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

Sidney Golstein
Laboratoire d'Electronique et Electromagnétisme, L2E
Wireless Communication Group
Sorbonne Université, Université Libre de Bruxelles
F-75005 Paris, France
sigolste@ulb.ac.be

Trung-Hien Nguyen
Wireless Communication Group
Université Libre de Bruxelles
1050 Brussels, Belgium
trung-hien.nguyen@ulb.ac.be

François Horlin
Wireless Communication Group
Université Libre de Bruxelles
1050 Brussels, Belgium
fhorlin@ulb.ac.be

Philippe De Doncker
Wireless Communication Group
Université Libre de Bruxelles
1050 Brussels, Belgium
Philippe.Dedoncker@ulb.ac.be

Julien Sarrazin
Laboratoire d'Electronique et Electromagnétisme, L2E
Sorbonne Université
F-75005 Paris, France
julien.sarrazin@sorbonne-universite.fr

***Abstract*—A frequency domain (FD) time-reversal (TR) precoder is proposed to perform physical layer security (PLS) in single-input single-output (SISO) system using orthogonal frequency-division multiplexing (OFDM). To maximize the secrecy of the communication, the design of an artificial noise (AN) well-suited to the proposed FD TR-based OFDM SISO system is derived. This new scheme guarantees the secrecy of a communication toward a legitimate user when the channel state information (CSI) of a potential eavesdropper is not known. In particular, we derive an AN signal that does not corrupt the data transmission to the legitimate receiver but degrades the decoding performance of the eavesdropper. A closed-form expression for the AN energy to inject is defined in order to maximize the secrecy rate (SR) of the communication. Simulation results are presented to demonstrate the security performance of the proposed secure FD TR SISO OFDM system.**

***Index Terms*—Physical layer security, time-reversal, eavesdropper, SISO-OFDM, artificial noise, secrecy rate, security.**

I. Introduction

Due to their broadcast nature, wireless communications remain unsecured. With the deployment of 5G as an heterogeneous network possibly involving different access technologies, physical layer security (PLS) has gained recent interests in order to secure wireless communications, [1]–[3]. 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, [4]. 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, or if not, 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 [5]–[9].

In [5], 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, [10]. To further enhance the secrecy, few works combine TR precoding with AN injection [7]–[9]. 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 the back-off rate (BOR), defined as the up/downsampling rate [11], has not been yet studied in the literature.

In this paper, a novel and original approach to establish secure communication using a frequency domain (FD) TR precoder in SISO systems is proposed. The TR precoder is applied in FD using orthogonal frequency-division multiplexing (OFDM), [6]. Furthermore, an AN signal is designed to maximize the secrecy rate (SR) of the communication in presence of a passive eavesdropper.

The reminder of this paper is organized as follows: the conventional FD TR-based OFDM system is presented in Section II as well as the way to design and inject the AN. In Section III, a closed-form expression of the amount of AN energy to be injected in order to maximize the SR is derived. Theoretical and numerical results are shown in Section IV. Section V concludes the paper.

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.

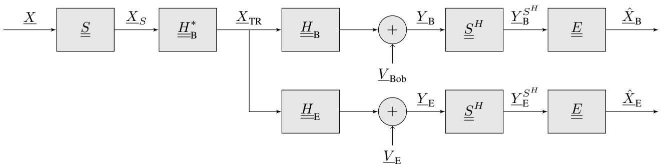

Fig. 1. Conventional FD TR SISO OFDM system

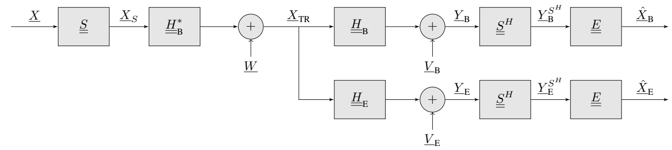

Fig. 2. FD TR SISO OFDM system with added Artificial Noise

Notation: the underlined upper-case letter denotes a column vector. Double-underlined upper-case letter corresponds to a matrix; $\underline{\underline{I}}_N$ is the $N \times N$ identity matrix; $(.)^{-1}$, $(.)^*$, $(.)^H$ are respectively the inverse, the complex conjugate, and the Hermitian transpose operators; $\mathbb{E}$ is expectation operator; $x!$ is the factorial of a positive integer x.

II. System Model

A. Conventional FD TR SISO OFDM communication

The FD TR precoding scheme is illustrated in Fig. 1. The communication is designed such that the data focuses at the legitimate receiver's position, i.e., at Bob. An eavesdropper, Eve, tries to intercept the data. We assume that the transmitter Alice does not have any information about Eve's CSI. The data is conveyed onto OFDM symbols with Q subcarriers. Without loss of generality, we consider that only one OFDM block $\underline{X}$ is sent over the FD TR precoding SISO OFDM system. A data block $\underline{X}$ 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 with variance $\mathbb{E}\left[|X_n|^2\right] = \sigma_X^2 = 1$ (i.e., a normalized constellation is considered). The data block $\underline{X}$ is then spread with a factor $U = Q/N$, called back-of rate (BOR), via the matrix $\underline{\underline{S}}$ of size $Q \times N$. The matrix $\underline{\underline{S}}$ stacks U times $N \times N$ diagonal matrices, with diagonal elements taken from the set $\{\pm 1\}$ and being identically and independently distributed in order not to increase the peak-to-average-power ratio (PAPR) as suggested in [12]. This matrix is normalized by a factor $\sqrt{U}$ in order to have $\underline{\underline{S}}^H \underline{\underline{S}} = \underline{\underline{I}}_N$. The effect of spreading is to transmit the same data symbol onto U different subcarriers. The spread sequence is then precoded before being transmitted. This requires the knowledge of Bob channel frequency response (CFR) at Alice. The channels between Alice and Bob ($\underline{\underline{H}}_{\text{B}}$) and between Alice and Eve ($\underline{\underline{H}}_{\text{E}}$) are assumed to be static during the transmission of one OFDM symbol. $\underline{\underline{H}}_{\text{B}}$ and $\underline{\underline{H}}_{\text{E}}$ are $Q \times Q$ diagonal matrices whose elements $H_{\text{B},q}$ and $H_{\text{E},q}$ (for $q = 0, ..., Q-1$) have variances equal to one. The precoding matrix $\underline{\underline{H}}_{\text{B}}^*$ is also a diagonal matrix with elements $H_{\text{B},q}^*$. At the receiver, a despreading operation is performed by applying $\underline{\underline{S}}^H$. We consider that Bob and Eve decoding abilities are identical. They both know the spreading sequence and apply a Zero Forcing (ZF) equalization. A perfect synchronization is assumed at Bob and Eve positions.

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

$$\underline{Y}_{\text{B}} = \underline{\underline{S}}^H \left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\, \underline{X} + \underline{\underline{S}}^H \underline{V}_{\text{B}} \tag{1}$$

where $\underline{V}_{\text{B}}$ is the FD complex additive white Gaussian noise (AWGN). The noise's auto-correlation is $\mathbb{E}[|V_{\text{B},n}|^2] = \sigma_{\text{V,B}}^2$ and the covariance matrix is $\mathbb{E}[(\underline{\underline{S}}^H \underline{V}_{\text{B}}).(\underline{\underline{S}}^H \underline{V}_{\text{B}})^H] = \sigma_{\text{V,B}}^2 . \underline{\underline{I}}_N$. We also assume that the signal X_n and noise $V_{\text{B,n}}$ are independent of each other. In (1), each transmitted symbol is affected by a real gain at the position of the legitimate receiver since the product $\underline{\underline{H}}_{\text{B}}\, \underline{\underline{H}}_{\text{B}}^*$ 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 equalization, we obtain:

$$\underline{\hat{X}}_{\text{B}} = \left(\underline{\underline{S}}^H \left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\right)^{-1} \left(\underline{\underline{S}}^H \left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\, \underline{X} + \underline{\underline{S}}^H \underline{V}_{\text{B}}\right) \tag{2}$$

From (2), we observe that the transmit data is perfectly recovered in the absence of noise.

2) Received sequence at the unintended position: After despreading, the data received at unintended position is given by:

$$\underline{Y}_{\text{E}} = \underline{\underline{S}}^H \underline{\underline{H}}_{\text{E}} \underline{\underline{H}}_{\text{B}}^* \underline{\underline{S}}\, \underline{X} + \underline{\underline{S}}^H \underline{V}_{\text{E}} \tag{3}$$

where $\underline{V}_{\text{E}}$ is the complex AWGN. The noise's auto-correlation is $\mathbb{E}[|V_{\text{E},n}|^2] = \sigma_{\text{V,E}}^2$ and the covariance matrix is $\mathbb{E}[(\underline{\underline{S}}^H \underline{V}_{\text{E}}).(\underline{\underline{S}}^H \underline{V}_{\text{E}})^H] = \sigma_{\text{V,E}}^2 . \underline{\underline{I}}_N$. In (3), $\underline{\underline{H}}_{\text{E}} \underline{\underline{H}}_{\text{B}}^*$ is a complex diagonal matrix, and each transmitted symbol is 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 will be obtained compared to the intended position. Nevertheless, the transmit sequence can be fully recovered, in the absence of noise, with a simple ZF equalization:

$$\underline{\hat{X}}_{\text{E}} = \left(\underline{\underline{S}}^H \underline{\underline{H}}_{\text{E}} \underline{\underline{H}}_{\text{B}}^* \underline{\underline{S}}\right)^{-1} \left(\underline{\underline{S}}^H \underline{\underline{H}}_{\text{E}} \underline{\underline{H}}_{\text{B}}^* \underline{\underline{S}}\, \underline{X} + \underline{\underline{S}}^H \underline{V}_{\text{E}}\right) \tag{4}$$

Equation (4) shows that the classical FD TR SISO OFDM communication scheme lacks of security. This motivates the addition of AN in order to corrupt the data detection at any unintended positions and to secure the communication.

B. FD TR SISO OFDM communication with Artificial Noise

In order to secure the communication between Alice and Bob, an AN signal $\underline{W}$ is added after precoding to the useful signal $\underline{X}_s$ at the transmitter side, as depicted in Fig. 2. 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. With these considerations, the transmitted sequence becomes:

$$\underline{X}_{\text{TR}} = \sqrt{\alpha}\ \underline{\underline{H}}_{\text{B}}^{*}\underline{\underline{S}}\ \underline{X} + \sqrt{1-\alpha}\ \underline{W} \tag{5}$$

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

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

$$\underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{B}}\underline{W} \ = \ \underline{0} \tag{6}$$

where $\underline{0}$ is the null vector of dimension $N \times 1$. From (6), the following system must be solved:

$$\underbrace{\begin{pmatrix} \pm1 & 0 & \dots & 0 & & \pm1 & 0 & \dots & 0 \\ 0 & \pm1 & \dots & 0 & \dots & 0 & \pm1 & \dots & 0 \\ \vdots & & \ddots & \vdots & \dots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \pm1 & & 0 & 0 & \dots & \pm1 \end{pmatrix}}_{N\times Q} \underbrace{\begin{pmatrix} H_{\text{B},0} \\ H_{\text{B},1} \\ \vdots \\ H_{\text{B},Q-1} \end{pmatrix}}_{Q\times 1} \odot \underbrace{\begin{pmatrix} W_0 \\ W_1 \\ \vdots \\ W_{Q-1} \end{pmatrix}}_{Q\times 1} = \underbrace{\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{N\times 1} \tag{7}$$

where "$\odot$" represents the element-wise (Hadamard) product. Equation (7) is a set of N equations with Q unknowns. Since $Q = NU$, as soon as $U \geq 2$, (7) becomes under-determined and the AN vector can be generated from a set of infinite possibilities. Let us define $\underline{\underline{S}}^{H} = [\underline{\underline{S}}_0\ \underline{\underline{S}}_1\ \dots\ \underline{\underline{S}}_{U-1}]$, where $\underline{\underline{S}}_i$ is the i^{th} diagonal matrix of $\underline{\underline{S}}^{H}$ of size $N \times N$. We define as $S_{i,p}$ as the p^{th} diagonal element of S_i. If we denote the i^{th} diagonal element of $\underline{\underline{H}}_{\text{B}}$ as H_i, (7) becomes:

$$\begin{cases} \sum\limits_{i=0}^{U-1} S_{i,0}H_{iN}W_{iN} & = & 0 \\ \sum\limits_{i=0}^{U-1} S_{i,1}H_{iN+1}W_{iN+1} & = & 0 \\ \vdots & & \vdots \\ \sum\limits_{i=0}^{U-1} S_{i,N-1}H_{iN+N-1}W_{iN+N-1} & = & 0 \end{cases} \tag{8}$$

In (8), each equation consists in a sum of U elements, with the channel components and the spreading sequence being known. The idea is to generate $U-1$ components of the AN vector in every equations of (8) as normal random variables, and to determine the last AN components that ensures (6) as follow:

$$\begin{cases} W_{Q-N} & = & -\dfrac{\sum\limits_{i=0}^{U-2} S_{i,0}H_{iN}W_{iN}}{S_{U-1,0}H_{Q-N}} \\ W_{Q-N+1} & = & -\dfrac{\sum\limits_{i=0}^{U-2} S_{i,1}H_{iN+1}W_{iN+1}}{S_{U-1,1}H_{Q-N+1}} \\ \vdots & & \vdots \\ W_{Q-1} & = & -\dfrac{\sum\limits_{i=0}^{U-2} S_{i,N-1}H_{iN+N-1}W_{iN+N-1}}{S_{U-1,N-1}H_{Q-1}} \end{cases} \tag{9}$$

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

$$\underline{Y}_{\text{B}} = \sqrt{\alpha}\ \underline{\underline{S}}^{H}\left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\ \underline{X}\ +\ \underline{\underline{S}}^{H}\underline{V}_{\text{B}} \tag{10}$$

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 (6) is respected. A ZF equalization is performed at the receiver:

$$\hat{\underline{X}}_{\text{B}} = \left(\sqrt{\alpha}\ \underline{\underline{S}}^{H}\left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\right)^{-1}\left(\sqrt{\alpha}\ \underline{\underline{S}}^{H}\left|\underline{\underline{H}}_{\text{B}}\right|^2 \underline{\underline{S}}\ \underline{X}\ +\ \underline{\underline{S}}^{H}\underline{V}_{\text{B}}\right) \tag{11}$$

From (11), a perfect data recovery is possible in the absence of noise.

3) Received sequence at the unintended position: After despreading, the received sequence at the unintended position has the form:

$$\underline{Y}_{\text{E}} = \sqrt{\alpha}\ \underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{\underline{H}}_{\text{B}}^{*}\underline{\underline{S}}\ \underline{X}\ +\ \sqrt{1-\alpha}\ \underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{W}\ +\ \underline{\underline{S}}^{H}\underline{V}_{\text{E}} \tag{12}$$

In (12), a term depending on the AN signal appears since $\underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{W} \neq \underline{0}$. 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:

$$\begin{split} \hat{\underline{X}}_{\text{E}} = &\left(\sqrt{\alpha}\ \underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{\underline{H}}_{\text{B}}^{*}\underline{\underline{S}}\right)^{-1} \\ &\left(\sqrt{\alpha}\ \underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{\underline{H}}_{\text{B}}^{*}\underline{\underline{S}}\ \underline{X}\ +\ \sqrt{1-\alpha}\ \underline{\underline{S}}^{H}\underline{\underline{H}}_{\text{E}}\underline{W}\ +\ \underline{\underline{S}}^{H}\underline{V}_{\text{E}}\right) \end{split} \tag{13}$$

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 $\underline{W}$ is generated from an infinite set of possibilities, even if Eve knows $\underline{\underline{H}}_{\text{B}}$, she cannot estimate the AN to try retrieving the data. The degree of security will depend on the amount of AN energy that is injected into the communication, as shown in Section III.

III. Performance Assessment

In the ergodic sense, 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, [13]. It can be expressed as:

$$C_S = \log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right) \quad , \quad \gamma_B > \gamma_E \tag{14}$$

with γ_B and γ_E being respectively the signal-to-interference-plus-noise Ratio (SINR) at Bob and Eve's positions. The SINRs have the following forms:

$$\gamma_B = \frac{\sigma^2_{\text{X}_{\text{D,B}}}}{\sigma^2_{\text{V,B}}} \quad \text{and} \quad \gamma_E = \frac{\sigma^2_{\text{X}_{\text{D,E}}}}{\sigma^2_{\text{AN}} + \sigma^2_{\text{V,E}}} \tag{15}$$

where $\sigma^2_{\text{X}_{\text{D,B/E}}}$, σ^2_{AN}, and $\sigma^2_{\text{V,B/E}}$ are respectively the energy of the useful signal after despreading, i.e., that conveys the data symbols, the AN signal, and the noise signal at Bob and Eve positions.

A. SINR determination

1) At the intended position: At Bob, the received signal after despreading is given by (10). The SINR can be computed for a particular transmitted symbol n as:

$$\gamma_{B,n} = \frac{\mathbb{E}\left[\alpha \left|K_n\ X_n\right|^2\right]}{\sigma^2_{\text{V,B}}} = \frac{\mathbb{E}\left[\alpha \left|K_n\right|^2\right] \mathbb{E}\left[\left|X_n\right|^2\right]}{\sigma^2_{\text{V,B}}} \tag{16}$$

where $K_n = \frac{1}{U}\ \sum_{i=0}^{U-1} \left|H_{\text{B},n+iN}\right|^2$ is a real random variable (RV) independent of the data symbol X_n. If $H_{\text{B},n+iN}$ and $H_{\text{B},n+(i+1)N}$ ($\forall i = 0, ..., U-2$) are assumed to be non-correlated[1], K_n can be approximated as following a chi-square distribution with U degrees of freedom, so that:

$$\mathbb{E}\left[\left|K_n\right|^2\right] = \int_0^{\infty} z^2 f_Z(z) dz = \frac{\alpha(U+1)}{U} \tag{17}$$

Furthermore, remembering that $\mathbb{E}\left[\left|X_n\right|^2\right] = 1$, the SINR for a particular symbol at the intended position is then given by:

$$\gamma_{B,n} = \frac{\alpha\ (U+1)}{U\ \sigma^2_{\text{V,B}}} \tag{18}$$

2) At the unintended position: The received signal after despreading is (12). Let's introduce $A_1 = \sqrt{1-\alpha}\underline{\underline{S}}^H \underline{\underline{H}}_{\text{E}} \underline{W}$ and $A_2 = \sqrt{\alpha}\underline{\underline{S}}^H \underline{\underline{H}}_{\text{E}} \underline{\underline{H}}^*_{\text{B}} \underline{\underline{S}}\ \underline{X}$. The SINR for a particular symbol n at the unintended position is thus given by:

$$\gamma_{E,n} = \frac{\mathbb{E}\left[\left|A_{2,n}\right|^2\right]}{\sigma^2_{\text{V,E}} + \mathbb{E}\left[\left|A_{1,n}\right|^2\right]} \tag{19}$$

Assuming $H_{\text{E},n+iN}$ and $H_{\text{E},n+(i+1)N}$ ($\forall i = 0, ..., U-2$) non-correlated and neglecting the correlation introduced in $\underline{W}$ by (9), the AN interference can be calculated as:

$$\begin{aligned}\mathbb{E}\left[\left|A_{1,n}\right|^2\right] &= \frac{(1-\alpha)}{U}\ \sum_{i=0}^{U-1} \mathbb{E}\left[\left|W_{n+iN}\right|^2\right]\ \underbrace{\mathbb{E}\left[\left|H_{\text{E},n+iN}\right|^2\right]}_{=1} \\ &= (1-\alpha)\ \sigma^2_{\text{AN}}\end{aligned} \tag{20}$$

where $\sigma^2_{\text{AN}} = \mathbb{E}\left[\left|W_{n+iN}\right|^2\right]$.
The energy related to the useful symbol is:

$$\begin{aligned}\mathbb{E}\left[\left|A_{2,n}\right|^2\right] &= \frac{\alpha}{U^2}\ \mathbb{E}\left[\left|\sum_{i=0}^{U-1} H_{\text{E},n+iN}\ H^*_{\text{B},n+iN}\ X_{n+iN}\right|^2\right] \\ &= \frac{\alpha}{U^2}\ \mathbb{E}\left[\left|\sum_{i=0}^{U-1} H_{\text{E},n+iN}\ H^*_{\text{B},n+iN}\right|^2\right]\ \underbrace{\mathbb{E}\left[\left|X_{n+iN}\right|^2\right]}_{=1} \\ &= \frac{\alpha}{U^2}\ \mathbb{E}\left[\left|Z_n\right|^2\right]\end{aligned} \tag{21}$$

with $Z_n = \sum_{i=0}^{U-1} Z_{n,i}$ and $Z_{n,i} = H_{\text{E},n+iN}.H^*_{\text{B},n+iN}$ (where $H_{\text{E},n+iN}$ and $H^*_{\text{B},n+iN}$ are assumed to be statistically independent and identically distributed (i.i.d.) complex Gaussian RVs of zero-mean and unit variance). Z_n, similarly to K_n, is the sum of uncorrelated complex RVs. Introducing $R = |Z_n|$, we obtain the PDF of R as in [6]:

$$f_R(r) = \frac{4r^U}{\Gamma(U)}\ \mathbb{K}_{U-1}\left(2r\right) \tag{22}$$

where $\Gamma(U) = (U-1)! = \int_0^{\infty} z^{U-1} e^{-z} dz$ is the Gamma function of the integer U. In (22), $\mathbb{K}_U$ is the U^{th} order modified Bessel function of the second kind which can be approximated by:

$$\mathbb{K}_U(x) \approx \sum_{q=0}^{D} \sum_{l=0}^{D} \psi(U,l,q)\ e^{-x}\ x^{q-U} \tag{23}$$

where D specifies the number of expansion terms and $\psi(U,l,q)$ is given by:

$$\psi(U,l,q) = \frac{(-1)^q\ \sqrt{\pi}\ \Gamma(2U)\ \Gamma(1/2+l-U)\ \mathbb{L}(l,q)}{2^{U-q}\ \Gamma(1/2-U)\ \Gamma(1/2+l+U)\ l!} \tag{24}$$

where $\mathbb{L}(l,q)$ is the Lah number [14] with the conventions $\mathbb{L}(0,0) = 1$, $\mathbb{L}(l,0) = 0$, $\mathbb{L}(l,1) = l!\ \forall l > 0$. Eq. (21) therefore becomes:

$$\begin{aligned}\mathbb{E}\left[\left|A_{2,n}\right|^2\right] &= \frac{\alpha}{U^2} \int_0^{\infty} r^2\ \frac{4r^U}{\Gamma(U)}\ \mathbb{K}_{U-1}(2r)\ dr \\ &= \frac{4\alpha}{U^2\ (U-1)!}\ \sum_{q=0}^{D}\sum_{l=0}^{D} \psi(U,l,q) \int_0^{\infty} r^{U+2}\ e^{-2r}\ (2r)^{q-U}\ dr \\ &= \frac{4\alpha}{U^2\ (U-1)!\ 2^{U+3}} \sum_{q=0}^{D}\sum_{l=0}^{D} \psi(U,l,q)\ \Gamma(q+3)\end{aligned} \tag{25}$$

Consequently, the SINR for a particular transmitted symbol at the unintended position can be expressed as:

$$\gamma_{E,n} = \frac{\frac{4\alpha}{U^2(U-1)!2^{U+3}} \sum_{q=0}^{D} \sum_{l=0}^{D} \psi(U,l,q)\Gamma(q+3)}{\sigma^2_{\text{V,E}}\ +\ (1-\alpha)\sigma^2_{\text{AN}}} \tag{26}$$

B. Optimal amount of Artificial Noise energy to maximize the secrecy capacity

With (18) and (26), it is possible to obtain a closed-form expression of the SR and determine the amount of AN energy to inject that maximizes the SR. By introducing the variable $A = \frac{1}{U^2\ (U-1)!\ 2^{U+3}} \sum_{q=0}^{D} \sum_{l=0}^{D} \psi(U,l,q)\ \Gamma(q+3)$, the SR is therefore:

$$\begin{aligned}C_s &= \log_2\left(1 + \frac{\alpha(U+1)}{U\sigma^2_{\text{V,B}}}\right) - \log_2\left(1 + \frac{4\alpha A}{\sigma^2_{\text{V,}}\ +\ (1-\alpha)\sigma^2_{\text{AN}}}\right) \\ &= \log_2\left(\frac{U\sigma^2_{\text{V,B}}\ +\ \alpha(U+1)}{U\sigma^2_{\text{V,B}}} \cdot \frac{\sigma^2_{\text{V,E}}\ +\ (1-\alpha)\sigma^2_{\text{AN}}}{\sigma^2_{\text{V,E}}\ +\ (1-\alpha)\sigma^2_{\text{AN}}\ +\ 4\alpha A}\right)\end{aligned} \tag{27}$$

Let us denote $T_1 = \sigma^2_{\text{AN}}(U+1)$, $T_2 = \sigma^2_{\text{V,E}}(U+1) - U\sigma^2_{\text{V,B}}\sigma^2_{\text{AN}} + \sigma^2_{\text{AN}}(U+1)$, $T_3 = U\sigma^2_{\text{V,B}}\left[\sigma^2_{\text{V,E}} + \sigma^2_{\text{AN}}\right]$ and $T_4 = 4AU\sigma^2_{\text{V,B}} - \sigma^2_{\text{V,B}}\sigma^2_{\text{AN}}$. After some manipulations, (27) becomes:

$$C_s = \log_2\left(\frac{-\alpha^2 T_1\ +\ \alpha T_2\ +\ T_3}{\alpha T_4\ +\ T_3}\right) \tag{28}$$

[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.

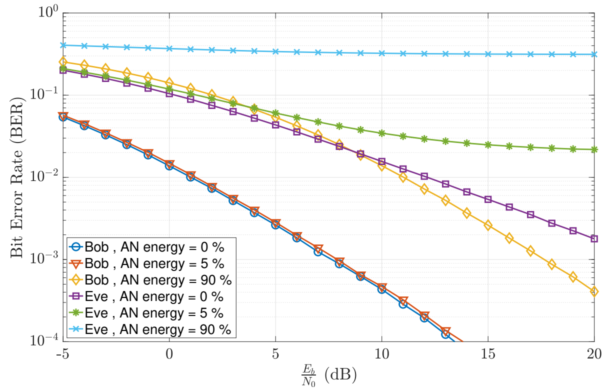

Fig. 3. BER as a function of the level of noise for different AN energy values, BOR = 4

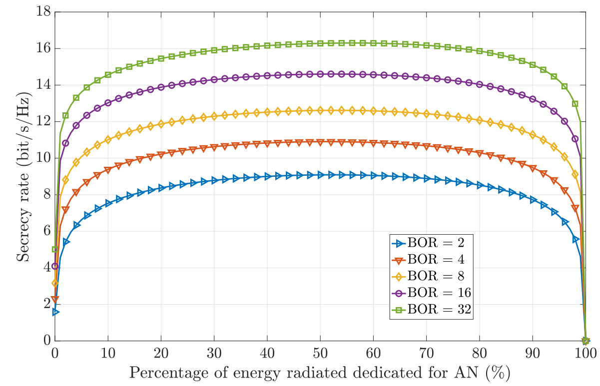

Fig. 5. Secrecy Rate as a function of the AN energy for different BOR values, $E_b/N_0 = 20$ dB

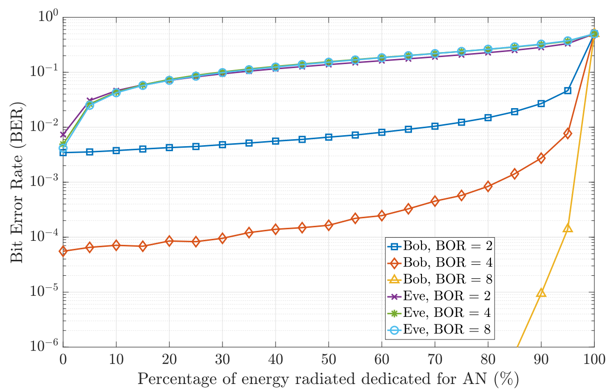

Fig. 4. BER as a function of AN energy for different BOR values, $E_b/N_0 =$ 15dB

We need to maximize the secrecy rate as a function of the parameter α, i.e., we have to find the zeroes of:

$$\frac{\partial C_s}{\partial \alpha} = \frac{\dfrac{-\alpha^2 T_1 T_4 - 2\alpha T_1 T_3 + (T_2 T_3 - T_3 T_4)}{(\alpha T_4 + T_3)^2}}{\dfrac{-\alpha^2 T_1 + \alpha T_2 + T_3}{\alpha T_4 + T_3} \ . \ \ln 2} \tag{29}$$

After some algebraic manipulations, one obtains:

$$\frac{\partial C_s}{\partial \alpha} = 0 \ \Leftrightarrow \ \alpha = \frac{\pm\sqrt{T_1^2 T_3^2 + T_1 T_2 T_3 T_4 - T_1 T_3 T_4^2} - T_1 T_3}{T_1 T_4} \tag{30}$$

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

IV. 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. 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. The number of expansion terms of the modified Bessel function is set to $D = 10$ for which convergence has been observed. Simulations with 100 channel realizations and 300 OFDM blocks were performed using a 4-QAM modulation scheme.

A. Decoding results

Fig. 3 and 4 show the system performance in terms of bit-error-rate (BER). In Fig. 3, 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 slowly. The reason is that the higher the percentage of energy dedicated to AN, the lower the received useful signal power at Bob. In Fig. 4, the BER is plotted as a function of the AN energy, at fixed E_b/N_0 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, as anticipated from Section II-A. One can notice that, when $\alpha \to 0$, the BER curves all converge to 0.5, as expected.

B. Secrecy results

Fig. 5 shows the SR evolution as a function of α for different BOR values. First, the SR obtained with the classical FD TR SISO OFDM system presented in Section II-A, 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. In addition, no more secrecy is obtained when $\alpha \to 0$, since the SINR's at Bob and Eve drop to zero.

Fig. 6 illustrates the values of α that maximize the SR determined from the closed-form expression (30) as well as obtained from the numerical simulations. The SR obtained by simulations are also plotted when using the values of α given by (30) and obtained numerically. The analytical estimation of the optimal amount of AN energy is not perfect but tends to the simulated one as the BOR increases. This due to the fact that RVs involved in the calculation of (30) are assumed to be non-correlated, while this is not so, especially for low BOR

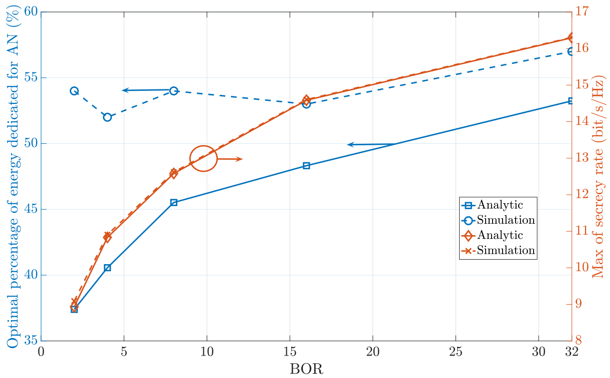

Fig. 6. Optimal AN energy to inject and maximal Secrecy Rate for different BOR values, $E_b/N_0 = 20$ dB

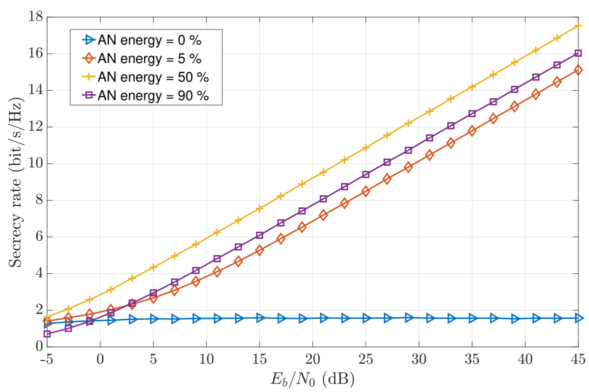

Fig. 7. Secrecy Rate as a function of the noise level for different AN energy values, BOR = 2

values due to (9). However, the resulting SR is very close to the real maximal SR. The reason can be observed in Fig. 5 where the SR varies very slowly about its maximum when α changes. So, for a given BOR value, a rough determination of α can be made at the transmitter side to maximize the SR if E_b/N_0 is known. Fig. 6 shows that the optimal amount of AN energy increases with the BOR.

Finally, the evolution of the SR as a function of the level of noise for different α values is plotted in Fig. 7. The SR saturates for the classical scenario but is monotonically increasing when the level of noise decreases as soon as AN is injected.

V. Conclusion

In this paper, 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 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. 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.

References

[1] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes", in IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372-375, 2012.

[2] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security for TAS/MRC with antenna correlation", in IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 254-259, 2013.

[3] D.-D. Tran, D.-B. Ha, V. Tran-Ha, and E.-K. Hong, "Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels", in IETE Journal of Research, Mar. 2015.

[4] A. D. Wyner, "The wire-tap channel", in Bell Syst. Tech. J., vol. 54, pp. 1355-1387, Oct. 1975.

[5] M. Li, S. Kundu, D.A. Pados, and S.N. Batalama, "Waveform Design for Secure SISO Transmissions and Multicasting", in IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, Sep. 2013.

[6] 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 Communications Systems", in arXiv e-prints, Apr. 2019.

[7] Q. Xu, P. Ren, Q. Du, and L. Sun, "Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission", in IEEE Transactions on Vehicular Technology, vol. 67, no. 7, June 2018.

[8] S. Li, N. Li, X, Tao, Z. Liu, H. Wang, and J. Xu, "Artificial Noise Inserted Secure Communication in Time-Reversal Systems", in IEEE Wireless Communications and Networking Conference, Apr. 2018.

[9] S. Li, N. Li, Z. Liu, H. Wang, J. Xu, and X. Tao, "Artificial Noise Aided Path Selection for Secure TR Communications", in IEEE/CIC International Conference on Communications in China (ICCC), Oct. 2017.

[10] C. Oestges, A.D. Kim, G. Papanicolaou, and A. J. Paulraj, "Characterization of Space-Time Focusing in Time-Reversed Random Fields", in IEEE Transactions on Antennas and Propagation, vol. 53, no. 1, Jan. 2005.

[11] T. Dubois, M. Crussière and M. Hélard, "On the use of Time Reversal for Digital Communications with Non-Impulsive Waveforms", in 4th International Conference on Sig. Process. and Commun. Sys., Dec. 2010.

[12] S. Ahmed, T. Noguchi, and M. Kawai, "Selection of Spreading Codes for Reduced PAPR in MC-CDMA systems", in IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Sep. 2007 .

[13] H-V. Tran, H. Tran and G. Kaddoum "Effective Secrecy-SINR Analysis of Time Reversal-Employed Systems over Correlated Multi-path Channel", in IEEE 11$^{\text{th}}$ international Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 527-532, Oct. 2015

[14] M. M. Molu, P. Xiao, M. Khalily, L. Zhang, and R. Tafazolli, "A novel equivalent definition of modified Bessel functions for performance analysis of multi-hop wireless communication systems," in IEEE Access, vol. 5, pp. 75947605, May 2017.