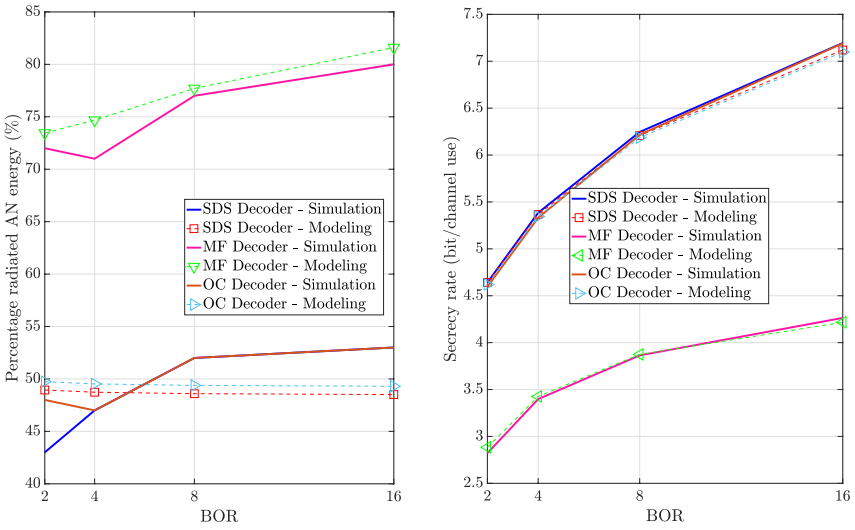

Figure 6. Optimal of AN energy to inject, δ_B = 15dB, δ_E = 15dB

The left part of Fig.6 illustrates the values of α_{opt} given by (36), (38), and (40) that maximize the ergodic SR determined from the closed-form approximations (35), (37), and (39), as well as obtained from the numerical simulations, as a function of the BOR. There is a slight discrepency between the analytical estimations of the optimal amount of data energy to inject using (36), (38), and (40), and its numerical estimation. However, the resulting analytical SR does not differ much from the maximal SR obtained in simulation, as it can be observed on the right part of Fig.6. Indeed, as observed in Fig.5, the SR is a function that varies slowly about its maximum, for all

models. So, for a given BOR value, Alice can make a rough determination of α_{opt}^{G} depending on Eve decoding structure, and therefore the available SR, if δ_B and δ_E are known. One can also note that much more AN power should be injected to maximize the SR when Eve matched filters the received signal compared to the two other scenarios.

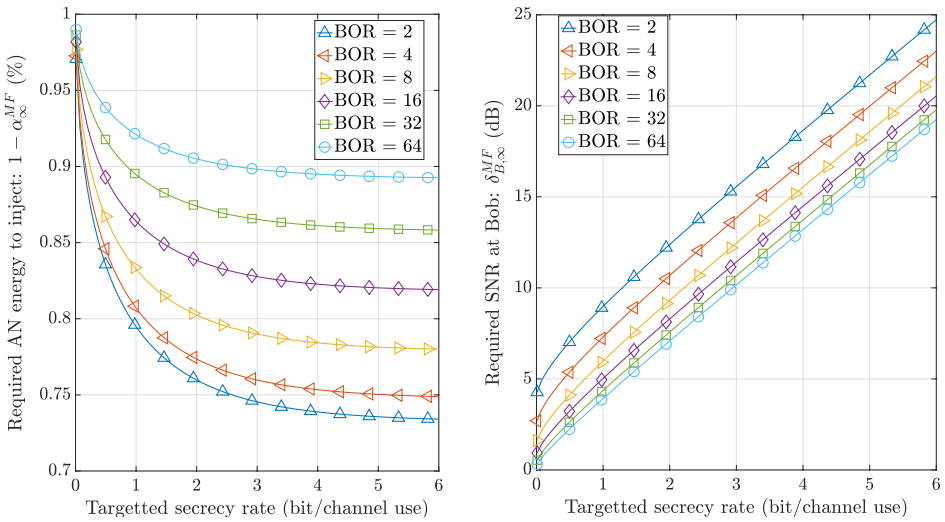

Figure 7. Guaranteeing SR, $\delta_E = \infty$

Fig.7 illustrates the discussion in section III-D, for the scenario where Eve implements a matched filter. Eve's SNR is set to $\delta_E = \infty$ such that it represents the conditions under which a desired SR is guaranteed with the proposed FD TR SISO OFDM precoder scheme.

The left part of Fig.7 shows the required amount of AN energy to inject (i.e., $1 - \alpha_{\infty}^{MF}$) for different BOR values, as a function of the targetted the SR (i.e., Δ), resulting from eq.(48). One can observe that less AN energy has to be injected when the BOR value decreases, for a fixed targetted SR. It is also worth to note that, when the targetted SR increases, the amount of AN to inject decreases.

The right part of Fig.7 represents the required SNR values at Bob, i.e., $\gamma_{B,\infty}^{MF}$ from eq.(45), when α is replaced by its expression (48). It is observed that a positive SR can always be garantueed, even for moderate SNR at Bob. In addition, one can observe that lower SNR values are required at Bob for higher BOR values since higher TR gains are obtained when the BOR increases. One can also see that the required SNR linearly increases with an increase of the targetted SR.

B. Waterfilling optimization performances

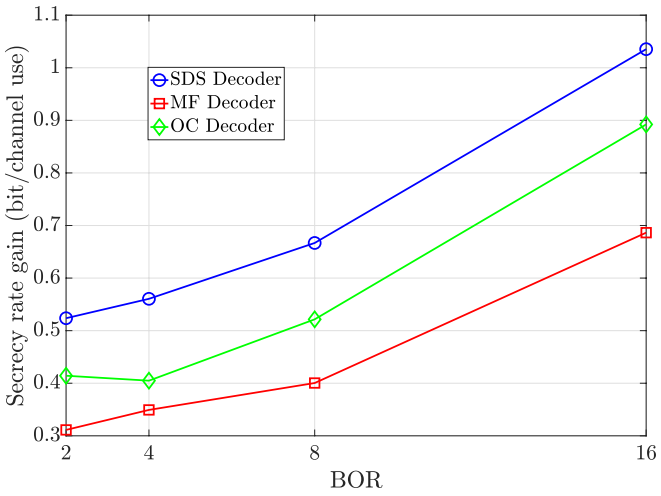

Figure 8. SR gain thanks to waterfilling optimization, δ_B = 15dB, δ_E = 15dB

Fig. 8 presents the SR enhancement thanks to the waterfilling optimization. The SR gain is defined as the difference between the maximal SR obtained after and before 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 (36), (38), and (40) 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 it can be observed, there is an increase of the SR gain for all three models and all BOR values thanks to the waterfilling.

V. Conclusions

In this paper, a new scheme is introduced in order to establish a secure communication at the physical layer between a base station, Alice, and a legitimate user, Bob, in the presence of a passive eavesdropper, Eve. Alice uses a time reversal precoder, implemented in the frequency domain with OFDM, to add to the transmitted data an artificial noise that lies in the null-space of Bob but degrade Eve's channel. The proposed technique only requires a single transmit antenna and is therefore well suited for devices with limited capabilities, such as in IoT for instance.

The ergodic secrecy rate performance is analytically derived, assuming Rayleigh channels, for three different optimal decoding structures at Eve, whose implementation depends on the

amount of CSI she can estimate, which in turn depends on the handshake procedure of the considered protocol. The obtained analytical formulations allow Alice to determine the optimal amount of artificial noise energy to inject in order to maximize the secrecy rate. The performance depends on the communication parameters but can be tuned thanks to the back-off rate factor (i.e., sampling rate to symbol rate ratio), used while implementing the time reversal precoder.

Under the assumptions of fast-fading and uncorrelated channels, it is shown that a positive secrecy rate can be guaranteed even when Eve's SNR is infinite, for moderate values of Bob's SNR. For instance, with an upsampling of 8, a secrecy rate of 0.75 and 2.2 bits/channel use is obtained with a Bob's SNR of 5 dB and 10 dB, respectively, with Eve's SNR is infinite. Furthermore, Alice can be aware of this guaranteed secrecy rate if she knows Bob's SNR. She can thus communicate while not exceeding this secrecy rate and therefore ensures the secrecy of the communication. Finally, an enhancement of this scheme is proposed via an optimal power allocation strategy over the subcarriers depending on the instantaneous CSI.

This paper shows, consequently, with analytical and simulation results, that a scheme exploiting only frequency degrees of freedom can achieve a positive ergodic secrecy rate to considerably jeopardize any attempt of an eavesdropper to retrieve the data. This approach can be easily integrated into existing standards based on OFDM and does not necessitate extra hardware. However, a perspective of this work is to extend it to multiple antenna systems to assess the benefit of the extra spatial degree of freedom.

APPENDIX A
SINR DERIVATION AT BOB

A. Data term

$$
\begin{aligned}
\mathbb{E}\left[|B_1|^2\right] =& \mathbb{E}\left[\left|\sqrt{\alpha}\ \mathbf{S}^H\,|\mathbf{H}_\mathrm{B}|^2\,\mathbf{S}\right|^2\right] \\
\mathbb{E}\left[|B_{1,n}|^2\right] =& \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right|^2\right] = \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right)\left(\sum_{j=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\right)^H\right] \\
=& \frac{\alpha}{U^2}\left(\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^4\right] + \mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right]\mathbb{E}\left[\sum_{\substack{j=0\\ j\neq i}}^{U-1}\left|h^*_{\mathrm{B},n+jN}\right|^2\right]\right) \\
=& \frac{\alpha}{U^2}\left(2U + U(U-1)\right) = \frac{\alpha(U+1)}{U}
\end{aligned}
\tag{56}
$$

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 $\mathbf{H}_\mathrm{B} \sim \mathcal{CN}(0,1)$.

B. AWGN term

$$\begin{aligned}\mathbb{E}\left[|B_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{B}\right|^2\right] = \mathbb{E}\left[\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)^H\right] = \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{B}\mathbf{v}_\mathrm{B}^*\mathbf{S}\right] \\ \mathbb{E}\left[|B_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{B},n+iN}|^2\right] = \sigma^2_{\mathrm{V,B}}\end{aligned} \tag{57}$$

Appendix B
SINR derivation at Eve

A. SDS Decoder

1) Data term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_1^{SDS}|^2\right] &= \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right|^2\right] \\ \mathbb{E}\left[|E_{1,n}^{SDS}|^2\right] &= \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|h_{\mathrm{B},n+iN}^*\right|^2\right] = \frac{\alpha}{U}\end{aligned} \tag{58}$$

2) AWGN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_2^{SDS}|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{E}\right|^2\right] = \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{E}\mathbf{v}_\mathrm{E}^*\mathbf{S}\right] \\ \mathbb{E}\left[|E_{2,n}^{SDS}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{E},n+iN}|^2\right] = \sigma^2_{\mathrm{V,E}}\end{aligned} \tag{59}$$

3) AN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_3^{SDS}|^2\right] &= \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{w}\right|^2\right] = (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*\mathbf{w}\mathbf{w}^*\mathbf{S}\right] \\ \mathbb{E}\left[|E_{3,n}^{SDS}|^2\right] &= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}w_{n+iN}|^2\right] = \frac{1-\alpha}{U}\end{aligned} \tag{60}$$

B. MF Decoder

1) Data term:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{MF}|^2\right] &= \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] = \frac{\alpha}{U^2}\mathbb{E}\Bigg[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^4\left|h_{\mathrm{E},n+iN}\right|^4 \\ &\quad + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^2\left|h_{\mathrm{B},n+iN}^*\right|^2\left|h_{\mathrm{E},n+jN}^*\right|^2\Bigg] \\ &= \frac{\alpha}{U^2}\left(U.2.2 + U(U-1)\right) = \frac{\alpha(U+3)}{U}\end{aligned} \tag{61}$$

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 $\mathbf{H}_{\mathrm{E}} \sim \mathcal{CN}(0,1)$.

2) AWGN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_2^{MF}|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*\mathbf{H}_{\mathrm{B}}\mathbf{v}_{\mathrm{E}}\right|^2\right] = \mathbb{E}\left[\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{B}}^*\mathbf{v}_{\mathrm{E}}\mathbf{v}_{\mathrm{E}}^*\mathbf{S}\right] \\ \mathbb{E}\left[|E_{2,n}^{MF}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2|h_{\mathrm{B},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2\end{aligned} \tag{62}$$

3) AN term: The component $\mathbf{A}_{3,n}$ depends on $\mathbf{w}$ and $\mathbf{H}_{\mathrm{B}}$ which are correlated via the AN design (3). The expectation is therefore not straightforward to compute. Remembering that $\mathbf{A} = \mathbf{S}^H\mathbf{H}_{\mathrm{B}}$. Omitting the $1-\alpha$ as well as the normalization factor in eq.(5), the AN term at Eve is given by:

$$\mathbf{v} = \mathbf{A}|\mathbf{H}_E|^2\mathbf{w} = \mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{w}' \tag{63}$$

Note that $\mathbf{w}'$ is independent of the other random variables and has a unit covariance matrix. Therefore, it can be shown that:

$$\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) = \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{V}_2^H|\mathbf{H}_E|^2\mathbf{V}_1\Sigma^H\mathbf{U}^H\right) \tag{64}$$

Let's rewrite $|\mathbf{H}_{\mathrm{E}}|^2 = \sum_{q=1}^{Q}|H_{E,q}|^2\mathbf{e}_q\mathbf{e}_q^T$ where $\mathbf{e}_q$ is an all zero vector except a 1 at row q:

$$\begin{aligned}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) &= \sum_{q=1}^{Q}\sum_{q'=1}^{Q}\mathbb{E}(|H_{E,q}|^2|H_{E,q'}|^2)\mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\Sigma^H\mathbf{U}^H\right) \\ &= \sum_{q=1}^{Q}\mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\Sigma^H\mathbf{U}^H\right) + \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H\mathbf{V}_2\mathbf{V}_2^H\mathbf{V}_1\Sigma^H\mathbf{U}^H\right)\end{aligned} \tag{65}$$

where the second term cancels out since $\mathbf{V}_2^H\mathbf{V}_1 = \mathbf{0}$. Since all elements of $\mathbf{v}$ have same variance, the following holds:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) = \frac{1}{N}\mathbb{E}\left(\Sigma^2\mathbf{V}_1^H\sum_{q=1}^{Q}\left(\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\right)\mathbf{V}_1\right) \tag{66}$$

Let's rewrite $\mathbf{V}_1 = \sum_l \mathbf{e}_l\mathbf{v}_{1,l}^H$ where $\mathbf{v}_{1,l}^H$ is the l-th row of $\mathbf{V}_1$ (of dimension $N\times 1$) with only one nonzero element.

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\left(\Sigma^2\mathbf{v}_{1,l}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{1,l}^H\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\Sigma^2\mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{v}_{1,q}^H\right) \tag{67}$$

Let's rewrite $\mathbf{V}_2 = \sum_l \mathbf{e}_l \mathbf{v}_{2,l}^H$ where $\mathbf{v}_{2,l}^H$ is the l-th row of $\mathbf{V}_2$ (of dimension $Q-N \times 1$) with $U-1$ nonzero elements:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\left(\Sigma^2 \mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{2,l}^H\mathbf{v}_{2,l'}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{v}_{1,q}^H\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\mathbf{v}_{1,q}^H\Sigma^2\mathbf{v}_{1,q}\right) \quad (68)$$

where $\mathbf{v}_{1,q}^H\Sigma^2\mathbf{v}_{1,q} \coloneqq \|\mathbf{v}_{1,q}\|^2\sigma_n^2$ is a scalar. Therefore:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\|\mathbf{v}_{1,q}\|^2\sigma_n^2\right) \quad (69)$$

Since $\mathbf{V}$ forms an orthonormal basis, i.e., $\mathbf{V}^H\mathbf{V} = \mathbf{I}_Q$, it is found that $\|\mathbf{v}_{1,q}\|^2 + \|\mathbf{v}_{2,q}\|^2 = 1$. Then:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left[\left(\|\mathbf{v}_{1,q}\|^2 - \|\mathbf{v}_{1,q}\|^4\right)\sigma_n^2\right] \quad (70)$$

To determine (70), the transformations performed by the SVD on $\mathbf{A}$ in order to obtain $\mathbf{v}_{1,q}$ and σ_n^2 need to be determined. One can show that:

$$\sigma_n = \sqrt{\sum_{i=1}^{U}\left|z_{(n-1)U+i}\right|^2}, n = 1...N \quad (71)$$

where $z_i = z_{i,x} + jz_{i,y} \sim \mathcal{CN}(0, \frac{1}{U})$. Therefore:

$$\mathbb{E}\left[\sigma_n^2\right] = 1 \quad (72)$$

Without loss of generality, $\mathbb{E}\left[\|v_1\|^2\right]$ and $\mathbb{E}\left[\|v_1\|^4\right]$ can be computed since all components of $\mathbf{V}_1$ are identically distributed:

$$\mathbb{E}\left[\|v_1\|^2\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^2\right] = \frac{1}{U} \quad (73)$$

For the moment of order 4, knowing that $\mathbb{E}\left[|z_i|^4\right] = \frac{2}{U^2}$:

$$\mathbb{E}\left[\|v_1\|^4\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^4\right] = \mathbb{E}\left[\frac{|z_1|^4}{\left(\sum_{i=1}^{U}|z_i|^2\right)^2}\right] = \mathbb{E}\left[\frac{|z_1|^4}{\sum_{i=1}^{U}|z_i|^4 + 2\sum_{i=1}^{U}\sum_{j<i}|z_i|^2\left|z_j\right|^2}\right] = \frac{2}{U(U+1)} \quad (74)$$

Finally, eq.(70) can be computed as:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\left[\left(\frac{1}{U} - \frac{2}{U(U+1)}\right)1\right] = \frac{U-1}{U+1} \quad (75)$$

Keeping into account the normalization factors, it follows:

$$\mathbb{E}\left[|E_{3,n}^{MF}|^2\right] = (1-\alpha)\frac{1}{U-1}\frac{U-1}{U+1} = \frac{1-\alpha}{U+1} \quad (76)$$

C. OC Decoder

1) Data term:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{OC}|^2\right] &= \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1} h_{\mathrm{B},n+iN}^{*}\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] \\ &= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^4 + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1} h_{\mathrm{B},n+jN}h_{\mathrm{B},n+iN}^{*}\left|h_{\mathrm{E},n+jN}\right|^2\left|h_{\mathrm{E},n+iN}^{*}\right|^2\right] \\ &= \frac{\alpha}{U^2}\left(U.2.1 + U(U-1).1.1.0\right) = \frac{2\alpha}{U}.\end{aligned} \tag{77}$$

2) AWGN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_2^{OC}|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_{\mathrm{E}}^{*}\mathbf{v}_{\mathrm{E}}\right|^2\right] = \mathbb{E}\left[\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\left|\mathbf{v}_{\mathrm{E}}\right|^2\mathbf{S}\right] \\ \mathbb{E}\left[|E_{2,n}^{OC}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2\end{aligned} \tag{78}$$

3) AN term:

$$\begin{aligned}\mathbb{E}\left[|\mathbf{E}_3^{OC}|^2\right] &= \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w}\right|^2\right] = (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w}\mathbf{w}^*\left|\mathbf{H}_{\mathrm{E}}^{*}\right|^2\mathbf{S}\right] \\ \mathbb{E}\left[|E_{3,n}^{OC}|^2\right] &= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^4|w_{n+iN}|^2\right] = \frac{2(1-\alpha)}{U}\end{aligned} \tag{79}$$

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] B. M. 1981, *Physical-layer security : from information theory to security engineering*. Cambridge New York Melbourne [etc: Cambridge University Press, 2011.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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

[13] 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.

[14] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[15] 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.

[16] 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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] *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

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] ——, "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.

[29] 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.

[30] 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.

[31] 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.

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

[33] F. Rottenberg, P. De Doncker, F. Horlin, and J. Louveaux, "Secrecy capacity of fbmc-oqam modulation over frequency selective channel," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1230–1234, 2020.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] D. Hu, W. Zhang, L. He, and J. Wu, "Secure transmission in multi-cell multi-user massive mimo systems with an active eavesdropper," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 85–88, 2019.