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

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

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

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

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

***Abstract*—The abstract goes here.**

***Index Terms*—Communications Society, IEEE, IEEEtran, journal, LaTeX, paper, template.**

I. Introduction

THIS demo file is intended to serve as a “starter file” for IEEE Communications Society journal papers produced under LaTeX using IEEEtran.cls version 1.8b and later. I wish you the best of success.

II. System Model

A. Handshake Protocol

Prior to the transmission of secure data between Alice and Bob, a handshake protocol must take place. Depending on the handshake, Eve will have different knowledges about the communication parameters which will lead to different decoding capabilities and so, different security performances.

In this paper, we consider a Fast Fading (FF) Time-Division Duplex (TDD) communication. In doing so, we will investigate 3 different decoding schemes at Eve depending on weither Alice or Bob wants to first establish the secure communication. The FF hypothesis means that each OFDM block sent by Alice will experience a different channel realization. The TDD hypothesis implies that channel reciprocity between Alice and Bob or Alice and Eve can be used.

The first investigated situation arises when Alice asks first to Bob for secure commnication. In this configuration, she sends an unprecoded pilot to Bob, allowing Eve to estimate her own channel frequency response (CFR) $\mathbf{H}_{\mathrm{E}}$. From that, Bob acknowledges to Alice without need of sending his channel estimation $\mathbf{H}_{\mathrm{B}}$. This comes from the channel reciprocity property in the TDD scheme. Finally, Alice will send precoded data without pilot to Bob. In this configuration, Eve can implement the *"own channel knowledge"* decoding structure since she only has the knowledge of her own channel.

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

The last 2 scenarios appear when Bob first asks to Alice for secure communication. In both cases, Bob sends an unprecoded pilot to Alice allowing her to know Bob’s channel. If Alice only transmits precoded data to Bob, Eve will not be able to know anything about the communication parameters. In that situation, she will implement the "*same decoding structure as Bob*", i.e., she will only despread the received sequence. However, if Alice sends precoded pilot and data to Bob, Eve will know her equivalent channel $\mathbf{H}_{\mathrm{B}}^{*}\mathbf{H}_{\mathrm{E}}$ and will implement the "*matched filtering*" decoding structure.

In the following, these 3 decoding schemes will be investigated.

B. Communication Protocol

When the handshaking between Alice and Bob is established, secure data can be transmitted to Bob. In order to do so, the useful data will be precoded and an AN signal $\mathbf{w}$ will be added to it before transmission, as depicted in fig. 1.

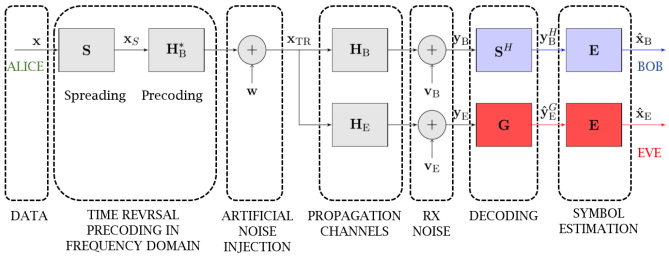

Figure 1. Communication scheme

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 by a factor $U = Q/N$, called back-off rate (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 independent and identically distributed (i.i.d.) in order not to increase the PAPR as suggested in [1]. 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 [2], 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 with $\mathbf{H}_{\mathrm{B}}^*$ before addition of the AN signal and transmission.

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

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

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

In order to precod the data, Alice needs to have the knowledge of Bob CFR. We consider that Alice can perfectly estimate Bob CFR. The channels between Alice and Bob ($\mathbf{H}_{\mathrm{B}}$) and between Alice and Eve ($\mathbf{H}_{\mathrm{E}}$) are assumed to be static during the transmission of one OFDM symbol. However, the CFRs differ between two subsequent OFDM blocks thanks to the FF hypothesis. $\mathbf{H}_{\mathrm{B}}$ and $\mathbf{H}_{\mathrm{E}}$ are $Q \times Q$ diagonal matrices whose elements are $h_{\mathrm{B},q}$ and $h_{\mathrm{E},q}$ (for $q = 0, ..., Q-1$) and follow a zero-mean unit-variance complex normal distribution, i.e., their modulus follow a Rayleigh distribution. We also consider that the overall channel energies are normalized to unity for each channel realization. The precoding matrix $\mathbf{H}_{\mathrm{B}}^*$ is also a diagonal matrix with elements $h_{\mathrm{B},q}^*$. At Bob, a despreading operation is performed by applying $\mathbf{S}^H$. We consider that Bob and Eve know the spreading sequence. Bob will then apply a ZF equalization. As stated in section II-A, 3 decoding structures $\mathbf{G}$ will be investigated at Eve. These different schemes will lead to different level of security performances. After decoding, she also perfoms a ZF equalization. A perfect synchronization is finally assumed at Bob and Eve positions.

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

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

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

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

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

$$\mathbf{w} = \beta\mathbf{V}_2\tilde{\mathbf{w}} \tag{5}$$

which ensures that (3) is satisfied for any arbitrary vector $\tilde{\mathbf{w}} \in \mathbb{C}^{Q-N\times 1}$. Since $Q = NU$, as soon as $U \geq 2$, there is a set of infinite possibilities to generate $\tilde{\mathbf{w}}$ and therefore the AN signal. In the following, we assume that $\tilde{\mathbf{w}}$ is a zero-mean circularly symmetric white complex Gaussian noise with covariance matrix $\mathbb{E}\left[\tilde{\mathbf{w}}(\tilde{\mathbf{w}})^H\right] = \mathbf{I}_{Q-N\times 1}$. The AN signal is then generated thanks to (5) with a weighting coefficient β to have an energy of 1/U.

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

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

where $\mathbf{v}_{\mathrm{B}}$ is the FD complex AWGN. The noise's auto-correlation is $\mathbb{E}\left[|v_{\mathrm{B},n}|^2\right] = \sigma_{\mathrm{V,B}}^2$ and the covariance matrix is $\mathbb{E}\left[(\mathbf{S}^H\mathbf{v}_{\mathrm{B}}).(\mathbf{S}^H\mathbf{v}_{\mathrm{B}})^H\right] = \sigma_{\mathrm{V,B}}^2.\mathbf{I}_N$. We also assume that the data and noise symbols, x_n and $v_{\mathrm{B,n}}$ respectively, are independent of each other. In (6), each transmitted symbol is affected by a real gain at the position of the legitimate receiver. This results from the data precoding at Alice leading to the product $\mathbf{H}_{\mathrm{B}}\mathbf{H}_{\mathrm{B}}^*$ in the received sequence at Bob, which is a real diagonal matrix. The gains differ between each symbol in the OFDM block but increases with an increase of the BOR value as each symbol would be sent on more subcarriers and would benefit from a larger frequency diversity gain. If we consider a fixed bandwidth, the TR focusing effect is enhanced for higher BOR's at the expense of the data rate.

From (6), we observe that 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 (6) since (3) is respected. A ZF equalization is performed at the receiver leading to:

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

From (7), a perfect data recovery is possible in high SNR scenario.

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

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

where $\mathbf{G}$ is a $N \times N$ filter matrix performed by Eve, $\mathbf{v}_{\mathrm{E}}$ is the complex AWGN. The noise auto-correlation is $\mathbb{E}\left[|v_{\mathrm{E,n}}|^2\right] = \sigma^2_{\mathrm{V,E}}$. In (8), $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}$ 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 coefficient, which can be real or complex depending on the decoding structure $\mathbf{G}$. If this coefficient is complex, its magnitude does not depend on the BOR value. It results in an absence of TR gain at the unintended position. As a consequence, worse decoding performance is obtained compared to the intended position. In addition, we observe in (8) a term depending on the AN signal. It results from the precoding at Alice since $\mathbf{G}\mathbf{H}_{\mathrm{E}}\mathbf{w} \neq \mathbf{0}$ in general. This term introduces an interference at Eve and thus scrambles the received constellation even in a noiseless environment. After ZF equalization, the estimated symbols are:

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

Equation (9) shows that the addition of AN in the FD TR SISO OFDM communication can secure the data transmission since a term depending on the AN signal still remains even in high SNR scenarios. It is to be noted that, since $\mathbf{w}$ is generated from an infinite set of possibilities, even if Eve knows its equivalent channel $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{B}}^{*}$ and the spreading sequence, she cannot estimate the AN signal to try retrieving the data. The degree of security will depend on the investigated scenario, i.e., decoding strcture $\mathbf{G}$ at Eve, and the amount of AN energy that is injected into the communication, as it will be explained in Section III.

III. Performance Assessments

The classical metric used to evaluate the degree of secrecy in a communication in the PLS field is the SR.
Parler p-e un peu plus de la strong/weak/perfect secrecy cfr bouquin de info theory + Joao Barrios! Cfr mes notes
The notion of Shannon perfect secrecy 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, [3]. In the ergodic sense, it can be expressed as:

$$\begin{aligned}C_S &= \mathbb{E}\left[\log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right)\right] \quad , \quad \gamma_B > \gamma_E \\ &\leq \log_2\left(1+\mathbb{E}\left[\gamma_B\right]\right) - \log_2\left(1+\mathbb{E}\left[\gamma_E\right]\right)\end{aligned} \tag{10}$$

with γ_B and γ_E being respectively the SINR at Bob and Eve's positions. The inequality in (10) arises from the Jensen's inequality. To estimate the SR of the communication, we observe from (10) that an analytic expression of Bob and Eve SINR must be derived.

A. Hypothesis

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

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

B. SINR determination

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

1) At the intended position: At Bob, a simple despreading operation is performed. As a reminder, due to the precoding at the transmitter side, every transmitted symbol will be affected by a real gain, as expressed in (6). The SINR for the transmitted symbols n is given by:

$$\begin{aligned}\mathbb{E}\left[\gamma_{B,n}\right] &= \mathbb{E}\left[\frac{\left|\sqrt{\alpha}A_{1,n}x_n\right|^2}{\left|A_{2,n}\right|^2}\right] = \alpha\mathbb{E}\left[\left|A_{1,n}x_n\right|^2\right]\mathbb{E}\left[\frac{1}{\left|A_{2,n}\right|^2}\right] \\ &\geq \frac{\alpha\mathbb{E}\left[\left|A_{1,n}x_n\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]} = \frac{\alpha\mathbb{E}\left[\left|A_{1,n}\right|^2\right]\mathbb{E}\left[|x_n|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]}\end{aligned} \tag{11}$$

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

[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.

For the term $A_{1,n}$, we have:

$$\begin{aligned}
\mathbb{E}\left[|A_1|^2\right] =& \mathbb{E}\left[\left|\sqrt{\alpha}\,\mathbf{S}^H\,|\mathbf{H}_\mathrm{B}|^2\,\mathbf{S}\right|^2\right] \\
\mathbb{E}\left[|A_{1,n}|^2\right] =& \mathbb{E}\left[\left|\frac{\sqrt{\alpha}}{U}\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right|^2\right] \\
=& \frac{\alpha}{U^2}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right)\left(\sum_{j=0}^{U-1}\left|h_{\mathrm{B},n+jN}\right|^2\right)^H\right] \\
=& \frac{\alpha}{U^2}\Big(\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^4\right] + \\
& \mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{\mathrm{B},n+iN}\right|^2\right]\mathbb{E}\left[\sum_{\substack{j=0\\ j\neq i}}^{U-1}|h^*_{\mathrm{B},n+jN}|^2\right]\Big) \\
=& \frac{\alpha}{U^2}\left(2U + U(U-1)\right) = \frac{\alpha(U+1)}{U}
\end{aligned} \tag{12}$$

where we used the fact that $\mathbb{E}\left[\left|h_{\mathrm{B},n+iN}\right|^2\right] = 1$ and $\mathbb{E}\left[\left|h_{\mathrm{B},n+iN}\right|^4\right] = 2$ since $\mathbf{H}_\mathrm{B} \sim \mathcal{CN}(0,1)$
The mean energy per noise symbol, $A_{2,n}$, can be derived as follow:

$$\begin{aligned}
\mathbb{E}\left[|A_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{B}\right|^2\right] \\
&= \mathbb{E}\left[\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)\left(\mathbf{S}^H\mathbf{v}_\mathrm{B}\right)^H\right] \\
&= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{B}\mathbf{v}_\mathrm{B}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{B},n+iN}|^2\right] = \sigma^2_{\mathrm{V,B}}
\end{aligned} \tag{13}$$

From (11), (12) and (13), the SINR for a particular symbol at the intended position is given by:

$$\mathbb{E}\left[\gamma_{B,n}\right] \geq \frac{\alpha\,(U+1)}{U\,\sigma^2_{\mathrm{V,B}}} \tag{14}$$

It was observed in simulations than the lower-bound (14) is tight enough to be used as an approximation of the averaged SINR at the intended position.

2) At the unintended position: At the unintended position, the received signal before ZF equalization is given by (8). Let's introduce $\mathbf{A}_1 = \sqrt{\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\mathbf{x}$, $\mathbf{A}_2 = \mathbf{G}\mathbf{v}_\mathrm{E}$ and $\mathbf{A}_3 = \sqrt{1-\alpha}\mathbf{G}\mathbf{H}_\mathrm{E}\mathbf{w}$ being respectively the data component, the noise component and the AN component of the received signal for a particular decoding structure $\mathbf{G}$. Using the Jensen's inequality, an approximation of a lower-bound of the averaged SINR of the symbols n at the unintended position can be derived as[2]:

[2]Neglecting the covariance between $\left|A_{1,n}\right|^2$ and $\left|A_{2,n}+A_{3,n}\right|^2$, as done in the first line of (15), 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.

$$\begin{aligned}
\mathbb{E}\left[\gamma_{E,n}\right] &= \mathbb{E}\left[\frac{\left|A_{1,n}\right|^2}{\left|A_{2,n}+A_{3,n}\right|^2}\right] \approx \mathbb{E}\left[\left|A_{1,n}\right|^2\right]\mathbb{E}\left[\frac{1}{\left|A_{2,n}+A_{3,n}\right|^2}\right] \\
&\gtrapprox \frac{\mathbb{E}\left[\left|A_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}+A_{3,n}\right|^2\right]} = \frac{\mathbb{E}\left[\left|A_{1,n}\right|^2\right]}{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]+\mathbb{E}\left[\left|A_{3,n}\right|^2\right]}
\end{aligned} \tag{15}$$

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 three of them.

a) Same decoding strucure as Bob: This scenario correspond to the situation where Bob wants first to establish a secure communication. He sends an unprecoded pilot to Alice and she answers with precoded data without pilot. As a consequence, Eve will not be able to know any communication parameter. The eavesdropper has the same capabilities as Bob, i.e., he despread the received signal thanks to $\mathbf{G} = \mathbf{S}^H$. In that case, the received signal is:

$$\mathbf{y}_\mathrm{E}^G = \sqrt{\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\,\mathbf{x} + \sqrt{1-\alpha}\,\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{w} + \mathbf{S}^H\mathbf{v}_\mathrm{E} \tag{16}$$

We define:

$$\begin{aligned}
A_{1,n} &= \sqrt{\alpha}\frac{1}{U}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}\; h^*_{\mathrm{B},n+iN} \\
A_{2,n} &= \frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} v_{\mathrm{E},n+iN} \\
A_{3,n} &= \sqrt{1-\alpha}\frac{1}{\sqrt{U}}\sum_{i=0}^{U-1} h_{\mathrm{E},n+iN}\; w_{n+iN}
\end{aligned} \tag{17}$$

For the data component, we have:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_1|^2\right] &= \mathbb{E}\left[\left|\sqrt{\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{B}^*\mathbf{S}\right|^2\right] \\
\mathbb{E}\left[|A_{1,n}|^2\right] &= \alpha\mathbb{E}\left[\frac{1}{U^2}\sum_{i=0}^{U-1}\left|h_{\mathrm{E},n+iN}\right|^2\left|h^*_{\mathrm{B},n+iN}\right|^2\right] \\
&= \frac{\alpha}{U}
\end{aligned} \tag{18}$$

For the noise component:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_2|^2\right] &= \mathbb{E}\left[\left|\mathbf{S}^H\mathbf{v}_\mathrm{E}\right|^2\right] \\
&= \mathbb{E}\left[\mathbf{S}^H\mathbf{v}_\mathrm{E}\mathbf{v}_\mathrm{E}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{2,n}|^2\right] &= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|v_{\mathrm{E},n+iN}|^2\right] = \sigma^2_{\mathrm{V,E}}
\end{aligned} \tag{19}$$

The AN term is given by:

$$\begin{aligned}
\mathbb{E}\left[|\mathbf{A}_3|^2\right] &= \mathbb{E}\left[\left|\sqrt{1-\alpha}\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{w}\right|^2\right] \\
&= (1-\alpha)\mathbb{E}\left[\mathbf{S}^H\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*\mathbf{w}\mathbf{w}^*\mathbf{S}\right] \\
\mathbb{E}\left[|A_{3,n}|^2\right] &= \frac{1-\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|h_{\mathrm{E},n+iN}w_{n+iN}|^2\right] = \frac{1-\alpha}{U}
\end{aligned} \tag{20}$$

From (15), (18), (19) and (20), the SINR for a particular symbol when Eve has the same capabilities as Bob is given by:

$$\mathbb{E}\left[\gamma_{E,n}\right] \gtrapprox \frac{\alpha}{U\sigma^2_{\mathrm{V,E}} + \frac{1-\alpha}{U}} \tag{21}$$

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.

b) Matched filtering:

c) Own channel knowledge:

C. Optimal amount of AN energy to inject

1) Same decoding strucure as Bob:

2) Matched filtering:

3) Own channel knowledge:

D. Required SINR at Bob for a targetted SR

E. Secrecy rate optimization via waterfilling

IV. Simulation Results

A. Model performances

Equivalent of fig10 and 11 p14 rapport

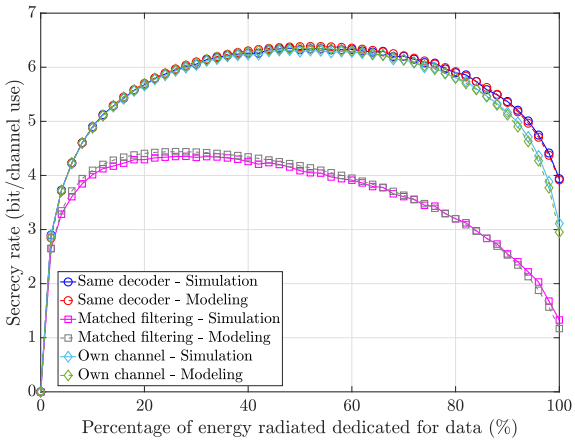

Figure 2. Models vs simulations, E_b/N_0 = 15dB at Bob, E_b/N_0 = 10dB at Eve, BOR = 4

B. Waterfilling optimization performances

Equivalent of fig13 p15 rapport + comments

ATTENTION: REFAIRE SIMU + LONGUE AU LABO

V. Conclusions

Appendix A
Derivation of.. to define

Appendix one text goes here.

Acknowledgment

The authors would like to thank...

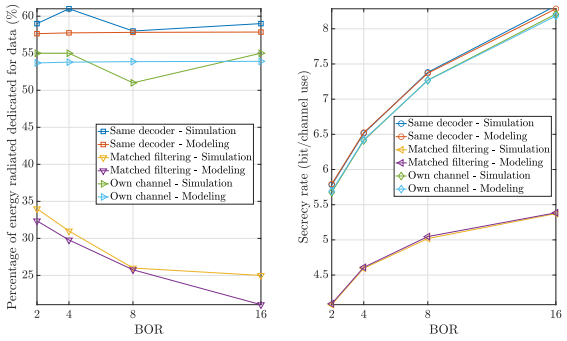

Figure 3. Optimal of AN energy to inject, E_b/N_0 = 15dB at Bob, E_b/N_0 = 5dB at Eve

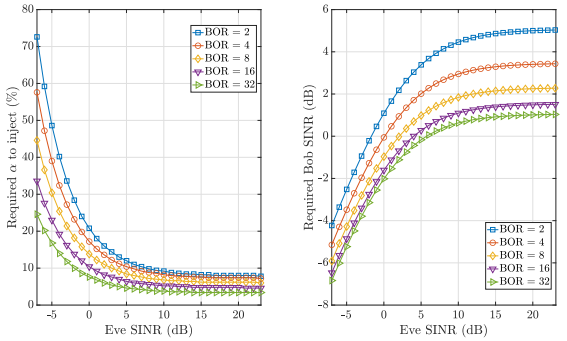

Figure 4. Targetted SR = 0 bit/channel use, matched filtering at Eve

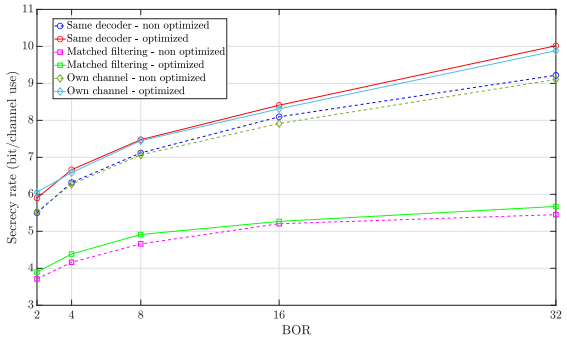

Figure 5. Waterfilling optimization, E_b/N_0 = 15dB at Bob and Eve, BOR = 4

References

[1] S. Ahmed, T. Noguchi, and M. Kawai, "Selection of spreading codes for reduced papr in mc-cdma systems," in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1–5.

[2] T.-H. Nguyen, J.-F. Determe, M. Van Eeckhaute, J. Louveaux, P. De Doncker, and F. Horlin, "Frequency-domain time-reversal precoding in wideband miso ofdm communication systems," *arXiv preprint arXiv:1904.10727*, 2019.

[3] H. Tran, H. Tran, G. Kaddoum, D. Tran, and D. Ha, "Effective secrecy-sinr analysis of time reversal-employed systems over correlated multi-path channel," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 527–532.