IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 1, 2022, accepted February 20, 2022, date of publication March 2, 2022, date of current version March 14, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3155594

Physical Layer Security in an OFDM Time Reversal SISO Communication With Imperfect Channel State Information

SIDNEY J. GOLSTEIN[1,2], (Student Member, IEEE), FRANÇOIS ROTTENBERG[3], (Member, IEEE), FRANÇOIS HORLIN[1], (Member, IEEE), PHILIPPE DE DONCKER[1], (Member, IEEE), AND JULIEN SARRAZIN[2], (Senior Member, IEEE)

[1]Wireless Communication Group, Université Libre de Bruxelles, 1050 Brussels, Belgium
[2]CNRS, Laboratoire de Génie Electique et Electronique de Paris, Sorbonne Université, 75252 Paris, France CentralSupélec, CNRS, Laboratoire de Génie Electrique et Electronique de Paris, Université Paris-Saclay, 91192 Gif-sur-Yvette, France
[3]KULeuven Department of Electrical Engineering (ESAT), DRAMCO, 9000 Ghent, Belgium

Corresponding author: Sidney J. Golstein (sidney.golstein@ulb.be)

This work was supported in part by the French Agence Nationale de la Recherche through the Agence nationale de la Recherche GEOcasting for HYPEr resolution spatial data focusing (ANR GEOHYPE) Project under Grant ANR-16-CE25-0003, and in part by the Framework of European Cooperation in Science and Technology (COST) Action CA20120 Intelligence-Enabling Radio Communications for Seamless Inclusive Interactions (INTERACT).

ABSTRACT A frequency domain time-reversal (TR) precoder is proposed to perform physical layer security in single-input single-output (SISO) systems using orthogonal frequency-division multiplexing (OFDM) and artificial noise (AN) injection. This scheme guarantees the secrecy of a communication towards a legitimate user, Bob, by exploiting the frequency diversity selective behaviour in multipath channels. The transmitter, Alice, has imperfect channel state information (CSI) of the legitimate link thanks to the channel reciprocity in time division duplex systems and does not know the instantaneous CSI of a potential eavesdropper, Eve. Three optimal decoding structures at Eve are considered in a block fading environment depending on the handshake procedure between Alice and Bob. Closed-form approximations of the signal-to-noise ratio required at Bob and the maximal CSI error that can be made at Alice, in order to guarantee a communication ergodic secrecy rate (ESR), are derived. Furthermore, the optimal amount of AN energy to inject, considering imperfect CSI, is also given as a closed-form expression. A trade-off on the choice of the spreading factor of the TR precoder is established between maximizing the ESR and decreasing the $\epsilon-$achievable secrecy rate. Finally, thanks to these results, Alice can be a priori aware of the ESR over which she can establish a secure communication.

INDEX TERMS Artificial noise, block-fading, eavesdropper, ergodic secrecy rate, physical layer security, $\epsilon-$achievable secrecy rate, SISO-OFDM, time division duplex, time-reversal.

I. INTRODUCTION

A. MOTIVATION

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

Cryptography-based approaches face several practical security problems. First, the eavesdropper is assumed to have limited computational complexity. With the fast development in computing power devices, secret keys that were secure decades ago are nowadays more subject to successful brut-force attacks. Second, 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 access technologies, such as 5G networks. Finally, the emergence

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

of power-limited, delay-sensitive 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 aforementioned issues, physical layer security (PLS) has emerged as an effective way to enhance security of wireless communications, [4]–[7]. PLS classically takes benefit from unpredictable wireless channel characteristics (e.g., multipath fading, noise, dispersion, diversity) to improve security of communications against potential eavesdroppers. It relies on information theory concepts. Therefore, the secrecy is theoretically ensured even if eavesdroppers have unlimited computing capabilities, [8], [9].

B. STATE OF THE ART

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, [10]. This work was later extended to the broadcast channel in [11], and to the Gaussian channel in [12].

The information-theoretic secrecy-capacity is used to quantify the degree of secrecy PLS can provide. It 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 (Eve), [13].

A non-zero secrecy capacity can be achieved by increasing the signal-to-noise-and-interference 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 space, time, and/or frequency domains, [1], [14], [15].

Channel-based adaptation secrecy schemes were first introduced in [16]–[18]. 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 can be optimized for Bob's channel but not for Eve's one since they experience different fading. The concept of AN addition was first established in [19]–[21]. The idea is to degrade Eve's channel by adding AN signal to the transmitter signal. This AN signal is designed in such a way not to degrade Bob's channel, therefore leading to positive SR, [1].

Many works implement these schemes with multiple antennas at the transmitter, using for instance frequency diverse array beamforming [22], [23], directional modulation [24], antenna subset modulation [25], near-field direct antenna modulation [26], [27], spatial diversity [28]–[31], or waveform design [32]. Only few works perform PLS using single-input single-output (SISO) systems [8], [33]–[41]. SISO systems are more suitable to resource-limited devices such as in IoT-type applications. In [33], 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, [34]. 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, [42]. 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 [43], was studied in [8], [34], limited non-optimal decoding capabilities were attributed to Eve, which led to too optimistic secrecy performance.

To further enhance the secrecy, few works combine precoding with AN injection, [8], [37]–[41], [44]. In [37]–[39], TD TR precoders are presented where 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 [44], a TD TR multi-users single-eavesdropper precoder with AN injection is presented. A convex optimization problem is solved numerically. It ensures a minimal signal power transmitted to the legitimate users under a SINR target constraint, while maximizing the amount of AN energy reaching the eavesdropper by designing the pre-filter and the AN signal. In [8], [40], [41], frequency domain (FD) precoders using OFDM and AN injection are presented. In [8], the AN is injected in the null space of Bob but only limited decoding capabilities are attributed to Eve. [40], [41] use several OFDM subcarriers for dummy data transmission. 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.

One key consideration when dealing with security is the channel state information (CSI) availability at the communication ends. Most studies generally assumed that the main channel state information is fully known at the transmitter side, which is not always the case. In real scenario, feedback can never obtain perfect CSI due to multiple reasons: asymmetric hardware's, asymmetric signal paths between UL and DL, channel estimation error introduced by devices movement.... In high mobility scenario, i.e., high Doppler spread channels, phase distortion and severe mismatches are observed with channel feedback. The channel estimation process is therefore not error-free, [28], [45]–[48]. [47], [48] particularly show that the secrecy performance of a communication system is strongly degraded when the CSI is imperfectly known because of mobility. In [28], no or partial information concerning the eavesdropper CSI is assumed and an imperfect main CSI is considered. The SINR is used as a metric and a robust approach to counter the effect of the

imperfect CSI is investigated. However, no outage constraint consideration is discussed. In [49], a secure on-off transmission scheme is adopted subject to constraints on secrecy outage probability, under quasi-static fading channel, when the eavesdropper CSI is known or partially known at the transmitter. In [50], the secrecy capacity optimization problem of fast fading channels under imperfect main channel estimation at the transmitter is studied. Alice knows the statistics of Eve's channel but does not know the rate over which she can safely communicate. In [51], authors derived the transmission probability, the connection outage probability, the secrecy outage probability (SOP), and the reliable and secure transmission probability when outdated main CSI is available. They then determined the optimal secrecy rates maximizing the secrecy throughput under dual connection and secrecy outage constraints. In [52], an optimization problem is resolved in order to maximize the secrecy throughput under SOP and reliability output probability constraints when imperfect main CSI is available.

C. CONTRIBUTIONS

In this paper, an original and novel FD TR precoder in SISO OFDM systems with AN injection by Alice is introduced to secure wireless communications in a practical way. Imperfect main channel state information is available at the transmitter side. The proposed scheme exploits only the frequency selective fading inherently present in multipath environments to achieve security thanks to the frequency diversity introduced by the TR precoder. 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]. Finally, the proposed scheme has low implementation complexity and the use of OFDM makes this approach compatible with LTE and 5G networks.

Three scenarios are investigated corresponding to the amount of channel's information Eve can obtain, which depends on the handshake procedure. In all scenarios, Bob's instantaneous CSI is imperfectly known at Alice, assuming 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 unknown. The contributions can be summarized as follows:

- It is shown that a trade-off on the spreading factor exists between maximizing the communication ergodic secrecy rate (ESR) and minimizing the amount of data leakage. To author's best knowledge, the influence of the TR spreading factor on the secrecy of the communication is assessed for the first time.
- Practical decoding structures are considered at Eve allowing Alice to guarantee an a priory known ESR without resolving any optimization problem. The decoding structures are optimal with respect to the amount of knowledge Eve can obtain.
- The maximal CSI error that Alice can perform to guarantee a given ESR is derived.
- The required SNR at Bob to target a given ESR as well as the optimal amount of AN energy to inject are derived.

Table 1 highlights the novelty of the proposed work with respect to the state of the art.

TABLE 1. Contributions of the work.

Contribution of this work	Other works
Three practical decoding structures are considered at Eve depending on the handshake procedure between Alice and Bob. Eve can use more sophisticated decoder than Bob.	In [28], it is considered that both Bob and Eve use the same decoding structure, i.e., a linear beamforming decoder. No decoding advantage is given to Eve. [49]–[52] do not consider any decoding capabilities at Eve.
Alice can guarantee the ESR over which she can safely communicate with Bob since: • A closed-form expression of the ESR is derived which is possible due to the precoding that does not necessitate an optimisation. • The worst case scenario is considered, i.e., Eve perfectly estimates her CSI, uses the best decoding structure depending on the amount of CSI she obtains, and is noiseless.	The same AWGN level at Bob and Eve is considered in [28] (which is not the worst case scenario). In [49], [51], a noisy Eve is assumed but her average SNR is assumed to be known by Alice. [50] derives bounds (no closed-form expression) of the ergodic secrecy capacity. In [52], a secrecy throughput maximization problem is numerically resolved which involves additional computational complexity. Therefore, in [50], [52], Alice cannot know the rate over which she can safely communicate.
A joint analysis between secure rate maximization and data leakage minimization is conducted.	An outage-based characterization is considered as the security performance measurement in [49]. [28], [50] only consider secure rate constraints without considering any outage constraint.

The reminder of this article is organized as follows: the communication and handshake procedures are respectively exposed in Sections II-A and II-C. Section III presents a closed-form approximation of the required SNR at Bob to guarantee a desired ESR. The maximal allowed CSI error that can be made at Alice is also derived. Finally, the expression of the optimal amount of AN energy to inject is given. 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; $(.)^{-1}$, $(.)^*$, $(.)^H$, $(.)^T$ are respectively the inverse, the complex conjugate, the Hermitian transpose, and the transpose operators; $\mathbb{E}[.]$ is the expectation operator; $|.|$ is the modulus operator (element-wize modulus if matrix); $\odot$ is the Hadamard product; $\mathbf{0}$ and $\mathbf{1}$ are respectively all-zero and all-one column vector.

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 $\mathbf{w}$ is added by Alice before transmission, as depicted in Figure 1.

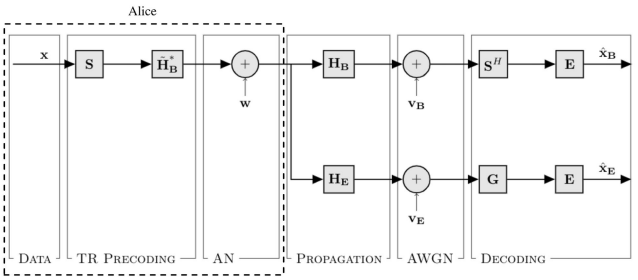

FIGURE 1. Communication scheme.

An OFDM communication scheme is considered. The number of subcarriers is denoted by Q. Without loss of generality, only one data block $\mathbf{x}$ is considered, and 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 with unit variance, i.e., $\mathbb{E}\left[|x_n|^2\right] = \sigma_x^2 = 1$. The block is then spread in the FD by a back-of-rate $U = Q/N$ thanks to a spreading matrix $\mathbf{S}$ of size $Q \times N$. $\mathbf{S}$ is the concatenation of U independent $N \times N$ diagonal matrices, whose diagonal values are randomly distributed and taken from the set $\{\pm 1\}$ in order not to increase the peak-to-average power ratio, as suggested in [53], [54].

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

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 estimation $\hat{\mathbf{H}}_B^*$, before addition of the AN signal $\mathbf{w}$ and transmission. The AN signal shares the same spectral content as the data signal and therefore does not disturb any other potential surrounding communications. $\mathbf{H}_B^*\mathbf{S}$ is the FD implementation of a TR precoder, [53]. The transmitted sequence becomes:

$$\mathbf{x}_{\text{TR}} = \sqrt{\alpha}\, \hat{\mathbf{H}}_B^* \mathbf{S}\, \mathbf{x} + \sqrt{1-\alpha}\, \mathbf{w}. \tag{2}$$

$\hat{\mathbf{H}}_B = \sqrt{1-\sigma}\mathbf{H}_B + \sqrt{\sigma}\Delta\mathbf{H}_B$ is the estimated channel at Bob, with $\mathbf{H}_B$ the channel between Alice and Bob and $\Delta\mathbf{H}_B$ the related CSI error. $\sigma \in [0, 1]$ is the estimation error variance and $\alpha \in [0, 1]$ defines the ratio between the useful and the total signal power.

The precoding matrix $\hat{\mathbf{H}}_B^*$ is a $Q \times Q$ diagonal matrix whose elements are $\hat{h}_{B,q}^*$ (for $q = 0, \ldots, Q-1$) and follow a zero mean circularly symmetric complex Gaussian (ZMC-SCG) distribution with unit variance, i.e., $\hat{h}_{B,q}^* \sim \mathcal{CN}(0, 1)$. $\mathbf{H}_B$ and the channel between Alice and Eve ($\mathbf{H}_E$) are $Q \times Q$ diagonal matrices whose elements are $h_{B,q} \sim \mathcal{CN}(0, 1)$ and $h_{E,q} \sim \mathcal{CN}(0, 1)$. The channel error matrix $\Delta\mathbf{H}_B$ is a $Q \times Q$ diagonal matrix with elements $\Delta h_{B,q} \sim \mathcal{CN}(0, 1)$. At Bob, a despreading operation is performed by applying $\mathbf{S}^H$. It is assumed that Bob and Eve know the spreading matrix. The amount of CSI Eve can estimate depends on the handshake procedure. Consequently, she uses the most suitable linear decoding structure $\mathbf{G}$, as explained in Section II-C. A perfect synchronization is finally assumed at Bob and Eve positions.

1) ARTIFICIAL NOISE DESIGN

The AN signal has to lie in Bob's null space in order not to have any impact at his position, while corrupting the received signal at Eve. To do so, Alice designs the AN signal such that:

$$\mathbf{S}^H \hat{\mathbf{H}}_B \mathbf{w} \;=\; \mathbf{0} \;\in \mathcal{C}^{N \times Q}. \tag{3}$$

However, because of the channel estimation error, $\mathbf{S}^H\mathbf{H}_B\mathbf{w} \neq \mathbf{0}$ and some of the AN energy will lie at the legitimate receiver after decoding. A singular value decomposition (SVD) is performed:

$$\mathbf{S}^H \hat{\mathbf{H}}_B = \mathbf{U} \begin{pmatrix} \Sigma & \mathbf{0}_{Q-N \times Q} \end{pmatrix} \begin{pmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{pmatrix} \tag{4}$$

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

$$\mathbf{w} = \frac{\mathbf{V}_2}{\sqrt{U|\mathbf{v}_{\mathbf{2,q}}^{\mathbf{H}}|^2}} \tilde{\mathbf{w}} \tag{5}$$

where $\mathbf{v}_{\mathbf{2,q}}^{\mathbf{H}}$ is the q-th row of $\mathbf{V}_2$ (of dimension $Q - N \times 1$) with $U - 1$ non-zero elements. Equation (5) ensures that (3) is satisfied for any arbitrary vector $\tilde{\mathbf{w}} \in \mathcal{C}^{Q-N \times 1}$. Since $Q = NU$, as soon as $U \geq 2$, there is an infinite set of solutions to generate $\tilde{\mathbf{w}}$ and therefore the AN signal. In the following, it is assumed that $\tilde{\mathbf{w}} \sim \mathcal{CN}(\mathbf{0}_{Q-N}, \mathbf{I}_{Q-N})$. 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:

$$\begin{aligned} \mathbf{y}_B^H &= \sqrt{\alpha}\mathbf{S}^H\mathbf{H}_B\hat{\mathbf{H}}_B^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_B\mathbf{w} + \mathbf{S}^H\mathbf{v}_B \\ &= \underbrace{\sqrt{\alpha(1-\sigma)}\mathbf{S}^H|\mathbf{H}_B|^2\mathbf{S}\mathbf{x} + \sqrt{\alpha\sigma}\mathbf{S}^H\mathbf{H}_B\Delta\mathbf{H}_B^*\mathbf{S}\mathbf{x}}_{\text{data}} \\ &\quad + \underbrace{\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_B\mathbf{w}}_{\text{interference}} + \underbrace{\mathbf{S}^H\mathbf{v}_B}_{\text{noise}} \end{aligned} \tag{6}$$

where $\mathbf{v}_B$ is the FD complex additive white Gaussian noise (AWGN) at Bob with noise's variance $\mathbb{E}\left[|v_{B,n}|^2\right] = \sigma_{V,B}^2$ and covariance matrix $\mathbb{E}\left[(\mathbf{S}^H\mathbf{v}_B)(\mathbf{S}^H\mathbf{v}_B)^H\right] = \sigma_{V,B}^2\mathbf{I}_N$. In (6), each transmitted data symbol is affected by a gain

$\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2+\frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},n+iN}\ \Delta h^*_{\mathrm{B},n+iN}$ at the position of the legitimate receiver. If Alice perfectly estimates Bob's CSI ($\sigma = 0$), the received useful signal power at Bob benefits from a real gain due to frequency diversity 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 in (6) that some AN leaks at Bob in case of CSI error.

3) RECEIVED SEQUENCE AT THE UNINTENDED POSITION

The received sequence at the eavesdropper position is given by:

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

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 $\mathbf{G}$ depends on the scenarios presented in the next Section II-C. The noise variance at Eve is $\mathbb{E}\left[|v_{\mathrm{E,n}}|^2\right]=\sigma^2_{\mathrm{V,E}}$. The gain of the data component in (7) depends on $\mathbf{G}$ and does not generally provide an SNR enhancement due to a TR effect. Similarly, the AN component does not generally cancel out, depending on $\mathbf{G}$. It is to be noted that, since $\mathbf{w}$ is generated from an infinite and random set of possibilities, even if Eve knows $\mathbf{H}_{\mathrm{E}}\hat{\mathbf{H}}_{\mathrm{B}}^{*}$ and $\mathbf{S}$, she cannot estimate the AN signal to try retrieving the data.

B. ASSUMPTIONS

The following assumptions are considered:

- $h_{B,i} \perp\!\!\!\perp h_{B,j}, \forall i \neq j$, 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.
- $h_{B,i} \perp\!\!\!\perp h_{E,j}, \forall i,j$, i.e., Bob and Eve are sufficiently spaced leading to no spatial correlation between them.
- $\Delta h_{B,i} \perp\!\!\!\perp h_{B,j}, \forall i,j$, i.e., no correlation between the subcarriers error made by Alice and Bob's subcarriers.
- $\Delta h_{B,i} \perp\!\!\!\perp \Delta h_{B,j}, \forall i \neq j$, i.e., no correlation between Bob's error subcarriers.

The uncorrelated frequency assumption is justify by the fact that, 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, i.e., typical urban/indoor environments in the sub-6GHz spectrum, and for sufficiently large bandwidths and moderate BOR values. In addition, 5G modulation allows for flexible numerology (e.g., subcarrier spacing) and carrier aggregation, such that resource blocks can be parametrized with flexible bandwidths and/or flexible frames. It is therefore possible to design the communication parameters, such that the BOR components of a symbol are spaced enough in frequency domain in order to experience non-correlated channels. The uncorrelated spatial assumption holds as soon as Bob and Eve are spaced by more than a few wavelengths, depending on the environment.

C. HANDSHAKE PROCEDURE

Depending on the protocol and the synchronization of the communication, different handshake procedures between Alice and Bob may be required. This in turns influences the amount of CSI Eve can estimate. In modern systems, the CSI is used to compensate for multi-paths components. PLS systems, implemented as part of a modem system, can thus access the CSI. So, depending on the available CSI, Eve can adopt different decoding strategies, which therefore leads to different security performance. It is assumed that the CSI Eve can estimate is error-free which represents the worst case scenario in terms of security. Common to all protocols, Alice learns Bob's instantaneous CSI with a certain estimation error. It is also considered that she is not aware of Eve instantaneous CSI who is considered as an external passive node of the network that tries to eavesdrop the data.

A block fading (BF) TDD communication is considered which implies that the channels remain constant over a coherence interval and are independent from one interval to another. During a coherence interval, an OFDM burst is sent by Alice that is composed of several OFDM blocks preceded or not by some pilots. Under BF assumption, two OFDM bursts experience different fading. In other words, Alice waits a coherence interval before performing a new channel estimation and sending a new OFDM burst, [13]. It results in an impossibility for Eve to learn some parameters from the communication, such as the AN variance, since Bob's channel varies between each sent burst.

Common to all procedures, Bob first sends to Alice an unprecoded pilot, which allows her to estimate Bob's channel $\hat{\mathbf{H}}_{\mathrm{B}}$. It also allows Eve to estimate $\mathbf{H}_{\mathrm{BE}}$, the channel between Bob and her. Then, depending on the structure of the OFDM burst sent by Alice, Eve may acquire different CSI knowledges.

If Alice sends an OFDM burst only composed of precoded data, Eve cannot estimate any communication parameter. In that scenario, shown in Figure 2, she can only implement the same decoding structure (SDS) as Bob. So, she despreads the received sequence using $\mathbf{G} = \mathbf{S}^H$.

If Alice sends an OFDM burst composed of a precoded pilot prior to precoded data, as shown in Figure 4, Eve is then able to perfectly evaluate her equivalent channel $\hat{\mathbf{H}}_{\mathrm{B}}^{*}\mathbf{H}_{\mathrm{E}}$. She can therefore implement a matched filtering (MF) decoding structure using $\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^{*}$.

If Alice sends an OFDM burst composed of an unprecoded pilot prior to precoded data, as shown in Figure 3, Eve is then able to perfectly evaluate her own channel $\mathbf{H}_{\mathrm{E}}$. She cannot do better but to implement a decoding structure that takes benefit of her own channel (OC) knowledge using $\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^{*}$.

A summary of the different handshake procedures is given in Table 2.

III. PERFORMANCE ASSESSMENT

To evaluate the degree of secrecy in a PLS communication, the ergodic secrecy capacity (ESC) is often considered, defined as the expectation of the secrecy capacity (SC).

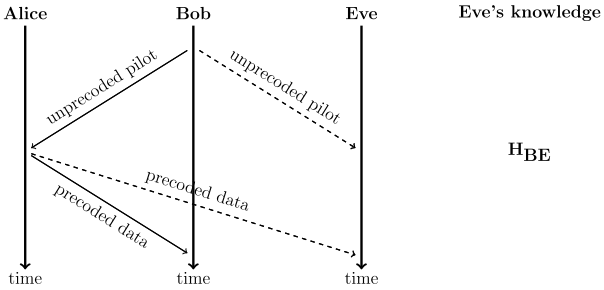

FIGURE 2. BF TDD, same decoding structure (SDS) decoder.

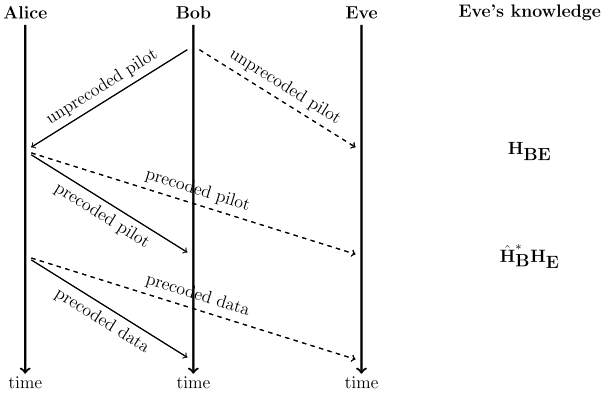

FIGURE 3. BF TDD, matched filtering (MF) decoder.

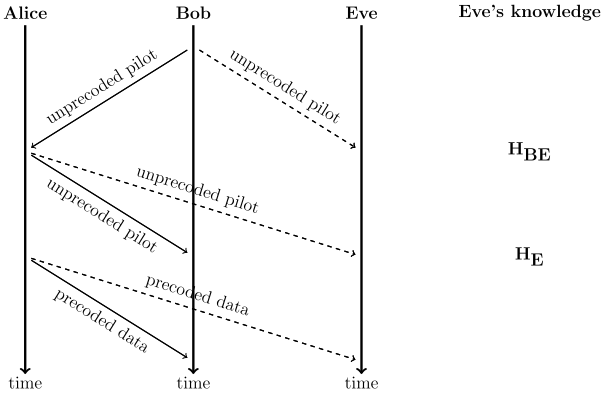

FIGURE 4. BF TDD, own channel (OC) decoder.

The SC is 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, [55]. The ESC is given by:

$$C_S = \mathbb{E}\left[\left[\log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right)\right]^+\right] \tag{8}$$

where $[x]^+ = \max(x, 0)$, γ_B and γ_E being respectively the SINR at Bob and Eve's positions. It was shown in [56], Lemma 1, that an achievable ESR, i.e., a positive rate smaller than or equal to the ESC, is given by:

$$R_S = \left[\mathbb{E}\left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]\right]^+. \tag{9}$$

TABLE 2. Handshake protocol.

Scenario	Figure 2	Figure 3	Figure 4
OFDM burst composition	Precoded data	Precoded pilot + precoded data	Unprecoded pilot + precoded data
Eve's decoder name	Same Decoding Structure (SDS) Decoder	Matched Filtering (MF) Decoder	Own Channel (OC) Decoder
Eve's decoding matrix	$\mathbf{G} = \mathbf{S}^H$	$\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^*$	$\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*$

The ESR is the considered metric in this paper. It comes:

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

Expression (10) is the ESR for the whole OFDM block. Keeping into account the spreading effect, the ESR per transmitted symbol x_n is derived by defining $\gamma_{B,n}$ (resp. $\gamma_{E,n}$) as Bob (resp. Eve) SINR for a particular transmitted symbol n:

$$R_{S,n} \approx \frac{1}{U}\left[\log_2(1+\mathbb{E}\left[\gamma_{B,n}\right]) - \log_2(1+\mathbb{E}\left[\gamma_{E,n}\right])\right]^+ \tag{11}$$

where $\frac{1}{U}$ is the rate decrease due to the spreading.

This Section III is organized as follows: In Subsection III-A, the SINR's at Bob and Eve's positions are derived to obtained a closed-form approximation of the ESR (11). Subsection III-B gives the required conditions to guarantee a communication ESR. In particular, the maximal ESR that can be guaranteed, the required SNR at Bob, the maximal CSI error that can be made, and the optimal amount of data energy to inject are derived. A summary of the different investigated scenarios is finally given in Subsection III-C.

A. SINR DETERMINATION

The ergodic SINRs in (11) for a particular transmitted symbol n at Bob and Eve's positions are derived, depending on the handshake procedure.

1) AT THE INTENDED POSITION

At Bob, a simple despreading operation is performed. An approximation of the averaged SINR of the n^{th} symbol is given by:

$$\begin{aligned}\mathbb{E}\left[\gamma_{B,n}\right] &= \mathbb{E}\left[\frac{\left|B_{1,n}\right|^2}{\left|B_{2,n}+B_{3,n}\right|^2}\right] \\ &\approx \mathbb{E}\left[\left|B_{1,n}\right|^2\right]\mathbb{E}\left[\frac{1}{\left|B_{2,n}+B_{3,n}\right|^2}\right] \\ &\approx \frac{\mathbb{E}\left[\left|B_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|B_{2,n}+B_{3,n}\right|^2\right]} = \frac{\mathbb{E}\left[\left|B_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|B_{2,n}\right|^2\right]+\mathbb{E}\left[\left|B_{3,n}\right|^2\right]}\end{aligned} \tag{12}$$

where $B_{1,n}$, $B_{2,n}$ and $B_{3,n}$ are respectively the data, noise and AN (i.e., interference) n^{th} symbol components of the received

signal at Bob's position:

$$\begin{aligned} B_{1,n} &= \frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2 \\ &\quad + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1} h_{\mathrm{B},n+iN}\,\Delta h^*_{\mathrm{B},n+iN} \\ B_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\mathrm{B},n+iN} \\ B_{3,n} &= \sqrt{\frac{1-\alpha}{U}}\sum_{i=0}^{U-1} h_{\mathrm{B},n+iN}\,w_{n+iN}. \end{aligned} \tag{13}$$

As detailed in V-A, V-B, and V-C, the components can respectively be derived as:

$$\begin{aligned} \mathbb{E}\left[|B_{1,n}|^2\right] &= \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U} \\ \mathbb{E}\left[|B_{2,n}|^2\right] &= \sigma^2_{\mathrm{V,B}} \\ \mathbb{E}\left[|B_{3,n}|^2\right] &= \frac{(1-\alpha)\sigma}{U}. \end{aligned} \tag{14}$$

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

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

2) AT THE UNINTENDED POSITION

At the unintended position, the received signal is given by (7). An approximation of the averaged SINR of the n^{th} symbol is derived as:

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

where $E^G_{1,n}$, $E^G_{2,n}$ and $E^G_{3,n}$ are respectively the data, noise and AN (i.e., interference) n^{th} symbol components of the received signal at Eve's position, for a particular decoding structure $\mathbf{G}$. The SINR at Eve depends on $\mathbf{G}$ and expression (16) is therefore derived for the three considered scenarios.

a: SDS DECODER

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

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

The symbol components can be written as:

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

As detailed in V-D1, V-D2, and V-D3, the components can respectively be expressed as:

$$\begin{aligned} \mathbb{E}\left[|E^{SDS}_{1,n}|^2\right] &= \frac{\alpha}{U} \\ \mathbb{E}\left[|E^{SDS}_{2,n}|^2\right] &= \sigma^2_{\mathrm{V,E}} \\ \mathbb{E}\left[|E^{SDS}_{3,n}|^2\right] &= \frac{1-\alpha}{U}. \end{aligned} \tag{19}$$

From (16) and (19), the ergodic SINR for a particular symbol n is given by:

$$\mathbb{E}\left[\gamma^{SDS}_{E,n}\right] \approx \frac{\alpha}{U\sigma^2_{\mathrm{V,E}}+(1-\alpha)}. \tag{20}$$

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

b: MF DECODER

In this scenario, depicted in Figure 3, Eve obtains the knowledge of $\hat{\mathbf{H}}^*_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}$, which allows her to implement a matched filtering decoding structure $\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{H}^*_{\mathrm{E}}$. Assuming that Eve makes no channel estimation error, the received signal is therefore given by:

$$\begin{aligned} \mathbf{y}^{MF}_{\mathrm{E}} &= \sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\left|\hat{\mathbf{H}}_{\mathrm{B}}\right|^2\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w} \\ &\quad + \mathbf{S}^H\mathbf{H}_{\mathrm{E}}\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{v}_{\mathrm{E}}. \end{aligned} \tag{21}$$

In this scenario, the symbol components become:

$$\begin{aligned} E^{MF}_{1,n} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|\hat{h}_{\mathrm{B},n+iN}\right|^2 \\ E^{MF}_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h^*_{\mathrm{E},n+iN}\,\hat{h}_{\mathrm{B},n+iN}\,v_{\mathrm{E},n+iN} \\ E^{MF}_{3,n} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1}\hat{h}_{\mathrm{B},n+iN}\left|h_{\mathrm{E},n+iN}\right|^2 w_{n+iN}. \end{aligned} \tag{22}$$

As detailed in V-E1, V-E2, and V-E3, the components can respectively be derived as:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{MF}|^2\right] &= \frac{\alpha(U+3)}{U}\\ \mathbb{E}\left[|E_{2,n}^{MF}|^2\right] &= \sigma_{\mathrm{V,E}}^2\\ \mathbb{E}\left[|E_{3,n}^{MF}|^2\right] &= \frac{1-\alpha}{U+1}.\end{aligned} \tag{23}$$

From (16) and (23), the ergodic SINR for a particular symbol n is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{MF}\right] \approx \frac{\alpha\frac{U+3}{U}}{\sigma_{\mathrm{V,E}}^2 + \frac{1-\alpha}{U+1}}. \tag{24}$$

The numerator in (24) is about U times larger than in (20) thanks to a frequency diversity gain.

c: OC DECODER

This situation is shown in Figure 4 where Eve knows perfectly her own channel and therefore can decode the data thanks to $\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*$. The received sequence is:

$$\mathbf{y}_{\mathrm{E}}^{OC} = \sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\hat{\mathbf{H}}_{\mathrm{B}}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w} + \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*\mathbf{v}_{\mathrm{E}}. \tag{25}$$

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

$$\begin{aligned}E_{1,n}^{OC} &= \frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\hat{h}_{\mathrm{B},n+iN}^*\\ E_{2,n}^{OC} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}h_{\mathrm{E},n+iN}^*v_{\mathrm{E},n+iN}\\ E_{3,n}^{OC} &= \frac{\sqrt{1-\alpha}}{\sqrt{U}}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2w_{n+iN}.\end{aligned} \tag{26}$$

As detailed in V-F1, V-F2, and V-F3, the components can respectively be expressed as:

$$\begin{aligned}\mathbb{E}\left[|E_{1,n}^{OC}|^2\right] &= \frac{2\alpha}{U}\\ \mathbb{E}\left[|E_{2,n}^{OC}|^2\right] &= \sigma_{\mathrm{V,E}}^2\\ \mathbb{E}\left[|E_{3,n}^{OC}|^2\right] &= \frac{2(1-\alpha)}{U}.\end{aligned} \tag{27}$$

From (16) and (27), the ergodic SINR for a particular symbol n is given by:

$$\mathbb{E}\left[\gamma_{E,n}^{OC}\right] \approx \frac{\alpha}{\frac{U\sigma_{\mathrm{V,E}}^2}{2} + (1-\alpha)}. \tag{28}$$

One can observe that (28) is very similar to (20). In particular, (28) leads to slightly higher SINR values at Eve than (20), especially at high $\sigma_{\mathrm{V,E}}^2$ and when $\alpha \to 1$.

Looking at SINR expressions (20), (24), and (28), respectively for the SINR when Eve implements an SDS, an MF, or an OC decoder, it can be seen that Eve's SINR is a decreasing function with respect to the injected AN energy. Furthermore, even in the worst case scenario where Eve is equipped with a noise-free hardware ($\sigma_{\mathrm{V,E}}^2 = 0$), Eve's SINR remains bounded when some AN is injected ($\alpha \neq 1$). On the opposite, when no AN is injected ($\alpha = 1$) and $\sigma_{\mathrm{V,E}}^2 = 0$, Eve's SINR is infinite. The AN injection therefore degrades Eve's channel condition and so, enhances the secrecy of the communication.

B. GUARANTEEING ESR

From simulations, the approximated SINRs, in (15), (20), (24), and (28), are observed to be very tight and are therefore used in the remaining to derive a closed-form expression of the per-symbol ESR (11), denoted by $R_{s,n}^G$, as a function of the communication parameters and the handshake procedure. It comes:

$$\begin{aligned}R_{s,n}^{SDS} \approx \frac{1}{U}\Bigg[&\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{U\sigma_{\mathrm{V,B}}^2+(1-\alpha)\sigma}\right)\\ &-\log_2\left(1+\frac{\alpha}{U\sigma_{\mathrm{V,E}}^2+(1-\alpha)}\right)\Bigg]\end{aligned} \tag{29}$$

$$\begin{aligned}R_{s,n}^{MF} \approx \frac{1}{U}\Bigg[&\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{U\sigma_{\mathrm{V,B}}^2+(1-\alpha)\sigma}\right)\\ &-\log_2\left(1+\frac{\alpha\frac{U+3}{U}}{\sigma_{\mathrm{V,E}}^2+\frac{1-\alpha}{U+1}}\right)\Bigg]\end{aligned} \tag{30}$$

$$\begin{aligned}R_{s,n}^{OC} \approx \frac{1}{U}\Bigg[&\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{U\sigma_{\mathrm{V,B}}^2+(1-\alpha)\sigma}\right)\\ &-\log_2\left(1+\frac{\alpha}{\frac{U\sigma_{\mathrm{V,E}}^2}{2}+(1-\alpha)}\right)\Bigg].\end{aligned} \tag{31}$$

In a practical scenario, Alice needs to know the per-symbol communication ESR over which she can securely communicate with Bob, depending on his SNR $\delta_{\mathrm{B}}^{\mathrm{G}}$. To derive the required SNR at Bob $\delta_{\mathrm{B}}^{\mathrm{G}}$ that ensures a targeted ESR $= \Delta$ (in bit per channel use), the worst case scenario is considered since Alice does not know Eve's instantaneous CSI. This corresponds to the situation where Eve SNR $\to \infty$, which is obtained with $\sigma_{\mathrm{V,E}}^2 \to 0$ in (29)-(31). This may correspond to the case where Eve is close to Alice and/or her hardware is low-noise. It is also assumed that Eve implements the best decoding structure $\mathbf{G}$ she can depending on the scenario.

1) MAXIMAL ESR THAT CAN BE GUARANTEED

Prior to any communication, Alice has to know the maximal ESR she can ensure when Eve's SNR is infinite, depending on the scenario. This maximal ESR, $\Delta_{\max}^{\mathrm{G}}$, is obtained by deriving an upper bound of the guaranteed ESR expressions, i.e., with $\sigma_{\mathrm{V,B}}^2 \to 0$ in (29)-(31). It corresponds to the situation where Bob SNR$\to \infty$. It comes:

$$\begin{aligned}\Delta_{\max}^{\mathrm{SDS}} = \frac{1}{U}\Bigg[&\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{(1-\alpha)\sigma}\right)\\ &-\log_2\left(\frac{1}{1-\alpha}\right)\Bigg]\end{aligned} \tag{32}$$

$$\Delta_{\max}^{\mathrm{MF}} = \frac{1}{U}\left[\log_2\left(1+\frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right|}{(1-\alpha)\sigma}\right) - \log_2\left(1+\frac{\alpha(U+1)(U+3)}{(1-\alpha)U}\right)\right] \quad (33)$$

$$\Delta_{\max}^{\mathrm{OC}} = \Delta_{\max}^{\mathrm{SDS}}. \quad (34)$$

From (32)-(34), $\Delta_{\max}^{\mathrm{SDS}}, \Delta_{\max}^{\mathrm{MF}}, \Delta_{\max}^{\mathrm{OC}} \to \infty$ if $\sigma \to 0$, i.e., any ESR value can theoretically be guaranteed as soon as Alice perfectly estimates Bob CSI and Bob's SNR$\to \infty$.

2) REQUIRED SNR AT BOB

The SNR at Bob $\delta_{\mathrm{B}}^{\mathrm{G}} = \frac{1}{U\sigma_{\mathrm{V,B}}^2}$ that is required to guarantee a per-symbol ESR $= \Delta$ is derived. The worst case scenario in terms of security is still considered, i.e., $\sigma_{\mathrm{V,E}}^2 \to 0$.

a: SDS DECODER

From (29) and after some algebraic manipulations, it is found that:

$$\delta_{\mathrm{B}}^{\mathrm{SDS}} = 10\log_{10}\left[\frac{\alpha + T_1^{SDS}}{\alpha^2 T_2^{SDS} + \alpha T_3^{SDS} + T_4^{SDS}}\right]\Bigg|_{\Delta\leq\Delta_{\max}^{\mathrm{SDS}}} \quad (35)$$

where

$$\begin{aligned} T_1^{SDS} &= 2^{\Delta U} - 1 \\ T_2^{SDS} &= (U+1)(\sigma-1) \\ T_3^{SDS} &= (U+1)(1-\sigma) + \sigma(2^{\Delta U}-1) \\ T_4^{SDS} &= \sigma\left(1-2^{\Delta U}\right). \end{aligned}$$

b: MF DECODER

Introducing $A = U^2+3U+3$ and reordering the terms in (30), one obtains:

$$\delta_{\mathrm{B}}^{\mathrm{MF}} = 10\log_{10}\left[\frac{\alpha T_0^{MF} + T_1^{MF}}{\alpha^2 T_2^{MF} + \alpha T_3^{MF} + T_4^{MF}}\right]\Bigg|_{\Delta\leq\Delta_{\max}^{\mathrm{MF}}} \quad (36)$$

where

$$\begin{aligned} T_0^{MF} &= U + 2^{\Delta U}A \\ T_1^{MF} &= U\left(2^{\Delta U}-1\right) \\ T_2^{MF} &= 2^{\Delta U}A\sigma - U(U+1)(1-\sigma) \\ T_3^{MF} &= 2^{\Delta U}U\sigma - 2^{\Delta U}\sigma A + U(U+1)(1-\sigma) - \sigma U \\ T_4^{MF} &= \sigma U\left(1-2^{\Delta U}\right). \end{aligned}$$

c: OC DECODER

It is easy to show that the required SNR at Bob to guarantee ESR $= \Delta$ is identical to the SDS Decoder scenario:

$$\delta_{\mathrm{B}}^{\mathrm{OC}} = \delta_{\mathrm{B}}^{\mathrm{SDS}}\Big|_{\Delta\leq\Delta_{\max}^{\mathrm{OC}}}. \quad (37)$$

3) MAXIMAL ALLOWED CSI ERROR

Expressions (35)-(37) give the required SNR at Bob to guarantee a communication ESR $= \Delta$, when Eve respectively implements the SDS Decoder, the MF Decoder, and the OC Decoder, as a function of the communication parameters. For a solution to exist, the argument of the log function in (35)-(37) must be positive, which in turns imposes a maximum CSI error $\sigma_{\max}^{\mathrm{G}}$ that can be made by Alice to possibly reach the targeted ESR.

a: SDS DECODER

The denominator of (35) is a second order expression depending on α. One needs to find the roots of this expression to determine the maximal allowed CSI error that cannot be exceeded by Alice, denoted by $\sigma_{\max}^{\mathrm{SDS}}$. After some manipulations, it can be found that:

$$\sigma_{\max}^{\mathrm{SDS}} = 1 - \frac{2^{\Delta U}-1}{(U+1)+\left(2^{\Delta U}-1\right)}\Bigg|_{\Delta\leq\Delta_{\max}^{\mathrm{SDS}}}. \quad (38)$$

From (38), if the targeted per-symbol ESR $\Delta \to \infty$, Alice must perfectly estimate Bob's CSI since $\sigma_{\max}^{\mathrm{SDS}} \to 0$, as anticipated from Section III-B1.

b: MF DECODER

The only condition needed to ensure a targeted ESR is that $T_2^{MF} < 0$ in (36), leading to:

$$\sigma_{\max}^{\mathrm{MF}} = 1 - \frac{2^{\Delta U}(U^2+3U+3)}{2^{\Delta U}(U^2+3U+3)+U(U+1)}\Bigg|_{\Delta\leq\Delta_{\max}^{\mathrm{MF}}}. \quad (39)$$

Alice has to perfectly estimate Bob CSI when $\Delta \to \infty$ since $\sigma_{\max}^{\mathrm{MF}} \to 0$, as explained in Section III-B1.

c: OC DECODER

The maximal allowed CSI error that can be made at Alice in order to guarantee an ESR $= \Delta$ is identical as in the SDS Decoder scenario:

$$\sigma_{\max}^{\mathrm{OC}} = \sigma_{\max}^{\mathrm{SDS}}\Big|_{\Delta\leq\Delta_{\max}^{\mathrm{OC}}}. \quad (40)$$

It is observed that $\lim_{\Delta\to 0^+}\sigma_{\max}^{\mathrm{SDS}} = 1$ and $\lim_{\Delta\to 0^+}\sigma_{\max}^{\mathrm{OC}} = 1$. However, $\lim_{\Delta\to 0^+}\sigma_{\max}^{\mathrm{MF}} < 1$, which imposes that Alice must estimate Bob's CSI more accurately when Eve implements the MF decoder, compared to the other scenarios, in order to ensure a positive ESR.

4) OPTIMAL AMOUNT OF DATA ENERGY TO INJECT

Equations (35)-(37) are convex expressions in α. So, one can minimize these expressions to determine the optimal amount of data energy to inject. This amount minimizes the required SNR at Bob to ensure ESR $= \Delta$, depending on the CSI error σ. It also depends on the decoding structure $\mathbf{G}$, and is denoted $\alpha_{\mathrm{opt}}^{G}$.

a: SDS DECODER

By denoting

$$A_1^{SDS} = (U+1)(1-\sigma)$$
$$A_2^{SDS} = \sigma\left(2^{\Delta U}-1\right)$$
$$A_3^{SDS} = A_1^{SDS} + A_2^{SDS},$$

one can show that:

$$\alpha_{\text{opt}}^{\text{SDS}} = \left.\frac{-2A_1^{SDS}\left(2^{\Delta U}-1\right)+\sqrt{\Sigma^{SDS}}}{2A_1^{SDS}}\right|_{\sigma\leq\sigma_{\max}^{\text{SDS}},\alpha_{\text{opt}}^{\text{SDS}}\in[0,1],\Delta\leq\Delta_{\max}^{\text{SDS}}} \tag{41}$$

with $\Sigma^{SDS} = 4(A_1^{SDS})^2\left(2^{\Delta U}-1\right)^2 - 4A_1^{SDS}\left[-\left(2^{\Delta U}-1\right)A_3^{SDS} - A_2^{SDS}\right]$.

b: MF DECODER

Introducing

$$A_1^{MF} = \sigma\left[2^{\Delta U}(U^2+3U+3)+U(U+1)\right] - U(U+1)$$
$$A_2^{MF} = \sigma\left[2^{\Delta U}U - 2^{\Delta U}(U^2+3U+3) - U(U+2)\right] + U(U+1)$$
$$A_3^{MF} = U + 2^{\Delta U}(U^2+3U+3)$$
$$A_4^{MF} = U\left(1-2^{\Delta U}\right),$$

one finds:

$$\alpha_{\text{opt}}^{\text{MF}} = \left.\frac{A_1^{MF}A_4^{MF} - \sqrt{\Sigma^{MF}}}{A_1^{MF}A_3^{MF}}\right|_{\sigma\leq\sigma_{\max}^{\text{MF}},\ \alpha_{\text{opt}}^{\text{MF}}\in[0,1],\ \Delta\leq\Delta_{\max}^{\text{MF}}} \tag{42}$$

with $\Sigma^{MF} = \left(A_1^{MF}A_4^{MF}\right)^2 + A_1^{MF}A_3^{MF}A_4^{MF}\left(\sigma A_3^{MF} + A_2^{MF}\right)$.

c: OC DECODER

The optimal amount of data energy to inject when Eve implements the OC Decoder is equivalent to the SDS Decoder, i.e.:

$$\alpha_{\text{opt}}^{\text{OC}} = \alpha_{\text{opt}}^{\text{SDS}}\Big|_{\sigma\leq\sigma_{\max}^{\text{OC}},\ \alpha_{\text{opt}}^{\text{OC}}\in[0,1],\ \Delta\leq\Delta_{\max}^{\text{OC}}}. \tag{43}$$

The estimation error σ made by Alice depends on her estimator as well as her SNR. It is therefore assumed that Alice is aware of the statistic of the CSI error she performs without knowing the error realization, i.e., she can estimate the parameter σ and adapt the communication parameters accordingly.

C. SCENARIO SUMMARY

Table 3 summarizes the main characteristics of the three investigated scenarios.

TABLE 3. Summary of the three investigated scenarios.

	SDS Decoder	MF Decoder	OC Decoder
ESR expression	Eq.(29).	Eq.(30).	Eq.(31).
Impact of imperfect CSI estimation	Eq.(38). Always possible to guarantee a positive ESR	Eq.(39). Condition on σ to guarantee a positive ESR	Eq.(40). Always possible to guarantee a positive ESR
Performance	Highest ESR values since very poor decoding performance at Eve.	Lowest ESR values since matched filtering at Eve, leading to a frequency diversity gain. SINR about U times bigger compared to the two other models.	Similar performance than for SDS decoder. However, slightly lower ESR values for high AWGN energy at Eve, and when $\alpha \to 1$. Exact same SNR required at Bob to guarantee a desired ESR than for SDS decoder.

IV. SIMULATION RESULTS

In this Section, results obtained with FD Matlab simulations are presented. A bit stream is QAM-modulated to N data symbols. These are spread by a factor U to form an OFDM block of Q = NU = 256 subcarriers. The AN signal is then generated in the FD and added to the data signal. The transmitted signal propagates through Bob and Eve's Rayleigh-fading channels. At the receiver, a perfect synchronization is considered. The SINRs are computed to obtain the capacities and thus, the secrecy rates. A Monte Carlo simulation is conducted with 2000 realizations since stable statistics are empirically observed from 1000 trials onwards. At each iteration, the channel is updated (i.e., BF assumption) and the instantaneous secrecy rate (ISR) is calculated. The ESR is obtained by averaging the ISR over these 2000 realizations. Table 4 summarizes the communication parameters used for simulations.

TABLE 4. Communication parameters.

Symbol	Description	Value
α	Ratio between the useful and the total signal power.	$\alpha \in [0,1]$
σ	CSI estimation error variance in dB.	$\sigma \in \mathbb{R}^-$
ϵ	Percentage of outage.	$\epsilon \in [0,1]$
Δ	Targeted ergodic secrecy rate in bit/channel use.	$\Delta \in \mathbb{R}^+$
Q	# of OFDM subcarriers.	$Q = 256$
U	Spreading factor.	$U = 2^n$, $n \in \{2,4,8,16,32\}$
N	# of symbols per OFDM block.	$N = Q/U$

Figure 5 shows the ergodic capacities at Bob and Eve, obtained via simulation, as a function of the percentage of AN energy injected, i.e., as a function of $1-\alpha$. At Eve, the capacity is represented for the three different scenarios. It can be seen that the AN considerably degrades Eve's capacities. In addition, it is observed that injecting AN also degrades Bob's capacity, but less severely that Eve's ones. More, it is outlined that, if no AN is injected, i.e., $1-\alpha = 0$, no secrecy can be provided if Eve implements an MF decoder since her capacity is larger than Bob's one. This justifies the need for AN injection in order to obtain positive ESR. Finally, when only AN is injected, Bob's and Eve's capacities become zero, which is expected.

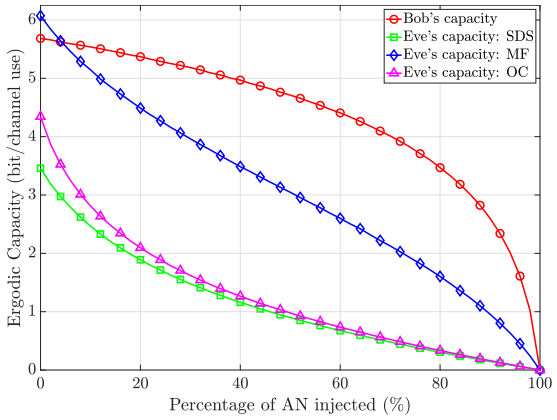

FIGURE 5. Ergodic capacity as a function of the percentage of AN injected, $\delta_B = 10$dB, $\delta_E = 10$ dB, U = 4, $\sigma = -\infty$dB.

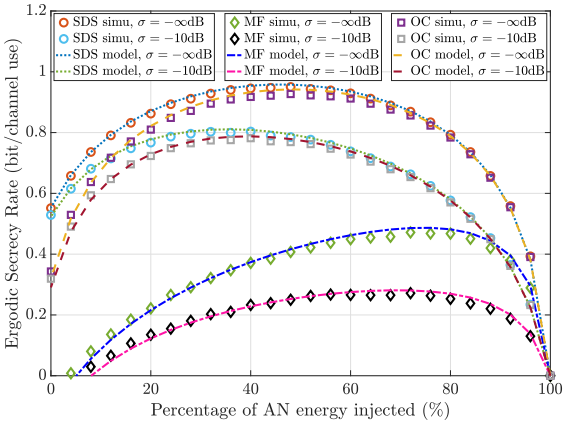

FIGURE 6. Models vs simulations, $\delta_B = 10$dB, $\delta_E = 10$ dB, U = 4.

Figure 6 shows the ESR as a function of the AN energy injected, for the three investigated scenarios. It also compares the simulation curves (markers) with the analytic ones (lines) for two different CSI errors made by Alice, $\sigma = -\infty$ dB, which corresponds to no CSI estimation error, and $\sigma = -10$ dB which corresponds to 10% of CSI estimation error.

First, it can be seen that the analytical models given by (29), (30), and (31) well approximate the simulation curves and are thus used to plot results in next figures. Second, one can notice the importance of AN on the ESR value. It is observed an ESR enhancement with the addition of AN, except for very high or very low percentages of injected AN. In particular, if Eve implements the MF decoder ($\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_\mathrm{B}\mathbf{H}_\mathrm{E}^*$), a positive ESR is only possible if more than 4% (resp. 8%) of AN energy is injected, when $\sigma = -\infty$ dB (resp. $\sigma = -10$ dB). Third, as anticipated from Subsections III-A2 and III-A2, higher ESR values are obtained when Eve implements the SDS decoder ($\mathbf{G} = \mathbf{S}^H$) or the OC decoder ($\mathbf{G} = \mathbf{S}^H\mathbf{H}_\mathrm{E}^*$) compared to the MF decoder. These two scenarios exhibit very similar behaviours except when very low percentage of AN energy is injected, as identified in Subsection III-A2. Lower ESR values are obtained with the MF decoder, which can be understood from (21) where each transmitted data symbol is affected by a frequency diversity gain at Eve. Eve's SINR is consequently about U times larger compared to the SDS and the OC decoders, leading to higher decoding performances, and so, lower ESR values. Fourth, the impact of the CSI error at Alice is considerable. With only 10% of CSI error and a BOR $U = 4$, the ESR decreases by 0.2 bit per channel use for the MF decoding structure (corresponding to a decrease of 41.7% from its maximal value), and by 0.155 bit per channel use for the SDS and OC decoding structures (corresponding to a decrease of 15.6% from its maximal value).

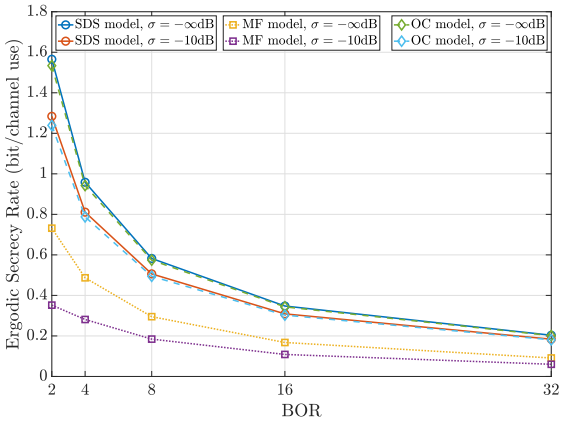

FIGURE 7. Achievable ESR as a function of the BOR, $\delta_B = 10$ dB, $\delta_E = 10$ dB.

Figure 7 illustrates the achievable ESR as a function of the BOR value, for the 3 scenarios and 2 CSI errors ($\sigma = -\infty$ dB and $\sigma = -10$ dB) obtained with closed-form expressions. First, it can be seen that the maximal ESR strongly decreases when the BOR increases, and in a quite similar proportion for all scenarios. In fact, when the BOR increases, the TR focusing gain increases at the expense of the data rate since less symbols are sent per OFDM block. This leads to a per-symbol ESR decrease. For example, for the error-free scenario, the maximal ESR decreases from 1.56 bit per channel use when $U = 2$, to 0.2 bit per channel use when $U = 32$ for the SDS decoder (decrease of 87.18%). It decreases from 0.73 bit per channel use when $U = 2$ to 0.09 bit per channel use when $U = 32$ for the MF decoder (decrease of 87.67%). Second, as it could have been anticipated, the ESR performance decreases with a CSI misestimate, for all BOR values.

In the following, only the scenario when Eve implements the MF decoder ($\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_\mathrm{B}\mathbf{H}_\mathrm{E}^*$) is investigated since it is the most challenging one to guarantee positive ESR.

Figure 8 shows the 5%-achievable secrecy rate as a function of the CSI estimation error, for different BOR values. For any $0 \leq \epsilon \leq 1$, the ϵ-achievable secrecy rate corresponds to the rate that is achievable securely while keeping an outage probability under ϵ, i.e., 100ϵ% of the realizations lead to lower secrecy values, [57]. First, it is observed that when

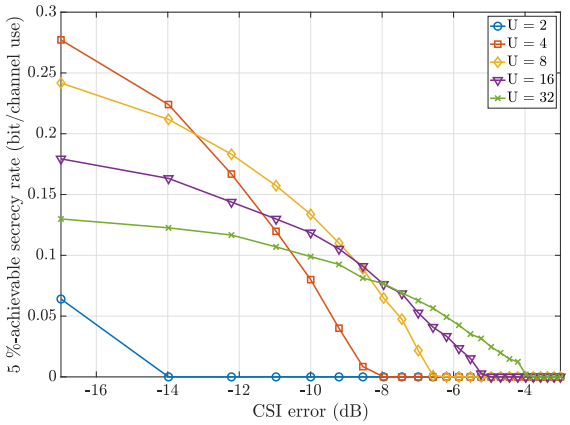

FIGURE 8. 5%-achievable secrecy rate as a function of the CSI error σ, $\delta_B = 10$ dB, MF Decoder.

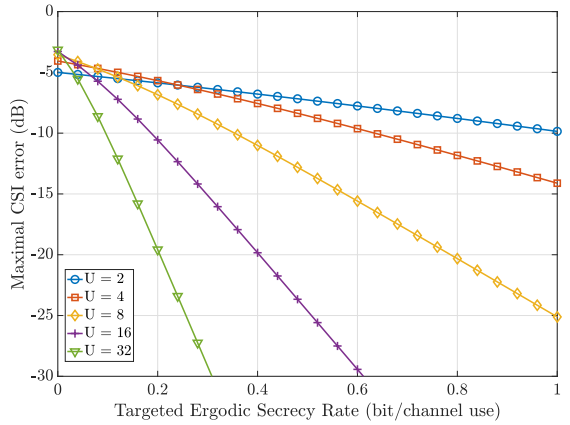

FIGURE 9. Maximal allowed CSI error as a function of the targeted ESR, MF Decoder.

$U = 2$, the 5%-achievable secrecy rate is very low and becomes zero, i.e., impossible to ensure a positive SR with less than 5% of outage, as soon as $\sigma > -14$ dB (corresponding to $\approx 4\%$ of CSI error). Increasing the BOR value allows to keep higher 5%-achievable secrecy rate for poor channel estimates. In particular, as soon as $\sigma > -7.5$ dB (corresponding to $\approx 18\%$ of CSI error), a spreading factor of $U = 32$ outperforms the lower BOR curves. Alice therefore needs to more accurately estimate Bob's CSI in order not to suffer from important outage when the BOR is low.

From Figures 7 and 8, it is observed that Alice's choice on the BOR value results from a trade-off. Knowing, the CSI error variance and Bob's SNR, Alice can choose a BOR value either to maximize the ESR (by decreasing the BOR value), i.e., higher data rate transmission, or to ensure a given ϵ-achievable secrecy rate (by increasing the BOR value), i.e., less data leakage.

Figure 9 presents the maximal allowed CSI error that can be made by Alice, given by (39), as a function of the targeted ESR, for different BOR values. It can be observed that, except for very low targeted ESR, lower CSI errors are required to target a particular ESR when the BOR increases. For example, when 0.2 bit per channel use is targeted, Alice can make an error of at most $\sigma = -20$ dB when $U = 32$ (corresponding to 1% of CSI error) but is allowed to misestimate Bob CSI with an error up to -6 dB when $U = 2$ (corresponding to $\approx 25\%$ of CSI error). There are two reasons. First, lower ESR values can be achieved when the BOR increases, as already observed in Figure 7. It leads to lower allowed CSI errors to target the same ESR for higher BOR than for lower ones. Second, when the BOR increases, the TR focusing gain increases at Bob as well. Therefore, a CSI estimation error has a greater impact for higher BOR values, leading to more ESR decrease.

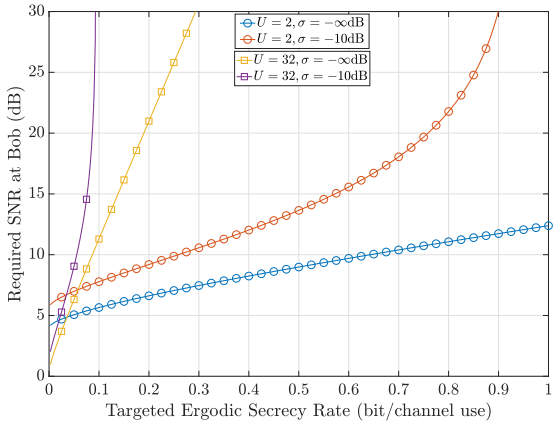

FIGURE 10. Required SNR at Bob as a function of the targeted ESR, MF Decoder.

Figure 10 illustrates the SNR that is needed at Bob as a function of the targeted ESR $= \Delta$, for different BOR values and for 2 different CSI errors ($\sigma = -\infty$ dB and $\sigma = -10$ dB). In particular, it represents (36) subject to constraint (39). As expected, the required SNR increases when the BOR increases to target a given ESR. The required SNR also increases when the CSI error increases. In particular, it is not possible to target ESR $= 0.1$ bit per channel use when $U = 32$ and $\sigma = -10$ dB. This can be anticipated from Figure 9 where the maximal CSI allowed error is equal to -10.3 dB when $U = 32$ and $\Delta = 0.1$ bit per channel use. In addition, when 1 bit per channel use is targeted, $U = 2$ and $\sigma = -10$dB, the required SNR at Bob $\to \infty$. From Figure 9, when $U = 2$ and $\Delta = 1$ bit per channel use, the maximal allowed CSI error is just above -10 dB. This leads to very high required SNR at Bob to achieve 1 bit per channel use when $\sigma = -10$ dB and $U = 2$.

V. CONCLUSION

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 an OFDM time reversal precoder to add to the transmitted data an artificial noise that lies in the null-space of Bob channel estimation while degrading 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. To achieve secrecy, an AN signal needs to be injected to the useful signal under constant total transmitted power constraint. This necessitates a frequency spreading which involves additional frequency resources.

Depending on the handshake procedure, the ESR performance is analytically derived, assuming Rayleigh-fading and uncorrelated channels, for three different well-suited decoding structures at Eve. The obtained analytical formulations consider imperfect Bob's CSI estimation made at Alice. The derivations allow Alice to determine the required SNR at Bob in order to guarantee a targeted communication ESR. The maximal allowed CSI errors are derived as well as the optimal amount of AN energy to inject. The performance 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.

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 and CSI errors. It is demonstrated that it is always possible to guarantee a positive ESR when Eve implements the SDS decoder ($\mathbf{G} = \mathbf{S}^H$), or the OC decoder ($\mathbf{G} = \mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*$), regardless the CSI estimation error made at Alice. It is also outlined that the choice of the spreading factor results from a trade-off, either to increase the ESR by decreasing the BOR, or to decrease the data leakage by increasing the BOR. For instance, when Eve implements the MF decoder ($\mathbf{G} = \mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^*$), with a BOR of 2 and 32 respectively, a per-symbol ESR of 0.27 and 0.06 bit per channel use is obtained with a Bob's SNR of 10 dB, with 10% of CSI estimation error, when Eve's SNR is infinite (see Figure 10). However, for the same situation, with a BOR of 2 and 32 respectively, the 5%−achievable secrecy rate is equal to 0 and 0.1 bit per channel use respectively (see Figure 8). Finally, Alice can be aware of the guaranteed ESR if she knows Bob's SNR and the CSI estimation error variance she makes. She can thus communicate while not exceeding this rate and therefore ensures the secrecy of the communication.

This paper shows 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, such as 5G or LTE, and does not necessitate extra hardware. These standards allow for flexible numerology such that it is possible to tune the communication parameters to meet the considered assumptions, i.e., independent channels between the BOR frequency components of a symbol. The scheme is practical and does not need to resolve complex optimization problems. As a perspective of this work, the influence of the frequency correlation between channel subcarriers needs to be investigated. Another perspective is to make the scheme compatible with multicast communications by designing a TR precoder where the AN signal lies in the null space of multiple legitimate users.

APPENDIX A
SINR DERIVATION AT BOB

A. DATA TERM

$$\begin{aligned}
\mathbb{E}\left[|B_1|^2\right] &= \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{B}}\hat{\mathbf{H}}_{\mathrm{B}}^*\mathbf{S}\right|^2\right] \\
&= \mathbb{E}\Big[\Big|\sqrt{\alpha(1-\sigma)}\mathbf{S}^H|\mathbf{H}_{\mathrm{B}}|^2\mathbf{S} \\
&\quad + \sqrt{\alpha\sigma}\mathbf{S}^H\mathbf{H}_{\mathrm{B}}\Delta\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\Big|^2\Big] \\
\mathbb{E}\left[|B_{1,n}|^2\right] &= \mathbb{E}\Bigg[\Bigg|\frac{\sqrt{\alpha(1-\sigma)}}{U}\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2 \\
&\quad + \frac{\sqrt{\alpha\sigma}}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},n+iN}\Delta h_{\mathrm{B},n+iN}^*\Bigg|^2\Bigg] \\
&= \frac{\alpha(1-\sigma)}{U^2}\Bigg[\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^4\right] \\
&\quad + \mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}|h_{\mathrm{B},n+iN}|^2|h_{\mathrm{B},n+jN}|^2\right]\Bigg] \\
&\quad + \frac{\alpha\sigma}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2|\Delta h_{\mathrm{B},n+iN}|^2\right] \\
&= \frac{1}{U^2}\alpha(1-\sigma)(2U+U(U+1)) + \frac{\alpha\sigma U}{U^2} \\
&= \frac{\alpha\left[(U+1)(1-\sigma)+\sigma\right]}{U} \qquad (44)
\end{aligned}$$

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

B. AWGN TERM

$$\begin{aligned}
\mathbb{E}\left[|B_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_{\mathrm{B}}\right|^2\right] \\
\mathbb{E}\left[|B_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{B},n+iN}|^2\right] = \sigma_{\mathrm{V,B}}^2 \qquad (45)
\end{aligned}$$

C. AN TERM

$$\mathbb{E}\left[|B_3|^2\right] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{B}}\mathbf{w}\right|^2\right]. \qquad (46)$$

We know that $\mathbf{S}^H\hat{\mathbf{H}}_{\mathrm{B}}\mathbf{w} = 0$ and $\hat{\mathbf{H}}_{\mathrm{B}} = \sqrt{1-\sigma}\mathbf{H}_{\mathrm{B}} + \sqrt{\sigma}\Delta\mathbf{H}_{\mathrm{B}}$, such that (46) becomes:

$$\begin{aligned}
\mathbb{E}\left[|B_3|^2\right] &= \mathbb{E}\left[\left|-\sqrt{\frac{(1-\alpha)\sigma}{1-\sigma}}\mathbf{S}^H\Delta\mathbf{H}_{\mathrm{B}}\mathbf{w}\right|^2\right] \\
&= \frac{(1-\alpha)\sigma}{1-\sigma}\mathbb{E}\left[\left|\mathbf{S}^H\Delta\mathbf{H}_{\mathrm{B}}\mathbf{w}\right|^2\right]. \qquad (47)
\end{aligned}$$

We define $\mathbf{w} = \sqrt{1-\sigma}\hat{\mathbf{w}} + \sqrt{\sigma}\mathbf{w}_\Delta$, where $\mathbf{S}^H\Delta\mathbf{H}_\mathrm{B}\mathbf{w}_\Delta = 0$ and $\hat{\mathbf{w}} \perp\!\!\!\perp \Delta\mathbf{H}_\mathrm{B}$, such that:

$$\mathbb{E}\left[|B_3|^2\right] = \frac{(1-\alpha)\sigma}{1-\sigma}(1-\sigma)\mathbb{E}\left[\left|\mathbf{S}^H\Delta\mathbf{H}_\mathrm{B}\hat{\mathbf{w}}\right|^2\right]$$

$$\mathbb{E}\left[|B_{3,n}|^2\right] = \frac{(1-\alpha)\sigma}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|\Delta h_{\mathrm{B},n+iN}\right|^2\left|\hat{w}_{n+iN}\right|^2\right] = \frac{(1-\alpha)\sigma}{U}U\frac{1}{U} = \frac{(1-\alpha)\sigma}{U}. \quad (48)$$

APPENDIX B
SINR DERIVATION AT EVE

D. SDS DECODER

1) DATA TERM

$$\mathbb{E}\left[|\mathbf{E}_1^{SDS}|^2\right] = \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\hat{\mathbf{H}}_\mathrm{B}^*\mathbf{S}\right|^2\right]$$

$$\mathbb{E}\left[|E_{1,n}^{SDS}|^2\right] = \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|\tilde{h}_{\mathrm{B},n+iN}^*\right|^2\right] = \frac{\alpha}{U}. \quad (49)$$

2) AWGN TERM

$$\mathbb{E}\left[|\mathbf{E}_2^{SDS}|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{E}\right|^2\right]$$

$$\mathbb{E}\left[|E_{2,n}^{SDS}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2. \quad (50)$$

3) AN TERM

$$\mathbb{E}\left[|\mathbf{E}_3^{SDS}|^2\right] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{w}\right|^2\right]$$

$$\mathbb{E}\left[|E_{3,n}^{SDS}|^2\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}w_{n+iN}|^2\right] = \frac{1-\alpha}{U}. \quad (51)$$

E. MF DECODER

1) DATA TERM

$$\mathbb{E}\left[|E_{1,n}^{MF}|^2\right] = \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\left|\tilde{h}_{\mathrm{B},n+iN}\right|^2\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] = \frac{\alpha}{U^2}(4U+U(U-1)) = \frac{\alpha(U+3)}{U} \quad (52)$$

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

$$\mathbb{E}\left[|\mathbf{E}_2^{MF}|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_\mathrm{E}^*\hat{\mathbf{H}}_\mathrm{B}\mathbf{v}_\mathrm{E}\right|^2\right]$$

$$\mathbb{E}\left[|E_{2,n}^{MF}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2|\tilde{h}_{\mathrm{B},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2. \quad (53)$$

3) AN TERM

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

$$\mathbf{v} = \mathbf{S}^H\hat{\mathbf{H}}_\mathrm{B}|\mathbf{H}_E|^2\mathbf{w} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{w}'. \quad (54)$$

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

$$\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) = \mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{V}_2^H|\mathbf{H}_E|^2\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right). \quad (55)$$

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:

$$\begin{aligned}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) &= \sum_{q=1}^{Q}\sum_{q'=1}^{Q}\mathbb{E}(|h_{E,q}|^2|h_{E,q'}|^2)\\ &\quad\mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_{q'}\mathbf{e}_{q'}^T\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right)\\ &= \sum_{q=1}^{Q}\mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right)\\ &\quad+\mathbb{E}\left(\mathbf{U}\mathbf{\Sigma}\mathbf{V}_1^H\mathbf{V}_2\mathbf{V}_2^H\mathbf{V}_1\mathbf{\Sigma}^H\mathbf{U}^H\right) \quad (56)\end{aligned}$$

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:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\mathbb{E}\left(\mathbf{v}\mathbf{v}^H\right) = \frac{1}{N}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{V}_1^H\sum_{q=1}^{Q}\left(\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\right)\mathbf{V}_1\right). \quad (57)$$

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 non-zero element.

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) &= \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\Big(\mathbf{\Sigma}^2\mathbf{v}_{1,l}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{e}_q^T\mathbf{V}_2\\ &\quad\mathbf{V}_2^H\mathbf{e}_q\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{1,l}^H\Big)\\ &= \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\mathbf{\Sigma}^2\mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{V}_2\mathbf{V}_2^H\mathbf{e}_q\mathbf{v}_{1,q}^H\right). \quad (58)\end{aligned}$$

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 $U-1$ non-zero elements:

$$\begin{aligned}\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) &= \frac{1}{N}\sum_{q=1}^{Q}\sum_{l}\sum_{l'}\mathbb{E}\Big(\mathbf{\Sigma}^2\mathbf{v}_{1,q}\mathbf{e}_q^T\mathbf{e}_l\mathbf{v}_{2,l}^H\\ &\quad\mathbf{v}_{2,l'}\mathbf{e}_{l'}^T\mathbf{e}_q\mathbf{v}_{1,q}^H\Big)\\ &= \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\mathbf{v}_{1,q}^H\mathbf{\Sigma}^2\mathbf{v}_{1,q}\right) \quad (59)\end{aligned}$$

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

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left(\|\mathbf{v}_{2,q}\|^2\|\mathbf{v}_{1,q}\|^2\sigma_n^2\right). \quad (60)$$

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:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\mathbb{E}\left[\left(\|\mathbf{v}_{1,q}\|^2 - \|\mathbf{v}_{1,q}\|^4\right)\sigma_n^2\right]. \quad (61)$$

To determine (61), 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:

$$\sigma_n = \sqrt{\sum_{i=1}^{U}\left|z_{(n-1)U+i}\right|^2}, n = 1\ldots N \quad (62)$$

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

$$\mathbb{E}\left[\sigma_n^2\right] = 1. \quad (63)$$

Without loss of generality, $\mathbb{E}\left[\|v_{1,1}\|^2\right]$ and $\mathbb{E}\left[\|v_{1,1}\|^4\right]$ can be computed since all components of $\mathbf{V}_1$ are identically distributed:

$$\mathbb{E}\left[\|v_1\|^2\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^2\right] = \frac{1}{U}. \quad (64)$$

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

$$\mathbb{E}\left[\|v_1\|^4\right] = \mathbb{E}\left[\left|\frac{z_1^*}{\sigma_1}\right|^4\right] = \mathbb{E}\left[\frac{|z_1|^4}{\left(\sum_{i=1}^{U}|z_i|^2\right)^2}\right] = \frac{2}{U(U+1)}. \quad (65)$$

Finally, eq.(61) can be computed as:

$$\frac{1}{N}\mathbb{E}\left(\|\mathbf{v}\|^2\right) = \frac{1}{N}\sum_{q=1}^{Q}\left[\left(\frac{1}{U} - \frac{2}{U(U+1)}\right)1\right] = \frac{U-1}{U+1}. \quad (66)$$

Keeping into account the normalization factors, it follows:

$$\mathbb{E}\left[|E_{3,n}^{MF}|^2\right] = (1-\alpha)\frac{1}{U-1}\frac{U-1}{U+1} = \frac{1-\alpha}{U+1}. \quad (67)$$

F. OC DECODER

1) DATA TERM

$$\mathbb{E}\left[|E_{1,n}^{OC}|^2\right] = \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}h_{\mathrm{B},n+iN}^*\left|h_{\mathrm{E},n+iN}\right|^2\right|^2\right] = \frac{\alpha}{U^2}\left(U.2.1 + U(U-1).1.1.0\right) = \frac{2\alpha}{U}. \quad (68)$$

2) AWGN TERM

$$\mathbb{E}\left[|\mathbf{E}_2^{OC}|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{H}_{\mathrm{E}}^*\mathbf{v}_{\mathrm{E}}\right|^2\right]$$

$$\mathbb{E}\left[|E_{2,n}^{OC}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] = \sigma_{\mathrm{V,E}}^2. \quad (69)$$

3) AN TERM

$$\mathbb{E}\left[|\mathbf{E}_3^{OC}|^2\right] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\left|\mathbf{H}_{\mathrm{E}}\right|^2\mathbf{w}\right|^2\right]$$

$$\mathbb{E}\left[|E_{3,n}^{OC}|^2\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^4|w_{n+iN}|^2\right] = \frac{2(1-\alpha)}{U}. \quad (70)$$

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 Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Feb. 2019.
[2] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.
[3] B. Matthieu, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[4] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
[5] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[6] D. D. Tran, D. B. Ha, V. T. Ha, and E. K. Hong, "Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels," *IETE J. Res.*, 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. 26350–26357, 2018.
[8] S. Golstein, T.-H. Nguyen, F. Horlin, P. D. Doncker, and J. Sarrazin, "Physical layer security in frequency-domain time-reversal SISO OFDM communication," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 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," *Ann. Telecommun.*, vol. 76, pp. 155–174, Sep. 2020.
[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Aug. 1975.
[11] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[12] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[13] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[14] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.
[15] R. Mellki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on OFDM physical layer security," *Phys. Commun.*, vol. 32, pp. 1–30, Feb. 2019.
[16] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[18] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[19] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Veh. Technol. Conf. (VTC-Fall)*, vol. 3, Sep. 2005, pp. 1906–1910.

[20] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Mil. Commun. Conf.*, vol. 3, Oct. 2005, pp. 1501–1506.

[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[22] J. Lin, Q. Li, and J. Yang, "Frequency diverse array beamforming for physical-layer security with directionally-aligned legitimate user and eavesdropper," in *Proc. 25th Eur. Signal Process. Conf. (EUSIPCO)*, 2017, pp. 2166–2170, doi: 10.23919/EUSIPCO.2017.8081593.

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

[24] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[25] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

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

[27] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE Int. Solid-State Circuits Conf.-Dig. Tech. Papers*, Feb. 2008, pp. 188–605.

[28] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[29] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[30] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9747–9760, Oct. 2019.

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

[32] F. Rottenberg, P. De Doncker, F. Horlin, and J. Louveaux, "Secrecy capacity of FBMC-OQAM modulation over frequency selective channel," *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1230–1234, Aug. 2020.

[33] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

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

[35] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure index and data symbol modulation for OFDM-IM," *IEEE Access*, vol. 5, pp. 24959–24974, 2017.

[36] 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. 25863–25875, 2017.

[37] Q. Xu, P. Ren, Q. Du, and L. Sun, "Security-aware waveform and artificial noise design for time-reversal-based transmission," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5486–5490, Jun. 2018.

[38] S. Li, N. Li, X. Tao, Z. Liu, H. Wang, and J. Xu, "Artificial noise inserted secure communication in time-reversal systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[39] S. Li, N. Li, Z. Liu, H. Wang, J. Xu, and X. Tao, "Artificial noise aided path selection for secure TR communications," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–6.

[40] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, Mar. 2017.

[41] K. Umebayashi, F. Nakabayashi, and Y. Suzuki, "A study on secure pilot signal design for OFDM systems," in *Proc. Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA), Asia–Pacific*, Dec. 2014, pp. 1–5.

[42] C. Oestges, A. Kim, G. Papanicolaou, and A. J. Paulraj, "Characterization of space-time focusing in time-reversed random fields," *IEEE Trans. Antennas Propag.*, vol. 53, no. 1, pp. 283–293, Jan. 2005.

[43] T. Dubois, M. Crussiere, and M. Helard, "On the use of time reversal for digital communications with non-impulsive waveforms," in *Proc. 4th Int. Conf. Signal Process. Commun. Syst.*, Dec. 2010, pp. 1–6.

[44] W. Lei, W. Zhang, M. Yang, H. Lei, and X. Xie, "Optimization of preprocessing filter for time-reversal multi-user secure transmission systems based on artificial noise," *Digit. Signal Process.*, vol. 109, Feb. 2021, Art. no. 102933.

[45] R. Cepeda, M. Fitton, and A. Nix, "The performance of robust adaptive modulation over wireless channels with non reciprocal interference," in *Proc. IEEE 55th Veh. Technol. Conf.*, vol. 3, May 2002, pp. 1497–1501.

[46] Y. Shi, M. Badi, D. Rajan, and J. Camp, "Channel reciprocity analysis and feedback mechanism design for mobile beamforming systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6029–6043, Jun. 2021.

[47] S. Kavaiya, D. K. Patel, Z. Ding, Y. L. Guan, and S. Sun, "Physical layer security in cognitive vehicular networks," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2557–2569, Apr. 2021.

[48] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "On the performance of underlay cognitive radio system with random mobility under imperfect channel state information," *Int. J. Commun. Syst.*, vol. 33, no. 15, p. e4561, Jul. 2020.

[49] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[50] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct. 2014.

[51] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On–off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6075–6088, Aug. 2016.

[52] P. Mu, Z. Li, and B. Wang, "Secure on–off transmission in slow fading wiretap channel with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9582–9586, Oct. 2017.

[53] T.-H. Nguyen, S. Monfared, J.-F. Determe, J. Louveaux, P. De Doncker, and F. Horlin, "Performance analysis of frequency domain precoding time-reversal MISO OFDM systems," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 48–51, Jan. 2020.

[54] S. Ahmed, T. Noguchi, and M. Kawai, "Selection of spreading codes for reduced PAPR in MC-CDMA systems," in *Proc. IEEE 18th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2007, pp. 1–5.

[55] H.-V. Tran, H. Tran, G. Kaddoum, D.-D. Tran, and D.-B. Ha, "Effective secrecy-SINR analysis of time reversal-employed systems over correlated multi-path channel," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 527–532.

[56] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[57] O. Güngör, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

SIDNEY J. GOLSTEIN (Student Member, IEEE) received the B.Sc. degree in electrical engineering from the Université Libre de Bruxelles (ULB), Brussels, Belgium, in 2016, and the M.Sc. degree in electrical engineering jointly from the ULB and the Vrij Universiteit of Brussels (VUB), Brussels, in 2018. He is currently pursuing the Ph.D. degree in electrical engineering jointly with the Laboratoire de Génie Electrique et Electronique de Paris (GeePs), Sorbonne Université (SU), Paris, France, and the Wireless Communication Group (WCG), ULB, funded by the Ecole Doctorale Informatique, Télécommunications et Electronique (EDITE) de Paris. His research interest includes physical-layer security.

FRANÇOIS ROTTENBERG (Member, IEEE) received the M.Sc. degree in electrical engineering from the Université Catholique de Louvain (UCLouvain), Louvain-la-Neuve, in 2014, and the Ph.D. degree jointly from the UCLouvain and the Université libre de Bruxelles (ULB), Brussels, in 2018. From 2018 to 2019, he was a Postdoctoral Researcher with the University of Southern California (USC), Los Angeles, CA, USA. From 2019 to 2021, he was a Postdoctoral Researcher with the UCLouvain and the ULB, funded by the Belgian National Science Foundation (FRS-FNRS). He has been a Regular Visitor and a Collaborator of the Centre Tecnològic Telecomunicacions Catalunya (CTTC), Castelldefels, Spain, and the National Institute of Information and Communications Technology (NICT), Tokyo, Japan. He is currently a Visiting Assistant Professor with the Katholieke Universiteit Leuven (KU Leuven). His main research interests include signal processing for next generations of communication systems, including novel modulation formats, multi-antenna systems, and physical-layer security.

FRANÇOIS HORLIN (Member, IEEE) received the Ph.D. degree from the Université Catholique de Louvain (UCL), in 2002. He specialized in the field of signal processing for digital communications. He joined the Inter-university Micro-Electronics Center (IMEC), as a Senior Scientist, in 2006. He worked on the design efficient transceivers that can cope with the channel and hardware impairments in the context of 4G cellular systems. In 2007, he became a Professor at the Université libre de Bruxelles (ULB). He is supervising a research team working on modern communication systems. Localization based on 5G signals, filterbank-based modulations, massive MIMO, and dynamic spectrum access, are examples of investigated research topics. Recently, the team focused on the design of passive radars, working by opportunistically capturing the Wi-Fi communication signals to monitor the crowd dynamics.

PHILIPPE DE DONCKER (Member, IEEE) received the M.Sc. degree in physics engineering and the Ph.D. degree in science engineering from the Université Libre de Bruxelles (ULB), Brussels, Belgium, in 1996 and 2001, respectively. He is currently a Full Professor with the ULB, where he also leads the research activities on wireless channel modeling and electromagnetics.

JULIEN SARRAZIN (Senior Member, IEEE) received the Engineering Diploma/Master of Research and Ph.D. degrees from the University of Nantes, France, in 2005 and 2008, respectively. In 2009 and 2010, he worked at the BK Birla Institute of Technology of Pilani, India. In 2011 and 2012, he was a Research Engineer at Telecom ParisTech, Paris. Since September 2012, he has been an Associate Professor at Sorbonne Université, Paris, where he is currently working with the Group of Electrical Engineering of Paris (GeePs) Research Institute in the field of spatial data focusing, antenna design, channel modeling, and physical layer security.