SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

ULB UNIVERSITÉ LIBRE DE BRUXELLES

PhD Thesis: T+12 Report

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

Sidney Golstein

Promotor:
Pr. Dr. Ir. Julien Sarrazin

Co-promotor:
Pr. Dr. Ir. Philippe De Doncker

April 9, 2020

Contents

List of Figures

1 Introduction

Due to their broadcast nature, wireless communications remain unsecured. With the deployment of 5G as an heterogeneous network possibly involving different radio access technologies, physical layer security (PLS) has gained recent interests in order to secure wireless communications, [**PLS_litt1**, **PLS_litt2**, **PLS_litt3**]. PLS classically takes benefit of the characteristics of wireless channels, such as multipath fading, to improve security of communications against potential eavesdroppers. A secure communication can exist as soon as the eavesdropper channel is degraded with respect to the legitimate user one, [**wyner**]. This can be achieved by increasing the signal-to-interference-plus-noise ratio (SINR) at the intended position and decreasing the SINR at the unintended position if its channel state information (CSI) is known, and/or, by adding an artificial noise (AN) signal that lies in the null space of the legitimate receiver's channel. While many works implement these schemes using multiple antennas at the transmitter, only few ones intend to do so with single-input single-output (SISO) systems [**PLS_litt4**, **TR_FD_TD**, **TR_AN_2018_xu**, **TR_AN_2017_Li**, **TR_AN_2018_Li**].

In [**PLS_litt4**], a technique is proposed that combines a symbol waveform optimisation in time-domain (TD) to reach a desired SINR at the legitimate receiver and an AN injection using the remaining available power at the transmitter when eavesdropper's CSI is not known. Another approach to increase the SINR in SISO systems is time-reversal (TR). This has the advantage to be implemented with a simple precoder at the transmitter. TR achieves a gain at the intended receiver position only, thereby naturally offering a possibility of secure communication, [**otges**]. TR is achieved by up/downsampling the signal in the TD. It as been shown in [**TR_FD_TD**] that TR can be equivalently achieved in frequency-domain (FD) by replicating and shifting the signal spectrum. FD implementation has the advantage to be easily performed using orthogonal frequency-division multiplexing (OFDM). To further enhance the secrecy, few works combine TD TR precoding with AN injection [**TR_AN_2018_xu**, **TR_AN_2017_Li**, **TR_AN_2018_Li**]. In these works, the AN is added either on all the channel taps or on a set of selected taps. While the condition for AN generation is given, its derivation is however not detailed. Furthermore, the impact of BOR, defined as the up/downsampling rate [**TR_bor**], has not been yet studied in the literature.

An approach to establish secure communication using a FD TR precoder in SISO OFDM systems is proposed. An AN signal is designed to maximize the secrecy rate (SR) of the communication in presence of a passive eavesdropper whose CSI is supposed unknown. The proposed scheme uses only frequency diversity inherently present in multipath environments to achieve security. It can therefore be used in SISO systems and is then well-suited for resource-limited nodes such as encountered in Internet-Of-Things (IoT) for instance. Indeed, multiple-input multiple-output (MIMO) capabilities require several antennas and as many transceivers and ADC/DAC, which might not fit into small-size sensors and could be too power-consuming for such IoT scenarios. Furthermore, the OFDM implementation makes this approach compatible with LTE and 5G systems.

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

2 System Model

A scheme of the secure FD TR SISO OFDM communication is presented in Fig.1 where Alice transmits wireless data to a legitimate receiver Bob. An eavesdropper (Eve) tries to eavesdrop the data. We assume that Alice does not have any information about Eve's CSI and perfectly knows Bob's instantaneous CSI.

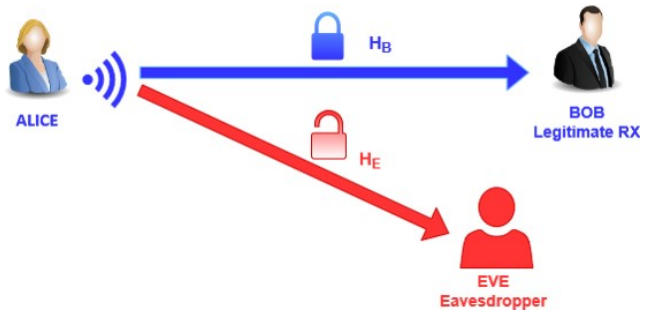

Figure 1: Security scenario

2.1 Conventional FD TR SISO OFDM Communication

The FD TR precoding scheme is illustrated in Fig.2. The communication is designed such that the data focuses at the legitimate receiver's position.

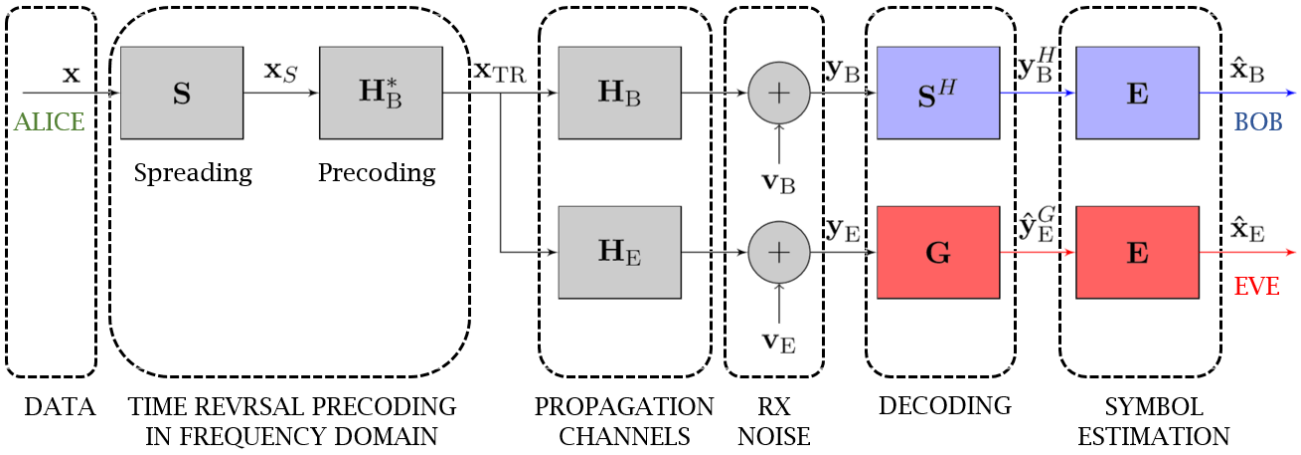

Figure 2: Conventional FD TR SISO OFDM system

The data is conveyed onto OFDM symbols with Q subcarriers. Without loss of generality, we consider that only one OFDM block $\mathbf{x}$ is sent over the FD TR precoding SISO OFDM system. A data block $\mathbf{x}$ is composed of N symbols x_n (for $n = 0, ..., N-1$, with $N \leq Q$). The symbol x_n is assumed to be a zero-mean random variable (RV) with variance $\mathbb{E}\left[|x_n|^2\right] = \sigma_x^2 = 1$ (i.e., a normalized constellation is considered). The data block $\mathbf{x}$ is then spread with a factor $U = Q/N$, called BOR, via the matrix $\mathbf{S}$ of size $Q \times N$. The matrix $\mathbf{S}$ is called the spreading matrix and stacks U times $N \times N$ diagonal matrices, with diagonal elements taken from the set $\{\pm 1\}$ and being identically and independently distributed (i.i.d.) in order not to increase the peak-to-average-power ratio (PAPR) as suggested in [**papr**]. This

matrix is normalized by a factor $\sqrt{U}$ in order to have $\mathbf{S}^H\mathbf{S} = \mathbf{I}_N$:

$$\mathbf{S} = \frac{1}{\sqrt{U}} \cdot \begin{pmatrix} \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \\ & \vdots & \vdots & \\ \pm 1 & 0 & \dots & 0 \\ 0 & \pm 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm 1 \end{pmatrix} \quad ; \quad [Q \times N] \tag{1}$$

As stated in [**TR_FD_TD**], the idea behind the spreading is that up-sampling a signal in the TD is equivalent to the repetition and shifting of its spectrum in the FD. In doing so, each data symbol will be transmitted onto U different subcarriers with a spacing of N subcarriers, introducing frequency diversity. The spread sequence is then precoded before being transmitted. This requires the knowledge of Bob channel frequency response (CFR) at Alice. We consider that Alice can perfectly estimate Bob CFR. The channels between Alice and Bob ($\mathbf{H}_\mathrm{B}$) and between Alice and Eve ($\mathbf{H}_\mathrm{E}$) are assumed to be static during the transmission of one OFDM symbol. $\mathbf{H}_\mathrm{B}$ and $\mathbf{H}_\mathrm{E}$ are $Q \times Q$ diagonal matrices whose elements are $h_{\mathrm{B},q}$ and $h_{\mathrm{E},q}$ (for $q = 0, ..., Q-1$) and follow a zero-mean unit-variance complex normal distribution, i.e., their modulus follow a Rayleigh distribution. We also consider that the overall channel energies are normalized to unity for each channel realization. The precoding matrix $\mathbf{H}_\mathrm{B}^*$ is also a diagonal matrix with elements $h_{\mathrm{B},q}^*$. At the receiver, a despreading operation is performed by applying $\mathbf{S}^H$. We consider that Bob knows the spreading sequence and apply a zero-forcing (ZF) equalization. In the following, different decoding structures $\mathbf{G}$ will be investigated at Eve. These different schemes will lead to different level of security performances. A perfect synchronization is also assumed at Bob and Eve positions.

An illustration of such a communication is presented in Fig.3 where a block of $N = 4$ symbols is spread by a factor $U = 4$ and then sent via $Q = 16$ subcarriers. We observe that, at Bob, the received sequence is perfectly recovered which is not the case at Eve's position.

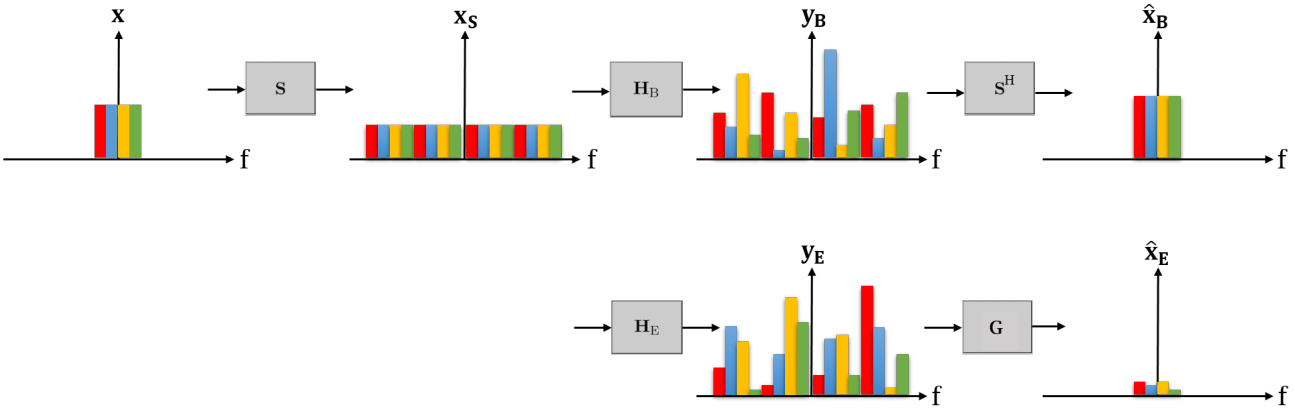

Figure 3: Illustration of conventional FD TR SISO OFDM system

2.1.1 Received sequence at the intended position

After despreading, the received sequence at Bob is:

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

where $\mathbf{v}_{\mathrm{B}}$ is the FD complex additive white Gaussian noise (AWGN). The noise's auto-correlation is $\mathbb{E}\left[|v_{\mathrm{B},n}|^2\right] = \sigma^2_{\mathrm{V,B}}$ and the covariance matrix is $\mathbb{E}\left[(\mathbf{S}^H\mathbf{v}_{\mathrm{B}}).(\mathbf{S}^H\mathbf{v}_{\mathrm{B}})^H\right] = \sigma^2_{\mathrm{V,B}}.\mathbf{I}_N$. We also assume that the data symbol x_n and noise $v_{\mathrm{B,n}}$ are independent of each other. In (2), each transmitted symbol is affected by a real gain at the position of the legitimate receiver since the product $\mathbf{H}_{\mathrm{B}}\ \mathbf{H}_{\mathrm{B}}^{*}$ is a real diagonal matrix. The gains differ between each symbol in the OFDM block but increases with an increase of the BOR value as each symbol would be sent on more subcarriers and would benefit from a larger frequency diversity gain. If we consider a fixed bandwidth, the TR focusing effect is enhanced for higher BOR's at the expense of the data rate. After ZF equalization, we obtain:

$$\hat{\mathbf{x}}_{\mathrm{B}} = \left(\mathbf{S}^{H} \left|\mathbf{H}_{\mathrm{B}}\right|^{2} \mathbf{S}\right)^{-1} \left(\mathbf{S}^{H} \left|\mathbf{H}_{\mathrm{B}}\right|^{2} \mathbf{S}\, \mathbf{x} + \mathbf{S}^{H} \mathbf{v}_{\mathrm{B}}\right) = \mathbf{x} + \left(\mathbf{S}^{H} \left|\mathbf{H}_{\mathrm{B}}\right|^{2} \mathbf{S}^{H}\right)^{-1} \mathbf{S}^{H} \mathbf{v}_{\mathrm{B}} \tag{3}$$

From (3), we observe that the transmit data is perfectly recovered at high signal-to-noise ratio (SNR).

2.1.2 Received sequence at the unintended position

The data received at the unintended position is given by:

$$\mathbf{y}_{\mathrm{E}}^{G} = \mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x} + \mathbf{v}_{\mathrm{E}} \tag{4}$$

where $\mathbf{G}$ is a $N \times N$ filter matrix performed by Eve, $\mathbf{v}_{\mathrm{E}}$ is the complex AWGN. The noise auto-correlation is $\mathbb{E}\left[|v_{\mathrm{E,n}}|^2\right] = \sigma^2_{\mathrm{V,E}}$ and the covariance matrix is $\mathbb{E}\left[(\mathbf{S}^H\mathbf{v}_{\mathrm{E}}).(\mathbf{S}^H\mathbf{v}_{\mathrm{E}})^H\right] = \sigma^2_{\mathrm{V,E}}.\mathbf{I}_N$. In (4), $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}$ is a complex diagonal matrix. Therefore, due to the precoding, i.e., since the data transmission is designed to reach Bob position, each received symbol component will be affected by a random complex coefficient. The magnitude of this coefficient does not depend on the BOR value. It results in an absence of TR gain at the unintended position. As a consequence, worse decoding performance is obtained compared to the intended position. Eve needs lower noise power than Bob to reach the same bit-error-rate (BER). After ZF equalization, one obtains:

$$\hat{\mathbf{x}}_{\mathrm{E}} = \left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1} \left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x} + \mathbf{v}_{\mathrm{E}}\right) = \mathbf{x} + \left(\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\right)^{-1} \mathbf{G}\mathbf{v}_{\mathrm{E}} \tag{5}$$

Equation (5) shows that in the classical FD TR SISO OFDM communication scheme, the data could potentially be recovered at Eve's position. A similar BER could be obtained at Eve if she is closer to Alice than Bob is and/or if its noise power is less than Bob's one. This motivates the addition of AN in order to corrupt the data detection at any unintended positions in order to secure the communication. In Section 3, different filtering structures $\mathbf{G}$ will be investigated leading to different security performances of the scheme.

2.2 FD TR SISO OFDM communication with AN addition

In order to secure the communication between Alice and Bob, an AN signal $\mathbf{w}$ is added after precoding to the useful signal $\mathbf{x}_S$ at the transmitter side, as depicted in Fig. 4. The AN should not have any impact at Bob's position but should be seen as interference everywhere else since Alice does not have any information about Eve's CSI. Furthermore, this signal should not be guessed at the unintended

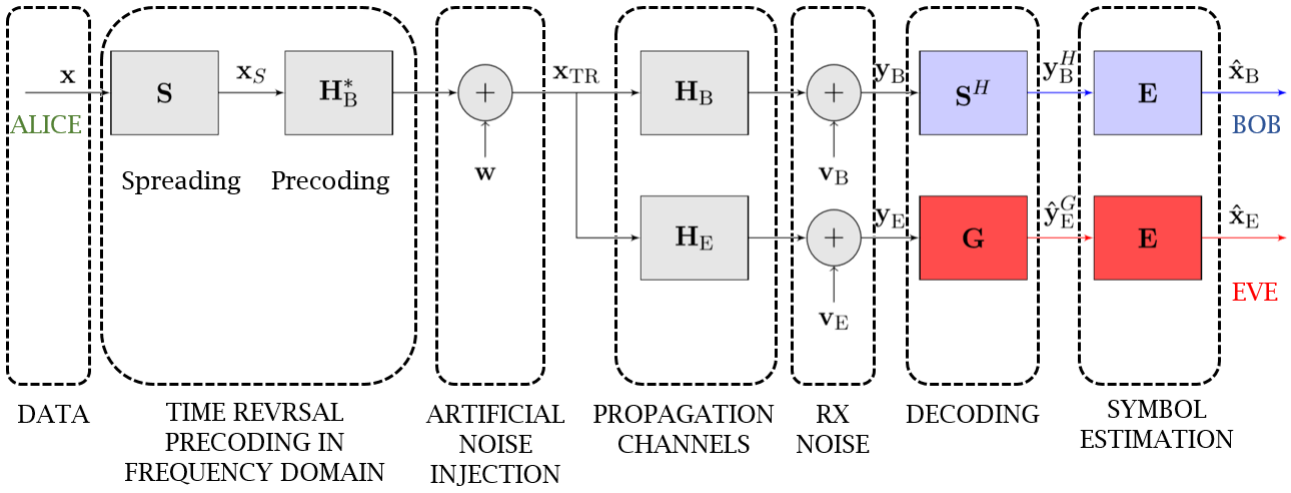

Figure 4: FD TR SISO OFDM system with added artificial noise

positions to ensure the secure communication. With these considerations, the transmitted sequence becomes:

$$\mathbf{x}_{\mathrm{TR}} = \sqrt{\alpha}\, \mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\, \mathbf{x} + \sqrt{1-\alpha}\, \mathbf{w} \tag{6}$$

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

Fig.5 illustrates a scheme with additive AN. We sent a block of $N = 4$ symbols which is spread by a factor $U = 4$, i.e., the data is conveyed onto $Q = 16$ subcarriers. A block of 16 AN symbols is added (in pink). At bob's position, there is no influence of these AN symbols and the data is perfectly recovered. At Eve, the received symbols are corrupted by the AN signal and by the data precoding.

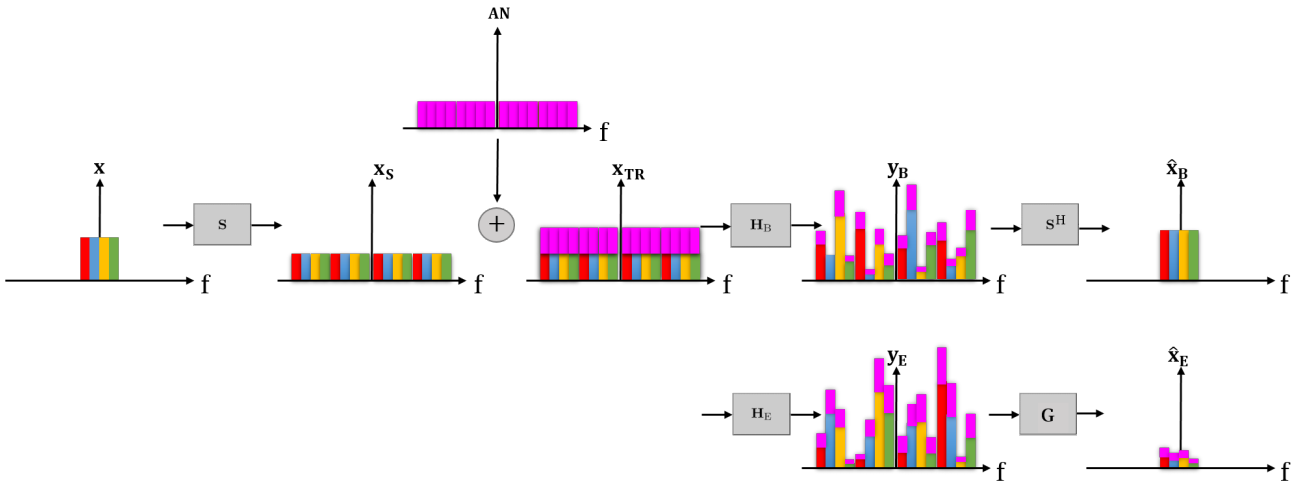

Figure 5: Illustration of FD TR SISO OFDM system with added artificial noise

2.2.1 AN Design

In order not to have any impact at the intended position, the AN signal must satisfy the following condition:

$$\mathbf{A}\mathbf{w} = \mathbf{0} \tag{7}$$

where $\mathbf{A} = \mathbf{S}^H\mathbf{H}_\mathrm{B} \in \mathbb{R}^{N\times Q}$. Condition (7) ensures that $\mathbf{w}$ lies in the right null space of $\mathbf{A}$. If we perform a singular value decomposition (SVD) of $\mathbf{A}$, we obtain:

$$\mathbf{A} = \mathbf{U}\left(\Sigma\ \mathbf{0}_{Q-N\times Q}\right)\begin{pmatrix}\mathbf{V}_1^H\\ \mathbf{V}_2^H\end{pmatrix} \tag{8}$$

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

$$\mathbf{w} = \mathbf{V}_2\tilde{\mathbf{w}} \tag{9}$$

which ensures that (7) is satisfied for any arbitrary vector $\tilde{\mathbf{w}} \in \mathbb{C}^{Q-N\times 1}$. Since $Q = NU$, as soon as $U \geq 2$, there is a set of infinite possibilities to generate $\tilde{\mathbf{w}}$ and therefore the AN signal. In the following, we assume that $\tilde{\mathbf{w}}$ is a zero-mean circularly symmetric white complex Gaussian noise with covariance matrix $\mathbb{E}\left[\tilde{\mathbf{w}}(\tilde{\mathbf{w}})^H\right] = \mathbf{I}_{Q-N\times 1}$, which implies that $\mathbb{E}\left[\mathbf{w}\mathbf{w}^H\right] = \mathbf{V}_2\mathbf{V}_2^H = \sigma_{\mathrm{AN}}^2\mathbf{I}_N$, where σ_{AN}^2 is the AN autocorrelation.

2.2.2 Received sequence at the intended position

After despreading, the received sequence at Bob is:

$$\mathbf{y}_\mathrm{B}^H = \sqrt{\alpha}\ \mathbf{S}^H\left|\mathbf{H}_\mathrm{B}\right|^2\mathbf{S}\mathbf{x}\ +\ \mathbf{S}^H\mathbf{v}_\mathrm{B} \tag{10}$$

Again, each transmitted symbol is affected by a real gain depending on the BOR value and weighted by $\sqrt{\alpha}$. One can observe that no AN contribution is present in (10) since (7) is respected. A ZF equalization is performed at the receiver leading to:

$$\hat{\mathbf{x}}_\mathrm{B} = \left(\sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_\mathrm{B}\right|^2\mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_\mathrm{B}\right|^2\mathbf{S}\mathbf{x} + \mathbf{S}^H\mathbf{v}_\mathrm{B}\right) = \mathbf{x} + \left(\sqrt{\alpha}\mathbf{S}^H\left|\mathbf{H}_\mathrm{B}\right|^2\mathbf{S}\right)^{-1}\mathbf{S}^H\mathbf{v}_\mathrm{B} \tag{11}$$

From (11), a perfect data recovery is possible in high SNR scenario.

2.2.3 Received sequence at the unintended position

The received sequence at the eavesdropper position has the form:

$$\mathbf{y}_\mathrm{E}^G = \sqrt{\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{w} + \mathbf{G}\mathbf{v}_\mathrm{E} \tag{12}$$

In (12), a term depending on the AN signal appears since $\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{w} \neq \mathbf{0}$. This term introduces an interference at Eve and thus scrambles the received constellation even in a noiseless environment. After ZF equalization, the estimated symbols are:

$$\begin{aligned}\hat{\mathbf{x}}_\mathrm{E} &= \left(\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right)^{-1}\left(\sqrt{\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\mathbf{x} + \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{w} + \mathbf{G}\mathbf{v}_\mathrm{E}\right)\\ &= \sqrt{\alpha}\mathbf{x} + \sqrt{1-\alpha}\left(\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{w} + \left(\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right)^{-1}\mathbf{G}\mathbf{v}_\mathrm{E}\end{aligned} \tag{13}$$

Equation (13) shows that the addition of AN in the FD TR SISO OFDM communication can secure the data transmission. It is to be noted that, since $\mathbf{w}$ is generated from an infinite set of possibilities, even if Eve knows its equivalent channel $\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*$ and the spreading sequence, she cannot estimate the AN signal to try retrieving the data. The degree of security will depend on the amount of AN energy that is injected into the communication and the decoding capabilities of Eve, as shown in Section 3.

3 Performance Assessment

The secrecy rate (SR) is defined as the maximum transmission rate that can be supported by the legitimate receiver's channel while ensuring the impossibility for the eavesdropper to retrieve the data, [**TR_Tran_secrecy_capa**]. In the ergodic sense, it can be expressed as:

$$\begin{aligned} C_S &= \mathbb{E}\left[\log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right)\right] \quad , \quad \gamma_B > \gamma_E \\ &\leq \log_2\left(1+\mathbb{E}\left[\gamma_B\right]\right) - \log_2\left(1+\mathbb{E}\left[\gamma_E\right]\right) \end{aligned} \tag{14}$$

with γ_B and γ_E being respectively the SINR at Bob and Eve's positions. The inequality in (14) arises from the Jensen's inequality.
In the following, we consider these assumptions:

- Bob and Eve channels are independent: $h_{B,i} \perp\!\!\!\perp h_{E,i},\ \forall i$
- No frequency correlation between subcarriers[1]: $h_{B,i} \perp\!\!\!\perp h_{B,j},\ \forall i \neq j$; $h_{E,i} \perp\!\!\!\perp h_{E,j},\ \forall i \neq j$

3.1 SINR determination

3.1.1 At Bob, i.e., the intended position

At Bob, the received signal after despreading is given by (10). Using the Jensen's inequality, a lower bound on the average SINR can be derived for the transmitted symbols n as:

$$\begin{aligned} \mathbb{E}\left[\gamma_{B,n}\right] &= \mathbb{E}\left[\frac{\alpha\left|k_n x_n\right|^2}{\left|v_{B,n}\right|^2}\right] = \alpha\mathbb{E}\left[\left|k_n x_n\right|^2\right]\mathbb{E}\left[\frac{1}{\left|v_{B,n}\right|^2}\right] \\ &\geq \frac{\alpha\mathbb{E}\left[\left|k_n x_n\right|^2\right]}{\mathbb{E}\left[\left|v_{B,n}\right|^2\right]} = \frac{\alpha\mathbb{E}\left[\left|k_n\right|^2\right]\mathbb{E}\left[\left|x_n\right|^2\right]}{\mathbb{E}\left[\left|v_{B,n}\right|^2\right]} \end{aligned} \tag{15}$$

where $k_n = \frac{1}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2$, x_n is the n^{th} data symbol, and $v_{B,n} = \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1}\left|v_{\mathrm{B},n+iN}\right|$ is the n^{th} noise symbol component and where it is observed that $k_n \perp\!\!\!\perp x_n \perp\!\!\!\perp v_{B,n}$. We find[2]:

$$\begin{aligned} \mathbb{E}\left[\left|k_n\right|^2\right] &= \frac{\alpha(U+1)}{U} \\ \mathbb{E}\left[\left|x_n\right|^2\right] &= 1 \\ \mathbb{E}\left[\left|v_{B,n}\right|^2\right] &= \sigma^2_{V,B} \end{aligned} \tag{16}$$

The SINR for a particular symbol at the intended position is then given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \geq \frac{\alpha\ (U+1)}{U\ \sigma^2_{\mathrm{V,B}}} \tag{17}$$

It was observed in simulations than the lower-bound (17) is tight enough to be used as an approximation of the averaged SINR at the intended position.

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

[2] See Appendix A

3.1.2 At Eve, i.e., the unintended position

At the unintended position, the received signal before ZF equalization is given by (12). Let's introduce $\mathbf{A}_1 = \sqrt{\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\mathbf{x}$, $\mathbf{A}_2 = \mathbf{G}\mathbf{v}_{\mathrm{E}}$ and $\mathbf{A}_3 = \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w}$ being respectively the data component, the noise component and the AN component of the received signal for a particular decoding structure $\mathbf{G}$. Using the Jensen's inequality, an approximation of a lower-bound of the averaged SINR of the symbols n at the unintended position can be derived as[3]:

$$\begin{aligned}\mathbb{E}\left[\gamma_{E,n}\right] &= \mathbb{E}\left[\frac{|A_{1,n}|^2}{|A_{2,n}+A_{3,n}|^2}\right] \approx \mathbb{E}\left[|A_{1,n}|^2\right]\mathbb{E}\left[\frac{1}{|A_{2,n}+A_{3,n}|^2}\right] \\ &\geq \frac{\mathbb{E}\left[|A_{1,n}|^2\right]}{\mathbb{E}\left[|A_{2,n}+A_{3,n}|^2\right]} = \frac{\mathbb{E}\left[|A_{1,n}|^2\right]}{\mathbb{E}\left[|A_{2,n}|^2\right]+\mathbb{E}\left[|A_{3,n}|^2\right]}\end{aligned} \tag{18}$$

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

3.1.2.1 Same structure as Bob

In this scenario, Eve has the same capabilities as Bob, i.e., she despread the received signal thanks to $\mathbf{G} = \mathbf{S}^H$. In that case, the received signal is:

$$\mathbf{y}_{\mathrm{E}}^{G} = \sqrt{\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{S}\,\mathbf{x} \;+\; \sqrt{1-\alpha}\,\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w} \;+\; \mathbf{S}^H\mathbf{v}_{\mathrm{E}} \tag{19}$$

We then have

$$\begin{aligned}A_{1,n} &= \sqrt{\alpha}\frac{1}{U}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}\; h_{\mathrm{B},n+iN}^{*} \\ A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\mathrm{E},n+iN} \\ A_{3,n} &= \sqrt{1-\alpha}\frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}\; w_{n+iN}\end{aligned} \tag{20}$$

After some mathematical manipulations, we have[4]:

$$\begin{aligned}\mathbb{E}\left[|A_{1,n}|^2\right] &= \frac{\alpha}{U} \\ \mathbb{E}\left[|A_{2,n}|^2\right] &= \sigma_{\mathrm{V,E}}^2 \\ \mathbb{E}\left[|A_{3,n}|^2\right] &= (1-\alpha)\sigma_{\mathrm{AN}}^2\end{aligned} \tag{21}$$

which lead to an ergodic SINR at the unintended position given by:

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

Low performances at Eve are expected with this decoding structure since the despreading operation will not coherently add the received symbol components. It is therefore suboptimal leading to high SR values. This will be confirmed in section 4.2.1.

[3] Neglecting the covariance between $\left|A_{1,n}\right|^2$ and $\left|A_{2,n}+A_{3,n}\right|^2$, as done in the first line of (18), makes the nature of the bound, i.e., lower or upper, obtained for $\mathbb{E}\left[\gamma_{E,n}\right]$ uncertain. However, we have observed by simulations that it remains a lower one for all considered scenarios.

[4] see Appendix A

3.1.2.2 Eve's estimator: matched Filtering

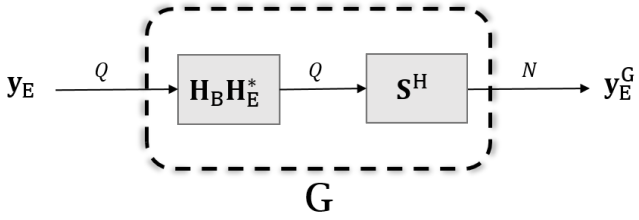

Figure 6: Matched filtering decoding structure

Eve can also perform a matched filtering to maximize its SNR before despreading. If we denote by $\Gamma_E = \mathbf{H}_E\mathbf{H}_B^*\mathbf{S}$, the decoding matrix is then given by: $\mathbf{G} = \Gamma_E^H$. It simply consists in performing a weight multiplication at each subcarrier and then perform despreading as shown in fig.6. This operation is possible since Eve can estimate $\mathbf{H}_E\mathbf{H}_B^*$ while receiving data from Alice. However, it requires more processing resources than the classical receiver of Bob since a processing is performed on the whole bandwidth, i.e., all Q subcarriers. This will lead to more efficient decoding performances at the eavesdropper. The received signal is then:

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

If we compare the received signal at Bob (10) with the received signal at Eve (23), we remark that the data component in (23) will be more amplified than in (10). In fact, we amplify the data by a factor $\frac{U+3}{U}$ in (23), and only by a factor $\frac{U+1}{U}$ in (10)[5]. However, we note that the AN component of the received signal will be amplified with teh matched filtering decoding strategy. With this structure, we have:

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

After computations, the expected values are:

$$\begin{aligned}
\mathbb{E}\left[\left|A_{1,n}\right|^2\right] &= \alpha\frac{U+3}{U} \\
\mathbb{E}\left[\left|A_{2,n}\right|^2\right] &= \sigma_{\mathrm{V,E}}^2 \\
\mathbb{E}\left[\left|A_{3,n}\right|^2\right] &= 2(1-\alpha)\left(\sigma_{\mathrm{AN}}^2 + \mathrm{cov}(\left|\mathbf{w}\right|^2, \left|\mathbf{H}_\mathrm{B}\right|^2)\right)
\end{aligned} \tag{25}$$

The details can be found in Appendix A. We then obtain an ergodic SINR which takes the following form:

$$\mathbb{E}\left[\gamma_{E,n}\right] \gtrapprox \frac{\alpha\frac{U+3}{U}}{\sigma_{\mathrm{V,E}}^2 + 2(1-\alpha)\left(\sigma_{\mathrm{AN}}^2 + \mathrm{cov}(\left|\mathbf{w}\right|^2, \left|\mathbf{H}_\mathrm{B}\right|^2)\right)} \tag{26}$$

3.1.2.3 Eve's estimator: AN killer

Eve can adapt her decoder to kill the AN signal. In fact, by performing $\mathbf{G} = \mathbf{S}^H\mathbf{H}_\mathrm{B}\mathbf{H}_\mathrm{E}^{-1}$, the AN term will become $\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{B}\mathbf{H}_\mathrm{E}^{-1}\mathbf{H}_\mathrm{E}\mathbf{w} = \sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{B}\mathbf{w} = \mathbf{0}$ since it is projected in the null space of

[5] see Appendix A

$\mathbf{S}^H\mathbf{H}_\mathrm{B}$. However, this considers that Eve is able to estimate its own channel $\mathbf{H}_\mathrm{E}$, which is a very strong assumption. If Alice always communicates to Bob using $\mathbf{H}_\mathrm{B}^*$ as a precoder, the data received by Eve is always affected by a term $\mathbf{H}_\mathrm{B}^*\mathbf{H}_\mathrm{E}$ which avoids Eve to estimate $\mathbf{H}_\mathrm{E}$ with classical preamble-based channel estimation methods for instance. However, if an uncoded reference signal is sent by Alice at some point, the Eve might be able to estimate $\mathbf{H}_\mathrm{E}$ (if the channel remains constant between the time at which Alice sends a reference signal and at which Alice sends the $\mathbf{H}_\mathrm{B}^*$-precoded data). It also requires a processing on the full bandwidth, as suggested in fig.7.

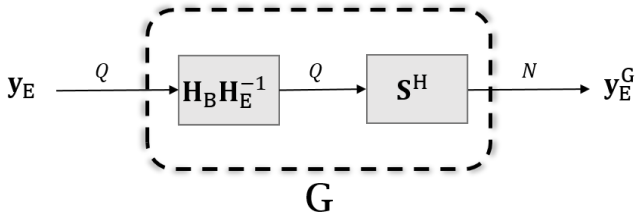

Figure 7: AN killer decoding structure

In that case, the received signal is:

$$\mathbf{y}_\mathrm{E}^G = \sqrt{\alpha}\mathbf{S}^H \left|\mathbf{H}_\mathrm{B}\right|^2 \mathbf{S}\,\mathbf{x} \;+\; \mathbf{S}^H\mathbf{H}_E^{-1}\mathbf{H}_B\,\mathbf{v}_\mathrm{E} \tag{27}$$

The received signal (27) is similar to Bob's one (10) except that the noise term is multiplied by $\mathbf{H}_E^{-1}$ which is not optimal. In fact, if $\mathbf{H}_E$ has low gains at some subcarriers, the noise will be highly amplified. In that situation, we obtain:

$$\begin{aligned} A_{1,n} &= \sqrt{\alpha}\frac{1}{U}\sum_{i=0}^{U-1} \left|h_{\mathrm{B},n+iN}\right|^2 \\ A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}^{-1}\, h_{\mathrm{B},n+iN}\, v_{\mathrm{E},n+iN} \end{aligned} \tag{28}$$

No analytic expression can be found for the expected value of the energy of the noise $\mathbb{E}\left[\left|A_{2,n}\right|^2\right]$ since we have to deal with $\frac{1}{|h_{\mathrm{E},n+iN}|^2}$ which follows an inverse chi-square distribution of $\nu = 2$ degrees of freedom. It therefore has an infinite mean[6]. Only the cumulative distribution function (CDF) of the noise energy can be derived, and consequently the CDF of the SINR for that decoding structure.
For the data symbol, we have:

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

The derivations are found in Appendix A.

3.1.2.4 Eve's estimator: LMMSE

The linear minimum mean square error (LMMSE) equalizer aims to minimize the mean square error (MSE) of the estimated symbol $\hat{\mathbf{x}}_\mathrm{E} = \mathbf{G}\mathbf{y}_\mathrm{E}^G$. The equalizer $\mathbf{G}$ has to fulfill the orthogonality principle which states that the estimator $\hat{\mathbf{x}}_\mathrm{E}$ achieves minimum mean square error (MMSE) if and only if:

$$\mathbb{E}\left[\left(\hat{\mathbf{x}}_\mathrm{E} - \mathbf{x}\right)\left(\mathbf{y}_\mathrm{E}^G\right)^H\right] = \mathbf{0} \tag{30}$$

[6]Intuitively, if one subcarrier has zero gain, which arises from example when two waves arrive with destructive interference, $\frac{1}{|h_{\mathrm{E},n+iN}|^2}$ will tend to infinity. This is why $\mathbb{E}\left[\left|A_{2,n}\right|^2\right] = +\infty$.

From (30), we find an expression of the equalizer as[7]:

$$\mathbf{G} = \sqrt{\alpha}\ \sigma_{\mathrm{X}}^2\ \Gamma_E^H \left(\alpha\ \sigma_{\mathrm{X}}^2\ \Gamma_E \Gamma_E^H + (1-\alpha)\left|\mathbf{H}_{\mathrm{E}}\right|^2 \sigma_{\mathrm{AN}}^2 + \sigma_{\mathrm{V,E}}^2 \mathbf{I}_{\mathrm{Q}}\right)^{-1} \tag{31}$$

where $\sigma_{\mathrm{X}}^2 \mathbf{I}_{\mathrm{N}} = \mathbb{E}\left[\mathbf{x}\mathbf{x}^H\right]$. We remark from (31) that the implementation of the LMMSE requires at Eve the knowledge of $\mathbf{H}_{\mathrm{E}}$ as well as the *AN* energy σ_{AN}^2
So far, no analytic expression of the SINR has been found for the LMMSE implementation.

3.2 Optimal amount of AN to inject

This section is only dedicated for the scenario where Eve has the same capabilities as Bob. This is subject to further completion where the different decoding structures will be included.

With (14), (17) and (22), it is possible to obtain a closed-form approximation of the SR upper bound and therefore to determine the amount of AN energy to inject that maximizes the SR. If we introduce: $T_1 = U(U+1)\sigma_{\mathrm{AN}}^2$, $T_2 = U(U+1)(\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{AN}}^2) - U^2\sigma_{\mathrm{B}}^2\sigma_{\mathrm{AN}}^2$, $T_3 = U(\sigma_{\mathrm{B}}^2 + \sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{AN}}^2)$, and $T_4 = U\sigma_{\mathrm{B}}^2(1 - U\sigma_{\mathrm{AN}}^2)$, we obtain[8]:

$$C_s \lessapprox \log_2\left(\frac{-\alpha^2 T_1\ +\ \alpha T_2\ +\ T_3}{\alpha T_4\ +\ T_3}\right) \tag{32}$$

To maximize the secrecy rate as a function of the parameter α, we find the zeroes of:

$$\frac{\partial C_s}{\partial \alpha} = \frac{\frac{-\alpha^2 T_1 T_4 - 2\alpha T_1 T_3 + (T_2 T_3 - T_3 T_4)}{(\alpha T_4 + T_3)^2}}{\frac{-\alpha^2 T_1 + \alpha T_2 + T_3}{\alpha T_4 + T_3}\ .\ \ln 2} \tag{33}$$

After some algebraic manipulations, one obtains:

$$\frac{\partial C_s}{\partial \alpha} = 0\ \Leftrightarrow\ \alpha_{opt} = \frac{\pm\sqrt{T_1^2 T_3^2\ +\ T_1 T_2 T_3 T_4\ -\ T_1 T_3 T_4^2}\ -\ T_1 T_3}{T_1 T_4} \tag{34}$$

where only the positive roots are solutions since $\alpha \in [0, 1]$.

3.3 Secrecy rate optimization via waterfilling

From section 3.2, the optimal amount of radiated energy dedicated for the transmission of the data signal is derived. The analytic expression (34) lead to the coefficient α_{opt} that maximizes the ergodic SR of the communication. As a reminder, this is only obtained for the scenario where Eve and Bob present the same decoding capabilities. Before despreading, the received signals at Bob and Eve are respectively given by:

$$\begin{aligned} \mathbf{y}_{\mathrm{B}} &= \sqrt{\alpha_{\mathrm{opt}}}\ \left|\mathbf{H}_{\mathrm{B}}\right|^2 \mathbf{S}\ \mathbf{x}\ +\ \mathbf{v}_{\mathrm{B}} \\ \mathbf{y}_{\mathrm{E}} &= \sqrt{\alpha_{\mathrm{opt}}}\ \mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\ \mathbf{x}\ +\ \sqrt{1-\alpha_{\mathrm{opt}}}\ \mathbf{H}_{\mathrm{E}}\mathbf{w}\ +\ \mathbf{v}_{\mathrm{E}} \end{aligned} \tag{35}$$

We observe from (35) that an unique coefficient α_{opt} weights the Q components of the useful data. That is, each subcarrier will be affected by the same coefficient. However, we know that the channel capacity at one subcarrier is proportional to the subcarrier energy. Therefore, subcarriers with higher gains will contribute more to the total channel capacity than subcarriers with lower gains. We also consider

[7] see Appendix A
[8] see Appendix B

throughout this paper that Alice can instantaneously estimate Bob's channel but does not have any information about Eve instantaneous CSI such that we can compute the instantaneous capacity at Bob but we only have access to the ergodic capacity at Eve. From this discussion, we can state that, if we could have access to Eve's instantaneous capacity, we could tune the weights at each subcarrier, i.e., applying a different weight at each subcarrier depending on its power, in such a way that it enhances the instantaneous capacity at Bob and it degrades the instantaneous capacity at the eavesdropper position.

Since we only have access to the ergodic capacity at Eve, we proceed as follows:
Based on the statistics of Bob and Eve channels, we obtain a closed form expression of the ergodic SR given by (32). From that, we find via (34) the value of α_{opt} that, in the ergodic sense, will maximize the SR. Then, at each channel realization, we determine a new set of coefficients, denoted by $\boldsymbol{\alpha}_{\text{w}} = [\alpha_{\text{w},0}, ..., \alpha_{\text{w},Q-1}]^T$, that enhances the instantaneous capacity at Bob while ensuring that:

1. The total radiated energy should remain constant:

$$\left|\sqrt{\alpha_{\text{opt}}}\,\mathbf{H}_{\text{B}}^{*}\mathbf{S}\mathbf{x} + \sqrt{1-\alpha_{\text{opt}}} \odot \mathbf{w}\right|^2 = \left|\sqrt{\boldsymbol{\alpha}_{\text{w}}}\,\mathbf{H}_{\text{B}}^{*}\mathbf{S}\mathbf{x} + \sqrt{1-\boldsymbol{\alpha}_{\text{w}}}\mathbf{w}\right|^2 \tag{36}$$

2. The energy radiated dedicated to the AN signal should remain constant:

$$\left|\sqrt{1-\alpha_{\text{opt}}}\mathbf{w}\right|^2 = \left|\sqrt{1-\boldsymbol{\alpha}_{\text{w}}} \odot \mathbf{w}\right|^2 \tag{37}$$

3. The AN signal should still lie in the null space of Bob:

$$\mathbf{S}^{H}\mathbf{H}_{\text{B}}\sqrt{1-\boldsymbol{\alpha}_{\text{w}}} \odot \mathbf{w} < \epsilon \tag{38}$$

Since we consider that Bob and Eve channels are independent, optimizing the coefficients that weight each subcarrier to enhance the capacity at Bob will not modify the capacity at Eve. In doing so, with the waterfilling optimization procedure, the SR will increase as it will be shown in section 4.2.3. However it is worth to note that this approach is computationally expensive since new weights have to be determined at each channel realization

4 Simulation Results

A 256-subcarrier SISO OFDM system is considered. Bob and Eve channels are assumed to be uncorrelated. Each subcarrier is Rayleigh distributed and there is no correlation between subcarriers. As a reminder, the overall channel energies are normalized to unity for each channel realization. Bob's CSI is assumed to be perfectly known at Alice. Bob and Eve have the same level of noise. Simulations with 100 channel realizations and 300 OFDM blocks were performed using a 4-QAM modulation scheme.

4.1 Decoding results

The presented results in this section were obtained for the scenario where Eve has the same capabilities as Bob. This is subject to further completion where the different decoding structures will be included.
Fig. 8 and 9 show the system performance in terms of BER obtained after ZF equalization at Bob and Eve. In Fig. 8, the BER is plotted as a function of E_b/N_0, where E_b is the energy per bit, calculated after spreading, and N_0 is the noise power spectral density. Different levels of AN energy are investigated at fixed BOR. It can be observed that, as soon as a small amount of radiated energy is dedicated to AN, e.g., 5%, Eve's BER strongly increases. At the intended position, the BER also increases but much

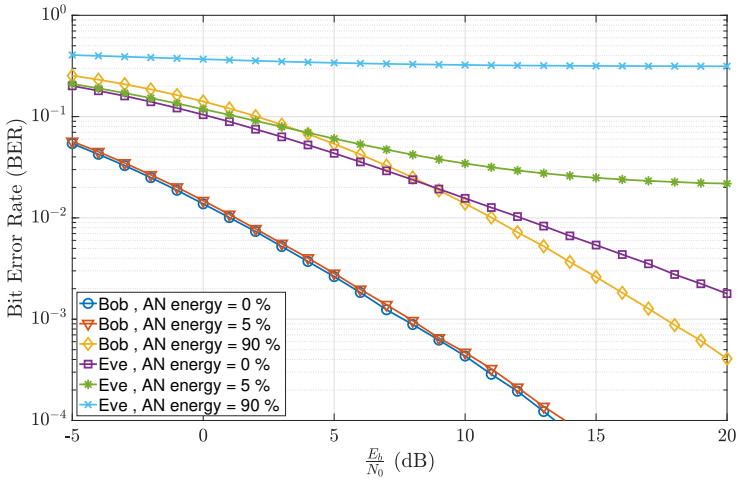

Figure 8: BER as a function of the level of noise for different AN energy values, BOR = 4

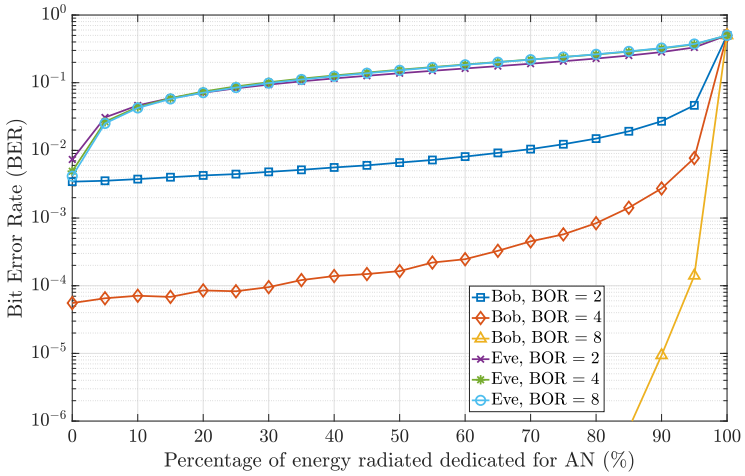

Figure 9: BER as a function of AN energy for different BOR values, $E_b/N_0 = 15$dB

slower. The reason is that the higher the percentage of energy dedicated to AN, the lower the received useful signal power at Bob. In Fig. 9, the BER is plotted as a function of the AN energy, at fixed $E_b/N_0 = 15$ dB and different BOR values. At the unintended position, the BER naturally increases with the amount of injected AN, whatever the BOR value. At Bob, low BER values can be maintained for high AN power by increasing the BOR. One can notice that, when $\alpha \to 0$, the BER curves all converge to 0.5, as expected.

4.2 Secrecy results

4.2.1 Eve and Bob with identical capacities

Fig. 10 shows the SR evolution as a function of α for different BOR values. It is considered that Eve's receiver is equivalent to Bob's one. First, it can be seen that analytic curves, given by (32), approximate well the simulation curves and remains a tight upper bound for all scenarios. In addition, the SR obtained with the classical FD TR SISO OFDM system, i.e., no AN signal, is enhanced with the addition of AN except for very high percentages of AN. Furthermore, the SR increases when the BOR becomes higher because the TR gain becomes larger at Bob for higher BOR values but not at Eve. No more secrecy is obtained when $\alpha \to 0$, since the SINR's at Bob and Eve drop to zero.

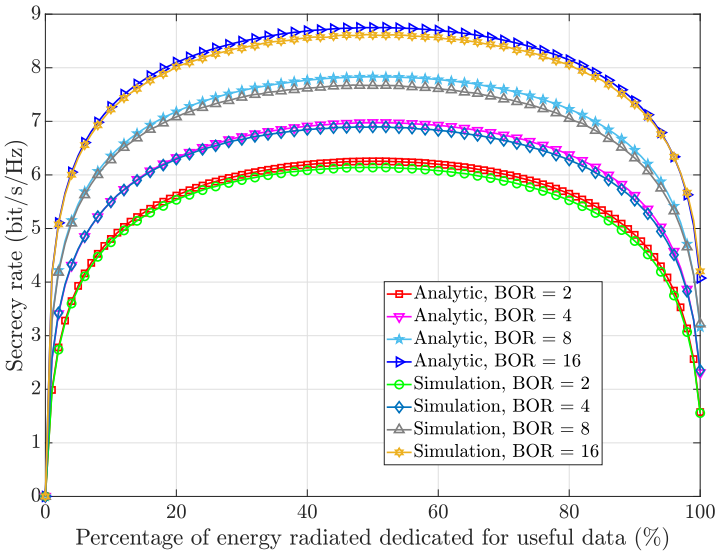

Figure 10: Secrecy Rate curves, analytic vs simulation, Bob and Eve with same capabilities, $E_b/N_0 = 20$ dB

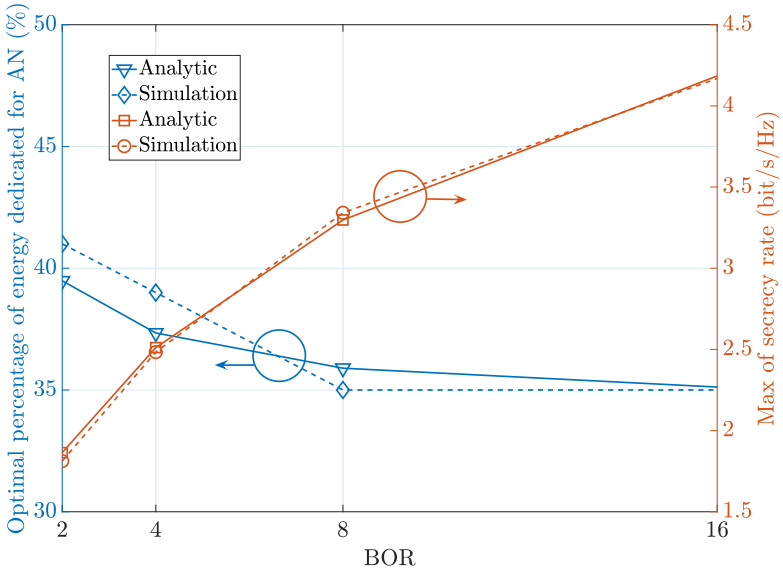

Figure 11: Optimal amount of AN to inject, Bob and Eve with same capabilities, $E_b/N_0 = 5$ dB

Fig. 11 illustrates the values of α_{opt} given by (34) that maximize the SR determined from the closed-form approximation (32), as well as obtained from the numerical simulations. The analytic estimation of the optimal amount of AN energy is not perfect but, the resulting simulated SR is very close to the maximal SR. The reason can be observed in Fig. 10 where the SR varies very slowly about its maximum when α changes. So, for a given BOR value, Alice can make a rough determination of α_{opt} and therefore the available SR, if E_b/N_0 is known.

4.2.2 Comparison between the different decoding structures

Fig.12 shows the secrecy performances for the 4 different structures implemented at the eavesdropper position, each of them assuming more computational resources and/or more knowledges at Eve as compared to Bob. It can be seen that when Eve implements the same receiving structure as Bob, the SR is very high compared to the other curves, as anticipated from Section 3.1.2.1. When the AN killer

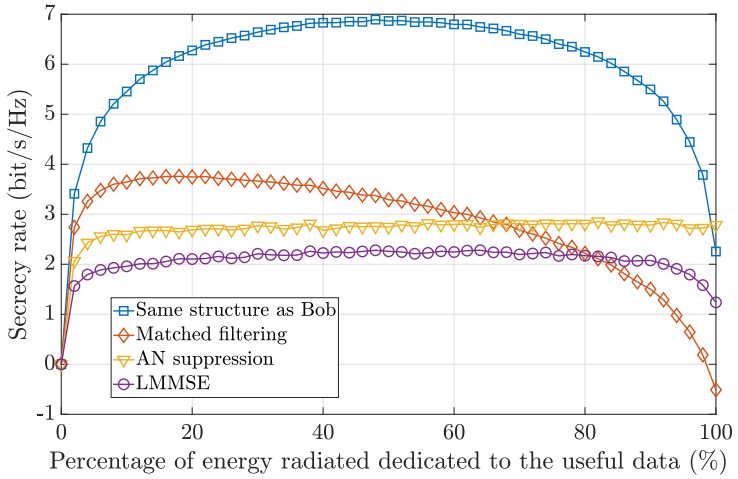

Figure 12: Secrecy Rate curves for the different decoding structures at Eve, $E_b/N_0 = 20$ dB, BOR = 4

algorithm is implemented, we observe that the curve remains flat, except for the situation where all the radiated energy is dedicated for the AN signal. The reason is that Eve's noise is amplify whatever the value of α since the AN signal is suppressed. The LMMSE curves exhibit the lower SR sice it performs a decoding tradeoff between suppressing the AN and amplifying its noise, except for very high percentages of energy dedicated to the useful signal. Finally, we note that the SR when Eve implements a matched filter is relatively low. Furthermore, it becomes negative when the transmitted signal only contains data. In fact, if Eve and Bob noise levels are identical, which is assumed throughout this report , the SINR ratio when no AN is radiated becomes:

$$\kappa \approx \frac{\mathbb{E}\left[\gamma_{B,n}\right]}{\mathbb{E}\left[\gamma_{E,n}\right]}\bigg|_{\alpha\to 1} \approx \frac{\frac{U+1}{U}}{\left(\frac{U+1}{U}\right)^2} = \frac{U}{U+1} < 1 \tag{39}$$

giving rise to a negative SR. The reason why the LMMSE decoding structure does not exhibit better decoding performances at Eve, i.e., lower SR values, compared to the matched filter receiver for all values of α has not been explained yet.

4.2.3 Waterfilling Optimization

Fig. 13 presents the maximal values of the SR obtained when Eve implements the despreading only receiving structure, i.e. the same structure as Bob, before and after waterfilling optimization. As a reminder, before and after optimization, the mean energy radiated dedicated to the useful data remains unchanged. This amount of energy is computed thanks to (34) in order to ensure a maximal SR. This SR is then further increased via the waterfilling optimization procedure, as described in section 3.3. As we can see, there is an increase of the SR for all BOR values thanks to the optimization. However, this increase decreases with an increase of the BOR. This can be explained since, when the BOR increases, the channel frequency diversity is better exploited by the TR scheme. Therefore, it becomes more difficult to gain from the coefficient optimization procedure and the SR is then less enhanced.

5 Conclusion & Perspectives

The problem of securing the FD TR SISO OFDM wireless transmission from a transmitter to a legitimate receiver in the presence of a passive eavesdropper is considered. A novel and original approach based on the addition of an AN signal onto OFDM blocks that improves the PLS is proposed. This approach can

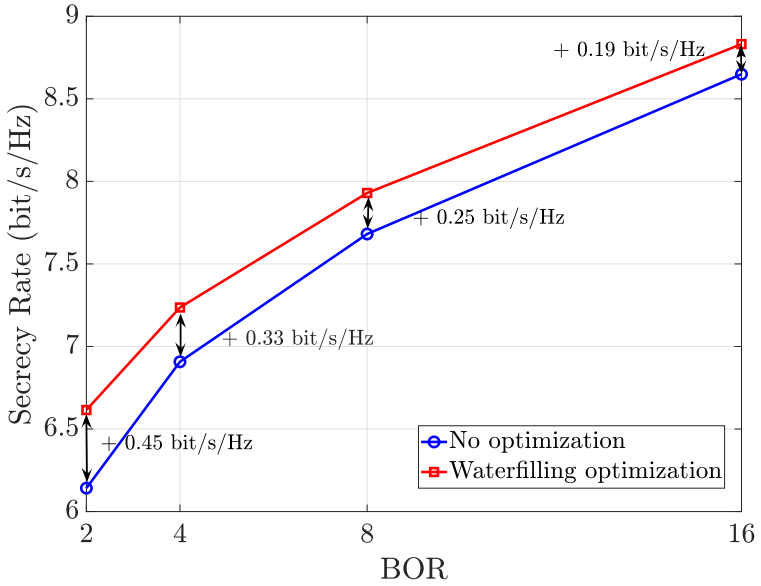

Figure 13: SR optimization via waterfilling, Bob and Eve with same capabilities, $E_b/N_0 = 20$ dB

be easily integrated into existing standards based on OFDM. It only requires a single transmit antenna and is therefore well suited for devices with limited capabilities. Analytic and simulation results show that the novel approach significantly improves the security of the communication and so considerably jeopardizes any attempt of an eavesdropper to retrieve the data.

In this work, four eavesdropper decoding structures are investigated giving rise to different secrecy performances. From the previous discussion, we remark that a simple matched filtering decoding structure strongly impacts the secrecy rate of the communication. As a result, one of the aspects of the future work will be to implement a more robust scheme. New AN injection methods and/or new precoding techniques will be investigated to try to further improve the security of the communication.

So far, only a SISO system has been considered. A natural extension of the work will be to consider a MIMO system. That way, in addition to benefiting from the frequency diversity of the channels, we will benefit from the spatial diversity. In doing so, any attempt to try to eavesdrop the data will be expected to become harder. In addition, we will consider that the passive eavesdropper will be equipped with multiple antennas which will gives him more decoding capabilities.

Furthermore, only a single-user communication is now considered. A multi-users scheme can be designed where each user channel can contribute to secure the whole communication. As a consequence, the level of security of the scheme is expected to improve.

At this point of the work, a very simple channel model was implemented. In fact, a multi-taps channel where each tap is Rayleigh distributed is considered. No correlation between the different subcarriers, i.e. frequency correlation, or spatial correlation between Bob and Eve channels have been taken into account. This leads to results that are relatively easy to compare with analytic models but that do not represent well real life scenarios. A natural extension of the work will be to consider these correlations in order to obtain more realistic results.

Finally, the objective will be to test the FD TR OFDM system with the Universal Software Radio Peripheral (USRP) devices in real indoor environments.

Appendices

A SINR derivation

Let A and B be 2 RV's. These basics properties will be used:

$$\begin{aligned}
&\mathbb{E}\left[\alpha A + \beta B\right] = \alpha\mathbb{E}\left[A\right] + \beta\mathbb{E}\left[B\right] \quad \alpha, \beta \in \mathbb{R} \\
&\mathbb{E}\left[AB\right] = \mathbb{E}\left[A\right]\mathbb{E}\left[B\right] \quad \text{if } A \text{ and } B \text{ are independent} \\
&\mathbb{E}\left[AB\right] = \mathbb{E}\left[A\right]\mathbb{E}\left[B\right] + \mathrm{cov}(A, B) \quad \text{if } A \text{ and } B \text{ are correlated}
\end{aligned} \tag{A.1}$$

A.1 At the intended position

As a recall, the received sequence is given by:

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

From (15) and (16), we have:

$$\mathbb{E}\left[|k|^2\right] = \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}^{2}\right|\mathbf{S}\right|^{2}\right] \tag{A.3a}$$

$$\mathbb{E}\left[|k_n|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2\right|^2\right] \tag{A.3b}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2\right)\left(\sum_{j=0}^{U-1}|h_{\mathrm{B},n+jN}|^2\right)^{H}\right] \tag{A.3c}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{j=0}^{U-1}|h_{\mathrm{B},n+iN}|^2\,|h_{\mathrm{B},n+jN}^{*}|^2\right] \tag{A.3d}$$

$$= \frac{\alpha}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^4 + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},n+iN}|^2\,|h_{\mathrm{B},n+jN}^{*}|^2\right] \tag{A.3e}$$

$$= \frac{\alpha}{U^2}\left(\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^4\right] + \mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},n+iN}|^2\,|h_{\mathrm{B},n+jN}^{*}|^2\right]\right) \tag{A.3f}$$

$$= \frac{\alpha}{U^2}\left(\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^4\right] + \mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{B},n+iN}|^2\right]\mathbb{E}\left[\sum_{\substack{j=0\\j\neq i}}^{U-1}|h_{\mathrm{B},n+jN}^{*}|^2\right]\right) \tag{A.3g}$$

$$= \frac{\alpha}{U^2}\left(2U + U(U-1)\right) = \frac{\alpha(U+1)}{U} \tag{A.3h}$$

Going from (A.3g) to (A.3h) arises from the fact that $\mathbb{E}\left[xf(x)\right] = \mathbb{E}\left[\frac{\partial f(x)}{\partial x^*}\right]$. It is then easy to show that $\mathbb{E}\left[|h_{\mathrm{B},n+iN}|^4\right] = 2$.

For the data symbol we have by definition $\mathbb{E}\left[|x_n|^2\right] = 1$, and for the noise symbol, we obtain:

$$\mathbb{E}\left[|\mathbf{v}_{\mathrm{B}}|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_{\mathrm{B}}\right|^2\right] \tag{A.4a}$$

$$= \mathbb{E}\left[\left(\mathbf{S}^H\mathbf{v}_{\mathrm{B}}\right)\left(\mathbf{S}^H\mathbf{v}_{\mathrm{B}}\right)^H\right] \tag{A.4b}$$

$$= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_{\mathrm{B}}\mathbf{v}_{\mathrm{B}}^*\mathbf{S}\right] \tag{A.4c}$$

$$\mathbb{E}\left[|v_{\mathrm{B,n}}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{B},n+iN}|^2\right] = \sigma^2_{\mathrm{V,B}} \tag{A.4d}$$

A.2 At the unintended position

At the unintended position, the received signal is given by:

$$\mathbf{y}_{\mathrm{E}}^G = \sqrt{\alpha}\mathbf{G}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}} \tag{A.5}$$

where $\Gamma_{\mathrm{E}} = \mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}$

A.2.1 Eve and Bob with identical capacities

In this scenario, we have:

$$\mathbf{y}_{\mathrm{E}}^G = \sqrt{\alpha}\mathbf{S}^H\Gamma_{\mathrm{E}}\mathbf{S}\,\mathbf{x} \;+\; \sqrt{1-\alpha}\,\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w} \;+\; \mathbf{S}^H\mathbf{v}_{\mathrm{E}} \tag{A.6}$$

From (21), we have:

$$\mathbb{E}\left[|\mathbf{A}_1|^2\right] = \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\right|^2\right] \tag{A.7a}$$

$$= \alpha\mathbb{E}\left[\left(\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\right)\left(\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^*\mathbf{S}\right)^H\right] \tag{A.7b}$$

$$\mathbb{E}\left[|A_{1,n}|^2\right] = \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}|^2\left|h_{\mathrm{B},n+iN}^*\right|^2\right] \tag{A.7c}$$

$$= \frac{\alpha}{U} \tag{A.7d}$$

For the noise component:

$$\mathbb{E}\left[|\mathbf{A}_2|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_{\mathrm{E}}\right|^2\right] \tag{A.8a}$$

$$= \mathbb{E}\left[\left(\mathbf{S}^H\mathbf{v}_{\mathrm{E}}\right)\left(\mathbf{S}^H\mathbf{v}_{\mathrm{E}}\right)^H\right] \tag{A.8b}$$

$$= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_{\mathrm{E}}\mathbf{v}_{\mathrm{E}}^*\mathbf{S}\right] \tag{A.8c}$$

$$\mathbb{E}\left[|A_{2,n}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{E},n+iN}|^2\right] = \sigma^2_{\mathrm{V,E}} \tag{A.8d}$$

The AN term is given by:

$$\mathbb{E}\left[|\mathbf{A}_3|^2\right] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w}\right|^2\right] \tag{A.9a}$$

$$= (1-\alpha)\mathbb{E}\left[\left(\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w}\right)\left(\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{w}\right)^H\right] \tag{A.9b}$$

$$= (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*\mathbf{w}\mathbf{w}^*\mathbf{S}\right] \tag{A.9c}$$

$$\mathbb{E}\left[|A_{3,n}|^2\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}w_{n+iN}|^2\right] = (1-\alpha)\sigma^2_{\mathrm{AN}} \tag{A.9d}$$

A.2.2 Matched Filtering

When Eve performs a matched filtering with the received signal, we obtain:

$$\mathbf{y}_{\mathrm{E}}^{G} = \sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\,\mathbf{x} \;+\; \sqrt{1-\alpha}\,\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\mathbf{w} \;+\; \mathbf{S}^{H}\mathbf{H}_{E}^{*}\mathbf{H}_{B}\,\mathbf{v}_{\mathrm{E}} \tag{A.10}$$

The data component is given by:

$$\mathbb{E}\left[\left|\mathbf{A}_{1}\right|^{2}\right] = \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\,\mathbf{x}\right|^{2}\right] \tag{A.11a}$$

$$= \alpha\mathbb{E}\left[\left|\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\right|^{2}\right]\mathbb{E}\left[\left|\mathbf{x}\right|^{2}\right] \tag{A.11b}$$

$$\mathbb{E}\left[\left|A_{1,n}\right|^{2}\right] = \alpha\mathbb{E}\left[\left|\frac{1}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{2}\right|^{2}\right] \tag{A.11c}$$

$$= \frac{\alpha}{U^{2}}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{2}\right)\left(\sum_{j=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{2}\right)^{H}\right] \tag{A.11d}$$

$$= \frac{\alpha}{U^{2}}\mathbb{E}\left[\sum_{i=0}^{U-1}\sum_{j=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{2}\left|h_{\mathrm{B},n+jN}^{*}\right|^{2}\left|h_{\mathrm{E},n+iN}^{*}\right|^{2}\right] \tag{A.11e}$$

$$= \frac{\alpha}{U^{2}}\left(\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^{4}\left|h_{\mathrm{E},n+iN}\right|^{4} + \sum_{i=0}^{U-1}\sum_{\substack{j=0\\ j\neq i}}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{2}\left|h_{\mathrm{B},n+jN}^{*}\right|^{2}\left|h_{\mathrm{E},n+iN}^{*}\right|^{2}\right) \tag{A.11f}$$

$$= \frac{\alpha}{U^{2}}\left(U.2.2 + U(U-1)\right) = \frac{\alpha(U+3)}{U} \tag{A.11g}$$

We remark that (A.11d) can be directly computed from (A.3c), which leads to (A.11g).

The noise component is:

$$\mathbb{E}\left[\left|\mathbf{A}_{2}\right|^{2}\right] = \mathbb{E}\left[\left|\mathbf{S}^{H}\mathbf{H}_{\mathrm{E}}^{*}\mathbf{H}_{\mathrm{B}}\mathbf{v}_{\mathrm{E}}\right|^{2}\right] \tag{A.12a}$$

$$= \mathbb{E}\left[\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{E}}^{*}\mathbf{H}_{\mathrm{B}}\mathbf{v}_{\mathrm{E}}\right)\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{E}}^{*}\mathbf{H}_{\mathrm{B}}\mathbf{v}_{\mathrm{E}}\right)^{H}\right] \tag{A.12b}$$

$$= \mathbb{E}\left[\mathbf{S}^{H}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^{*}\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{B}}^{*}\mathbf{v}_{\mathrm{E}}\mathbf{v}_{\mathrm{E}}^{*}\mathbf{S}\right] \tag{A.12c}$$

$$\mathbb{E}\left[\left|A_{2,n}\right|^{2}\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^{2}\left|h_{\mathrm{B},n+iN}\right|^{2}\left|v_{\mathrm{E},n+iN}\right|^{2}\right] = \sigma_{\mathrm{V,E}}^{2} \tag{A.12d}$$

The AN component is:

$$\mathbb{E}\left[\left|\mathbf{A}_{3}\right|^{2}\right] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\,\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\mathbf{w}\right|^{2}\right] \tag{A.13a}$$

$$= (1-\alpha)\mathbb{E}\left[\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\mathbf{w}\right)\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\mathbf{w}\right)^{H}\right] \tag{A.13b}$$

$$\mathbb{E}\left[\left|A_{3,n}\right|^{2}\right] = \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^{2}\left|h_{\mathrm{E},n+iN}\right|^{4}\left|w_{n+iN}\right|^{2}\right] \tag{A.13c}$$

$$= 2(1-\alpha)\left(\sigma_{\mathrm{AN}}^{2} + \mathrm{cov}(\left|\mathbf{w}\right|^{2}, \left|\mathbf{H}_{\mathrm{B}}\right|^{2})\right) \tag{A.13d}$$

Since the AN signal and Bob channel are not independent, we cannot compute the expectations in (A.13c) separately. This is why we have to add the covariance in (A.13d).

A.2.3 AN suppression

In this scenario, the received signal at Eve is given by:

$$\mathbf{y}_{\mathrm{E}}^{G} = \sqrt{\alpha}\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\mathbf{S}\,\mathbf{x} \;+\; \mathbf{S}^{H}\mathbf{H}_{\mathrm{E}}^{-1}\mathbf{H}_{B}\,\mathbf{v}_{\mathrm{E}} \tag{A.14}$$

In what concerns the data component, the computation is straightforward since it is similar to (A.3). We then obtain $\mathbb{E}\left[|A_{1,n}|^2\right] = \alpha\frac{U+1}{U}$.
The noise term is:

$$\mathbb{E}\left[|\mathbf{A}_2|^2\right] = \mathbb{E}\left[\left|\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^{-1}\mathbf{v}_{\mathrm{E}}\right|^2\right] \tag{A.15a}$$

$$= \mathbb{E}\left[\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^{-1}\mathbf{v}_{\mathrm{E}}\right)\left(\mathbf{S}^{H}\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{E}}^{-1}\mathbf{v}_{\mathrm{E}}\right)^{H}\right] \tag{A.15b}$$

$$= \mathbb{E}\left[\mathbf{S}^{H}\left|\mathbf{H}_{\mathrm{B}}\right|^{2}\left|\mathbf{H}_{\mathrm{E}}^{-1}\right|^{2}\left|\mathbf{v}_{\mathrm{E}}\right|^{2}\mathbf{S}\right] \tag{A.15c}$$

$$\mathbb{E}\left[|A_{2,n}|^2\right] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}^{-1}|^2|h_{\mathrm{B},n+iN}|^2|v_{\mathrm{E},n+iN}|^2\right] \tag{A.15d}$$

$$= \sigma_{\mathrm{V,E}}^2\,\mathbb{E}\left[|h_{\mathrm{E},n+iN}^{-1}|^2\right] = \sigma_{\mathrm{V,E}}^2\,\mathbb{E}\left[\frac{1}{|h_{\mathrm{E},n+iN}|^2}\right] \tag{A.15e}$$

The issue that arises in (A.15e) is that the variable $X = \frac{1}{|h_{\mathrm{E},n+iN}|^2}$ follows an inverse chi-square distribution of $\nu = 2$ degrees of freedom. The expected value of such a distribution is given by:

$$\mathbb{E}\left[X\right] = \frac{1}{\nu-2} = +\infty \tag{A.16}$$

Eq. (A.16) suggests that the expected value of the energy of the noise component is infinite which implies that the ergodic SINR at Eve tends to zero and that the ergodic SR of the communication tends to the ergodic capacity of Bob. However, this is only the case when $|h_{\mathrm{E},n+iN}|^2 = 0$, i.e. when a subcarrier of Eve's channel has a zero gain. From (A.15), we clearly understand that this decoding structure will amplify the noise component which is not optimal, as already anticipated from section 3.1.2.3. However, we can compute the probability p that our RV X is bigger that a certain threshold t, i.e., we can compute the upper-bound value of the SR with a given probability. The probability density function (PDF) of X has the form:

$$f_X(x) = \frac{2^{-\nu/2}}{\Gamma(\nu/2)}x^{-\nu/2-1}e^{\frac{-1}{2x}} \tag{A.17}$$

where $\Gamma(a) = (a-1)! = \int_0^\infty z^{a-1}e^{-z}dz$ is the Gamma function of the integer a. The probability that our RV X is bigger than t is given by:

$$\begin{aligned} Pr(t < X) &= \int_t^{+\infty} f_X(x)dx = p \\ \Leftrightarrow\; p &= \int_t^{+\infty}\frac{2^{-1}}{\Gamma(1)}x^{-2}e^{\frac{-1}{2x}}dx \\ \Leftrightarrow\; p &= \int_{1/t}^{0} e^{-u/2}du \\ \Leftrightarrow\; p &= 1 - e^{\frac{-1}{2t}} \\ \Leftrightarrow\; t &= \frac{-2}{\ln\left(1-p\right)} \end{aligned} \tag{A.18}$$

This relation is plotted in fig.A.1 where we see that we have for example a probability of $p = 5\%$ that our decoding structure will amplify the noise component by a factor $t = 27$.

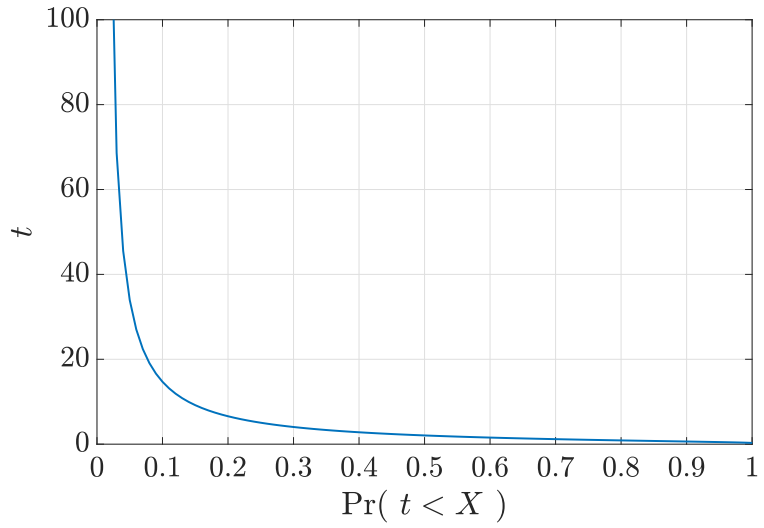

Figure A.1: CDF of the inverse chi-square distribution of $\nu = 2$ degrees of freedom.

A.2.4 LMMSE

As a recall, the LMMSE equalizer $\mathbf{G}$ needs to satisfy the orthogonality principle. In doing so, we have:

$$\mathbb{E}\left[(\hat{\mathbf{x}}_{\mathrm{E}} - \mathbf{x})\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbf{0} \tag{A.19a}$$

$$\Leftrightarrow \mathbb{E}\left[(\mathbf{G}\mathbf{Y}_{\mathrm{E}} - \mathbf{x})\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbf{0} \tag{A.19b}$$

$$\Leftrightarrow \mathbb{E}\left[\mathbf{G}\mathbf{Y}_{\mathrm{E}}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] = \mathbb{E}\left[\mathbf{x}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right] \tag{A.19c}$$

$$\Leftrightarrow \mathbf{G} = \mathbb{E}\left[\mathbf{x}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right]\left(\mathbb{E}\left[\mathbf{Y}_{\mathrm{E}}\mathbf{y}_{\mathrm{E}}^{\mathrm{H}}\right]\right)^{-1} \tag{A.19d}$$

$$\begin{aligned}\Leftrightarrow \mathbf{G} = {} & \mathbb{E}\left[\mathbf{x}\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)^{H}\right] \\ & \left(\mathbb{E}\left[\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)\left(\sqrt{\alpha}\Gamma_{\mathrm{E}}\mathbf{x} + \sqrt{1-\alpha}\mathbf{H}_{\mathrm{E}}\mathbf{w} + \mathbf{v}_{\mathrm{E}}\right)^{H}\right]\right)^{-1}\end{aligned} \tag{A.19e}$$

$$\begin{aligned}\Leftrightarrow \mathbf{G} = {} & \left(\sqrt{\alpha}\mathbb{E}\left[\mathbf{x}\mathbf{x}^{H}\Gamma_{\mathrm{E}}^{H}\right] + \sqrt{1-\alpha}\mathbb{E}\left[\mathbf{x}\mathbf{w}^{H}\mathbf{H}_{\mathrm{E}}^{H}\right] + \mathbb{E}\left[x\mathbf{v}_{\mathrm{E}}^{H}\right]\right) \\ & \left(\mathbb{E}\left[\alpha\Gamma_{\mathrm{E}}\Gamma_{\mathrm{E}}^{H}\mathbf{x}\mathbf{x}^{H} + (1-\alpha)\mathbf{H}_{\mathrm{E}}\mathbf{w}\mathbf{w}^{H}\mathbf{H}_{\mathrm{E}}^{H} + \mathbf{v}_{\mathrm{E}}\mathbf{v}_{\mathrm{E}}^{H}\right]\right)^{-1}\end{aligned} \tag{A.19f}$$

$$\Leftrightarrow \mathbf{G} = \sqrt{\alpha}\sigma_{\mathrm{X}}^{2}\Gamma_{\mathrm{E}}^{H}\left(\alpha\sigma_{\mathrm{X}}^{2}\Gamma_{\mathrm{E}}\Gamma_{\mathrm{E}}^{H} + (1-\alpha)\left|\mathbf{H}_{\mathrm{E}}\right|^{2}\sigma_{\mathrm{AN}}^{2} + \sigma_{\mathrm{VE}}^{2}\mathbf{I}_{N}\right)^{-1} \tag{A.19g}$$

B Optimal amount of AN to inject derivation

As a recall, the SINR at Bob and Eve are respectively given by:

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

The SR becomes:

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

$$\Leftrightarrow C_s = \log_2\left(\frac{\alpha(U+1) + U\sigma^2_{\mathrm{V,B}}}{U\sigma^2_{\mathrm{V,B}}}\right) - \log_2\left(\frac{\alpha + U\sigma^2_{\mathrm{V,E}} + (1-\alpha)U\sigma^2_{\mathrm{AN}}}{U\sigma^2_{\mathrm{V,E}} + (1-\alpha)U\sigma^2_{\mathrm{AN}}}\right) \tag{B.2b}$$

$$\Leftrightarrow C_s = \log_2\left(\frac{-\alpha^2(U+1)U\sigma^2_{\mathrm{AN}} + \alpha\left[U(U+1)(\sigma^2_{\mathrm{V,E}} + \sigma^2_{\mathrm{AN}}) - U^2\sigma^2_{\mathrm{V,B}}\sigma^2_{\mathrm{AN}}\right] + U(\sigma^2_{\mathrm{V,B}} + \sigma^2_{\mathrm{V,E}} + \sigma^2_{\mathrm{AN}})}{\alpha U\sigma^2_{\mathrm{V,B}}(1 - U\sigma^2_{\mathrm{AN}}) + U(\sigma^2_{\mathrm{V,B}} + \sigma^2_{\mathrm{V,E}} + \sigma^2_{\mathrm{AN}})}\right) \tag{B.2c}$$

If we introduce $T_1 = (U+1)U\sigma^2_{\mathrm{AN}}$, $T_2 = U(U+1)(\sigma^2_{\mathrm{V,E}} + \sigma^2_{\mathrm{AN}}) - U^2\sigma^2_{\mathrm{V,B}}\sigma^2_{\mathrm{AN}}$, $T_3 = U(\sigma^2_{\mathrm{V,B}} + \sigma^2_{\mathrm{V,E}} + \sigma^2_{\mathrm{AN}})$, and $T_4 = U\sigma^2_{\mathrm{V,B}}(1 - U\sigma^2_{\mathrm{AN}})$, we come back to (32).