On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes

João Madeira [1,*], **João Guerreiro** [2,3,4], **Rui Dinis** [1,3] **and Paulo Montezuma** [1,3] **and Luís Miguel Campos** [4]

1   FCT, Universidade Nova de Lisboa, Monte de Caparica, 2829-516 Caparica, Portugal;
    rdinis@fct.unl.pt (R.D.); pmc@fct.unl.pt (P.M.)
2   UAL, Universidade Autónoma de Lisboa, 1169-023 Lisboa, Portugal; jfguerreiro@autonoma.pt
3   IT, Instituto de Telecomunicações, 1049-001 Lisboa, Portugal
4   PDMFC, Projeto Desenvolvimento Manutenção Formação e Consultadoria LDA, 1300-609 Lisboa, Portugal;
    luis.campos@pdmfc.com
*   Correspondence: jf.madeira@campus.fct.unl.pt

Abstract: Multi-Input, Multi-Output (MIMO) techniques are seeing widespread usage in wireless communication systems due to their large capacity gains. On the other hand, security is a concern of any wireless system, which can make schemes that implement physical layer security key in assuring secure communications. In this paper, we study the physical layer security issues of MIMO with Singular Value Decomposition (SVD) schemes, employed along with Single-Carrier with Frequency-Domain Equalization (SC-FDE) techniques. More concretely. the security potential against an unintended eavesdropper is analysed, and it is shown that the higher the distance between the eavesdropper and the transmitter or receiver, the higher the secrecy rate. In addition, in a scenario where there is Line of Sight (LOS) between all users, it is shown that the secrecy rate can be even higher than in the previous scenario. Therefore, MIMO-SVD schemes combined with SC-FDE can be an efficient option for highly secure MIMO communications.

Keywords: MIMO; SC-FDE; Physical Layer Security; SVD

1. Introduction

Multiple-Input, Multiple-Output (MIMO) techniques are being increasingly considered for new wireless communication systems, due to their huge capacity over traditional single-antenna techniques. In fact, it can be shown that the capacity can even scale linearly with the number of antenna elements [1–4]. As such, several MIMO techniques have been selected to integrate wireless communications standards, such as WiFi [5] and Long Term Evolution (LTE) [6], and will likely be key elements in future 5G systems [7].

Although wireless channels have considerable advantages, they also present additional security difficulties when compared with wired channels. In fact, since anyone in range can listen to the channel (such as an eavesdropper that knows the transmitting characteristics such as the frame and block structures and carrier frequency), the security levels of conventional wired communications might not be enough, particularly for Internet-of-Things (IoT) devices [8]. Therefore, it is desirable to have an additional physical layer security level [9–11] on top of conventional security measures, so as to increase the overall system security. Thanks to their increased security capabilities, the physical layer security techniques have become increasingly attractive for both industry, [12] and IoT applications [13]. Security measures in the physical layer can take advantage of the different characteristics of the legitimate and eavesdropper links, which can be done using channel estimates, equalization schemes,

beamforming, randomised cyclic prefix (CP), among others [14–16]. There is significant research of this subject for OFDM systems [17,18], however, there are few published works on this subject for Single Carrier with Frequency Domain Equalization (SC-FDE) systems.

Recently, a promising MIMO technique for SC-FDE was proposed in [19]. This technique employs a Singular Value Decomposition (SVD) scheme [20,21] that combines precoding [22] and decoding [23] at the frequency level, along with a powerful receiver based on the Iterative Block Decision Feedback Equalizer (IB-DFE) [24], that allows for excellent performance, even in severely time-dispersive channels. Techniques based on SVD, such as this one, can be an interesting option for 5G systems [25,26].

In this paper, we consider MIMO-SVD schemes combined with SC-FDE techniques as in [19]. By taking advantage of the different legitimate and eavesdropper's channels, we analyze the potential security at the physical layer. It is shown that the secrecy rate increases sharply with the distance between the eavesdropper and the transmitter or the receiver, which means that we can have highly secure MIMO communications whenever the eavesdropper is not co-located with the transmitter or the receiver, even if the eavesdropper is able to receive all the training blocks shared between the legitimate transmitter and receiver.

The notation is as follows: bold letters denote matrices or vectors. Capital letters are associated to the frequency-domain and small letters are associated to the time-domain. $(\cdot)^H$ denotes the Hermitian operator. $\mathbf{I}_P$ denotes a $P \times P$ identity matrix. $\mathbb{E}[\cdot]$ represent the expected value.

This paper is organized as follows: in Section 2 we begin by characterizing the point-to-point MIMO system with its intended receiver B and eavesdropper E, followed by an analysis of the system capacity and secrecy rate calculations. Section 3 shows the simulated Bit Error Rate (BER) and secrecy rate for both transmitter-receiver pairs. In addition, results and corresponding analysis are presented for a scenario where there is a Line-of-Sight (LOS) link between all users. Lastly, Section 4 concludes this paper.

2. Materials and Methods

2.1. System Characterization

In this paper we consider a point-to-point MIMO system with a transmitter, denoted A (Alice in conventional wiretap channels nomenclature), employing *T* antennas and a receiver, denoted B (Bob in conventional wiretap channels nomenclature), employing *R* antennas. For the sake of simplicity we assume $T = R$, although this work could easily be extended to the case where $T \neq R$. In addition, there is a third user, denoted E (Eve in conventional wiretap channels nomenclature), that is attempting to eavesdrop the signal transmitted between A and B. Although we are assuming a scenario with a single eavesdropper, a scenario with more eavesdroppers can also be taken into account [27]. However, a scenario with multiple co-located eavesdroppers, can be approximated by a single eavesdropper with *KR* antennas, where *K* is the number of eavesdroppers. This three user scenario is shown in Figure 1. The distance between each antenna at the transmitter and the receiver is assumed much larger than the transmitted signal's wavelength, and the receiver is in the far field region of the transmitter. The transmitter can send up to $C = R$ data streams over a highly frequency-selective channel. To cope with the strong levels of inter-symbol interference (ISI) associated to such channels, we employ an SC-FDE transmission technique. The data blocks are composed of *N* quadrature phase shift keying (QPSK) symbols (the generalization to other constellations with IB-DFE is straightforward [28]), plus an appropriate CP that is larger than the maximum overall channel impulse response. A block diagram of the considered system is depicted in Figure 2.
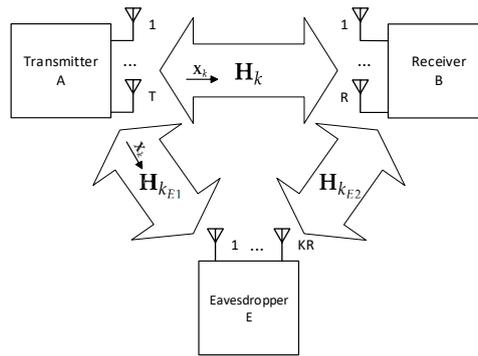
Figure 1. Considered MIMO-SVD system with an eavesdropper.
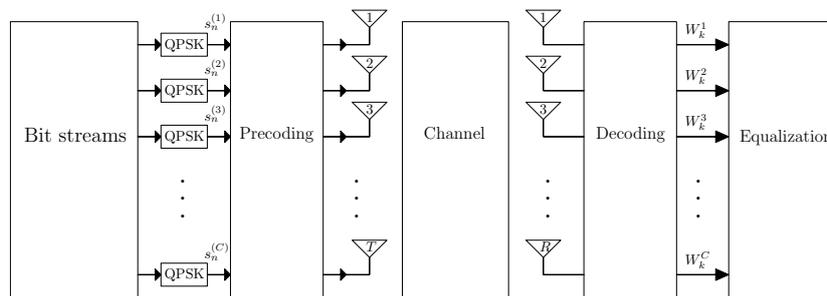
Figure 2. Proposed MIMO SVD-based system, employing T transmitting antennas and R receiving antennas.

The data symbols to be transmitted by the C single-carrier data streams will be denoted by the $N \times C$ matrix **s**, where each data stream is represented as an $N \times 1$ vector $\mathbf{s}^{(c)} = [s_1^{(c)}\ s_2^{(c)}\ \cdots\ s_N^{(c)}]$. In that context, $s_n^{(c)}$ represents the QPSK symbol transmitted on the cth stream at the nth time instant. The frequency-domain counterpart of the transmitted data is defined by the discrete Fourier transform (DFT) of **s**, which is the $N \times C$ matrix **S**. The group of symbols associated to the kth sub-carrier are represented as the $1 \times C$ vector $\mathbf{S}_k = [S_k^{(1)}\ S_k^{(2)}\ ... S_k^{(C)}]$.

The channel frequency response for the kth sub-carrier is modeled by the $R \times T$ matrix

$$\mathbf{H}_k = \begin{bmatrix} H_k^{(1,1)} & H_k^{(1,2)} & \cdots & H_k^{(1,T)} \\ H_k^{(2,1)} & H_k^{(2,2)} & \cdots & H_k^{(2,T)} \\ \vdots & \vdots & \ddots & \vdots \\ H_k^{(R,1)} & H_k^{(R,2)} & \cdots & H_k^{(R,T)} \end{bmatrix}. \tag{1}$$

Since we are considering a point-to-point communication where we have a multi-antenna transmitter and a multi-antenna receiver, the separation of the MIMO streams can be done using the SVD technique [20]. To perform the SVD, we need channel knowledge at both the transmitter and receiver. To achieve this, the transmitter and receiver exchange training sequences. This process is relatively straightforward in time division duplex (TDD) schemes, where we can take advantage of the channel's reciprocity.

The SVD technique allows us to obtain up to C decoupled channels, onto which we can multiplex up to C data streams. Since we are employing SC-FDE schemes over frequency-selective channels, this decomposition is made at the sub-carrier level. Therefore, we can decompose the channel matrix associated to a given sub-carrier $\mathbf{H}_k$ as

$$\mathbf{H}_k = \mathbf{U}_k \mathbf{\Lambda}_k \mathbf{V}_k^H, \tag{2}$$

where $\mathbf{U}_k$ is the $R \times R$ decoding matrix, $\mathbf{V}_k$ is the $T \times T$ precoding matrix and $\mathbf{\Lambda}_k$ is a $C \times C$ diagonal matrix composed by the singular values of $\mathbf{H}_k$, which are sorted in descending order according to their power.

2.1.1. Transmission

Although SVD techniques allow for the orthogonalisation of the different data streams, the performance associated to each steam can vary substantially. This is explained by the fact that the performance depends essentially on the magnitude of the singular values, which vary considerably from stream to stream [29]. To overcome this problem, one can employ appropriate loading techniques, with power and/or constellation differentiation between different streams, as it is proposed for some OFDM-based systems [30]. An interesting alternative for SC-FDE MIMO-SVD systems was described in [19], which is based on interleaving the data to be transmitted between all streams, thereby forcing each stream to be affected by singular values with different powers, and avoiding streams with very poor performance (that would determine the average BER performance). We define $\mathbf{S}'_k$ as the interleaved data symbols associated with sub-carrier.

As already pointed out, the channel estimates at the transmitter side, required for computing the precoding matrix, can be obtained from a training sequence that was previously sent by the receiver. After that, the transmitter sends a training sequence to the receiver (typically at the beginning of the data block), which is used by the receiver to compute the detection matrix, perform the channel equalization and complete the SVD decomposition (the details are described below). Naturally, we assume that the channel coherence time is greater than the time it takes to transmit both sequences and the data block. The eavesdropper listens to both training sequences, so it can compute its own channel estimate.

We can summarize this process into three steps, as shown in Figure 3. In the first step, the receiver sends a training sequence to the transmitter, which is overheard by the eavesdropper. In this step, both the transmitter and eavesdropper obtain channel estimates. In the second step, the transmitter sends a sequence of training symbols, so that the receiver can obtain a channel estimate and compute the decoding matrix to complete the SVD. The eavesdropper also listens to this sequence and obtains another channel estimate. The third and last step is when the data transmission begins. The transmitter uses its channel estimate to precode the signal, while the receiver uses its channel estimate in order to perform the decoding of the received signal. Similarly, the eavesdropper tries to decode the overheard signal. To increase the accuracy of its detection, the eavesdropper uses a channel calculated as an average of its two channel estimates.
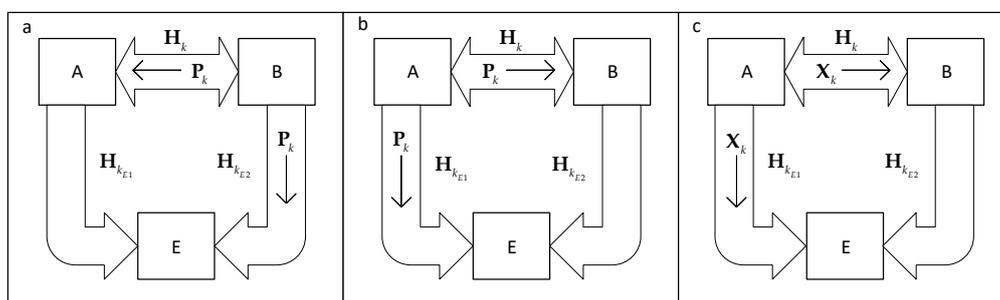
Figure 3. Steps for obtaining the channel estimates. (**a**) the receiver sends a training sequence, $\mathbf{P}_k$, that is received by the transmitter and the eavesdropper. (**b**) the transmitter sends a training sequence that is received by the receiver and the eavesdropper. (**c**) the transmitter begins sending data to the receiver, that is also received by the eavesdropper.

As described in [31], the channel can be expressed as

$$\mathbf{H}_k = \rho_A \hat{\mathbf{H}}_{k_A} + \boldsymbol{\epsilon}_k, \tag{3}$$

where $\hat{\mathbf{H}}_{k_A}$ is the channel estimate used by the transmitter, ρ_A is a correlation factor with the true channel, and $\boldsymbol{\epsilon}_k$ is the error associated to the channel estimation process (our analysis can be easily extended to other models for the channel estimation errors). This error $\boldsymbol{\epsilon}_k$ is characterized as a complex variable with Gaussian distribution and variance $2\sigma_N^2/\beta$, where σ_N^2 is the noise variance for a specific Signal-to-Noise Ratio (SNR) value and β is a scaling factor. For $\beta \to \infty$ and $\rho_A = 1$, there is a perfect channel estimation, i.e., $\hat{\mathbf{H}}_k = \mathbf{H}_{k_A}$.

The SVD decomposition of $\hat{\mathbf{H}}_{k_A}$ is as follows

$$\hat{\mathbf{H}}_{k_A} = \hat{\mathbf{U}}_{k_A} \hat{\mathbf{\Lambda}}_{k_A} \hat{\mathbf{V}}_{k_A}^H. \tag{4}$$

Therefore, the transmitter computes the precoded symbols with the $T \times 1$ vector $\hat{\mathbf{V}}_{k_A}$ as

$$\mathbf{X}_k = \hat{\mathbf{V}}_{k_A} \mathbf{S}_k'. \tag{5}$$

2.1.2. Reception

Both the correct receiver and the eavesdropper employ the same reception approach. However, the channel that they observe will be different, i.e., they will work with different channel estimates, since in general the eavesdropper is at a position different from the transmitter and the receiver. We also consider the pessimistic scenario where the eavesdropper knows the interleaving pattern in use (in practice, this could add an extra security layer, that is not considered in this paper).

The received signal can be expressed as

$$\mathbf{Z}_k = \mathbf{H}_k \mathbf{X}_k + \mathbf{N}_k, \tag{6}$$

where $\mathbf{N}_k$ denotes the frequency-domain additive white Gaussian noise (AWGN) samples associated to the kth sub-carrier.

Naturally, both the receiver and the eavesdropper must perform the decoding operation. For the intended receiver, B, we can define the channel as in (3), namely

$$\mathbf{H}_k = \rho_B \hat{\mathbf{H}}_{k_B} + \boldsymbol{\epsilon}_k. \tag{7}$$

We can assume that there is little difference between the estimation of the transmitter and the intended receiver, so it is reasonable to approximate $\rho_A = \rho_B \approx 1$. For the sake of simplicity, we will also assume that the power of the channel estimation error is equal for A and B (the generalization for other cases is straightforward).

The SVD decomposition done at the intended receiver's side is

$$\hat{\mathbf{H}}_{k_B} = \hat{\mathbf{U}}_{k_B} \hat{\mathbf{\Lambda}}_{k_B} \hat{\mathbf{V}}_{k_B}^H, \tag{8}$$

with $\hat{\mathbf{U}}_{k_B}$, $\hat{\mathbf{\Lambda}}_{k_B}$ and $\hat{\mathbf{V}}_{k_B}^H$ being the corresponding estimates of the matrices defined in (2). It should be noted that the eavesdropper cannot directly estimate the channel between A and B, since its actual value is never transmitted between A and B. Therefore, the eavesdropper can only approximate such estimation by estimating the channel between A and E and between B and E. The eavesdropper obtains these estimates by listening to the training sequences exchanged between A and B. We can define both of these channels as

$$\mathbf{H}_{k_{E1}} = \rho_{E1} \hat{\mathbf{H}}_{k_{E1}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{9}$$

and

$$\mathbf{H}_{k_{E2}} = \rho_{E2}\hat{\mathbf{H}}_{k_{E2}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k, \tag{10}$$

with ρ_{E1} and ρ_{E2} referring to the correlation between the different channels and the real channels and $\boldsymbol{\xi}_k$ being an appropriate Gaussian distributed error term with variance σ_N^2/β_M, where β_M is a scaling factor. Since the eavesdropper does not know the channel, we can assume that $\rho_{E1} = \rho_{E2} < 1$. As mentioned before, in order to improve the quality of the estimation of the channel between A and B, the eavesdropper can calculate an average of the estimates of the intermediate channels, i.e.,

$$\mathbf{H}_k = \frac{\mathbf{H}_{k_{E1}} + \mathbf{H}_{k_{E2}}}{2}. \tag{11}$$

As in conventional SVD techniques, the decoding is made by multiplying the received signal by the decoding matrix estimate $\hat{\mathbf{U}}_{k_B}^H$ for the intended receiver; or $\hat{\mathbf{U}}_{k_E}^H$ for the eavesdropper. Since the process is the same for both receivers, we will use $\hat{\mathbf{U}}_k^H$ as a place-holder for either receiver. The decoding is then computed as

$$\mathbf{W}_k' = \hat{\mathbf{U}}_k^H \mathbf{Z}_k, \tag{12}$$

where $\mathbf{W}_k'$ is a $C \times 1$ column vector with the interleaved, decoded symbols. These symbols can be written as

$$\mathbf{W}_k' = \hat{\boldsymbol{\Lambda}}_k \mathbf{S}_k' + \hat{\mathbf{U}}_k^H \mathbf{N}_k, \tag{13}$$

with $\hat{\boldsymbol{\Lambda}}_k$ corresponding to the diagonal matrix composed by the singular values of the estimated channel.

However, before performing equalization, we must group all the data symbols associated to a given stream, i.e., restore the original symbol order. This is done by applying the deinterleaving to the matrix $\mathbf{W}_k'$, which yields

$$\mathbf{W}_k = \hat{\boldsymbol{\Lambda}}_k' \mathbf{S}_k + \hat{\mathbf{U}}_k'^H \mathbf{N}_k'. \tag{14}$$

Thanks to the interleaving, each stream becomes affected by a frequency-selective channel, composed by the interleaving of the different singular values.

2.1.3. Multiple Eavesdroppers

Let us now assume a scenario with K eavesdroppers. Moreover, let us consider the worst case, i.e., the case where the different eavesdroppers are co-located and can perform joint estimation and equalisation. Under these conditions, we can model the existence of K eavesdroppers by considering one eavesdropper with KR receive antennas. Thus, the channel being estimated by the eavesdroppers can be defined as

$$\mathbf{H}_{k_E} = \frac{\mathbf{H}_{k_{E1}} + \mathbf{H}_{k_{E2}}}{2}. \tag{15}$$

The received signal $\mathbf{Z}_{k_E}$ is expressed as

$$\mathbf{Z}_{k_E} = \mathbf{H}_{k_E}\mathbf{X}_k + \mathbf{N}_k. \tag{16}$$

It should be noted that the eavesdroppers do not require any changes to the equalization algorithm, since the number of singular values is the same, not to mention they can take advantage of the increased singular value power due to employing more receiving antennas. Considering the SVD, the channel represented in (15) can be decomposed as

$$\hat{\mathbf{H}}_{k_E} = \hat{\mathbf{U}}_{k_E} \hat{\boldsymbol{\Lambda}}_{k_E} \hat{\mathbf{V}}_{k_E}^H, \tag{17}$$

where $\hat{\mathbf{\Lambda}}_{k_E}$ is a $C \times C$ diagonal matrix composed by the singular values of $\hat{\mathbf{H}}_{k_E}$, $\hat{\mathbf{V}}_{k_E}$ is the $T \times T$ precoding matrix, that is not utilised by the eavesdroppers, and $\hat{\mathbf{U}}_{k_E}$ is the $KR \times T$ decoding matrix, computed economically so as to not have null columns.

2.1.4. Line-of-Sight Link Scenario

Another possible scenario is the one where there is LOS between the transmitter and both the receiver and eavesdropper. Under these conditions, the channel is defined as the sum of a LOS component (that does not suffer fading effects) with several multipath rays (assumed uncorrelated and with fading effects). In a worst case scenario, we can assume that the eavesdropper can estimate the LOS component (eventually with a certain error), although that is not feasible for the remaining multipath rays [32]. In this case, we define the channel as

$$\mathbf{H}_{k,los} = \mathbf{D}_{k_{los}} + \mathbf{R}_{k_{mp}}, \tag{18}$$

where $\mathbf{D}_{k_{los}}$ is the low-fading, highly-correlated LOS component and $\mathbf{R}_{k_{mp}}$ is the high-fading multipath component of the channel. We then substitute this channel in (3) and (7), as

$$\mathbf{H}_{k,los} = \rho_A \hat{\mathbf{H}}_{k_A,los} + \boldsymbol{\epsilon}_k, \tag{19}$$

$$\mathbf{H}_{k,los} = \rho_B \hat{\mathbf{H}}_{k_B,los} + \boldsymbol{\epsilon}_k. \tag{20}$$

The intended receiver and transmitter's remaining operations are calculated as described previously.

The eavesdropper, however, cannot estimate the multipath component of the channel, and must instead rely on the estimate of the LOS component. We define this component as

$$\mathbf{D}_{k_{los}} = \frac{\mathbf{H}_{k_{E1},los} + \mathbf{H}_{k_{E2},los}}{2}, \tag{21}$$

where

$$\mathbf{H}_{k_{E1},los} = \rho_{E1} \hat{\mathbf{H}}_{k_{E1},los} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{22}$$

and

$$\mathbf{H}_{k_{E2},los} = \rho_{E2} \hat{\mathbf{H}}_{k_{E2},los} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k. \tag{23}$$

In this scenario, the channel estimates $\hat{\mathbf{H}}_{k_{E1},los}$ and $\hat{\mathbf{H}}_{k_{E2},los}$ only concerns the LOS component between A and E and B and E, respectively. The difference between these estimates and the real channel will be proportional to the power of the multipath component. We define the ray power coefficient as

$$\alpha_{RP} = \frac{P_R}{P_D + P_R}, \tag{24}$$

where P_D and P_R are the powers of the LOS and multipath components, respectively. Clearly, if $\alpha_{RP} = 0$, the channel is only composed by the LOS component, whereas at $\alpha_{RP} = 1$ the channel is composed of only the multipath component.

2.1.5. Iterative Equalization

In order to reduce the ISI, we employ a nonlinear FDE technique based on the IB-DFE concept [24,33]. The IB-DFE is a frequency-domain receiver which utilizes an iterative equalization based on the minimum mean squared error (MMSE). This equalization is done on a sub-carrier basis, and is composed by a feedforward and feedback equalization, which is employed to remove the residual ISI. The equalization processes are iterative and can be repeated up to L times.

The set of equalized symbols associated with the kth sub-carrier and lth iteration are given by

$$\tilde{\mathbf{S}}_k^{(l)} = \mathbf{F}_k^{(l)} \mathbf{W}_k - \mathbf{B}_k^{(l)} \bar{\mathbf{S}}_k^{(l-1)}, \tag{25}$$

where $\bar{\mathbf{S}}_k$ is a $C \times 1$ matrix with the soft-decisions of the previous iteration, and $\mathbf{F}_k^{(l)}$ and $\mathbf{B}_k^{(l)}$ are the feedforward and feedback equalization matrices for the kth sub-carrier and lth iteration, respectively. The feedforward equalization matrix for the kth sub-carrier and lth iteration is defined as

$$\mathbf{F}_k^{(l)} = \frac{\hat{\mathbf{\Lambda}}_k'}{\left(1 - |\rho^{(l-1)}|^2\right) \hat{\mathbf{\Lambda}}_k'^2 + \frac{1}{\text{SNR}}}, \tag{26}$$

where $\rho^{(l-1)}$ denotes the block-wise reliability associated to the data estimated in the $(l-1)$th iteration (when $l = 1$, we have $\rho^{(0)} = 0$). On the other hand, the feedback equalization matrix is defined as

$$\mathbf{B}_k^{(l)} = \mathbf{F}_k^{(l)} \hat{\mathbf{\Lambda}}_k' - \mathbf{I}. \tag{27}$$

The soft-decision estimates of the transmitted data, employed in the feedback equalization, are calculated using the reliability of each bit in each symbol, expressed as a log-likelihood ratio (LLR), as

$$L_n^{(\text{I},i)} = \frac{2}{\sigma_i^2} \text{Re}\left(\tilde{s}_n^{(i)}\right), \tag{28}$$

and

$$L_n^{(\text{Q},i)} = \frac{2}{\sigma_i^2} \text{Im}\left(\tilde{s}_n^{(i)}\right), \tag{29}$$

where

$$\sigma_i^2 = \frac{1}{2} \mathbb{E}\left[\left|s_n - \tilde{s}_n^{(i)}\right|^2\right] \approx \frac{1}{2N} \sum_{n=0}^{N-1} \left|\hat{s}_n - \tilde{s}_n^{(i)}\right|^2. \tag{30}$$

After obtaining the LLR for each bit, we can calculate the soft decision of a given data symbol as

$$\bar{s}_n^{(i)} = \tanh\left(\frac{L_n^{(\text{I},i)}}{2}\right) + j \tanh\left(\frac{L_n^{(\text{Q},i)}}{2}\right). \tag{31}$$

The estimated data symbols are obtained through the hard-decision of the equalized symbols.

2.2. Secrecy Rate

The secrecy rate is defined as the difference between the capacity of the channel between A and B, and the capacity of the channel between A and E [34–36]. For simplicity, we define the total capacity as the sum of the capacity of each sub-carrier, i.e.,

$$C = \sum_{k=1}^{N} C_k, \tag{32}$$

where C_k denotes the capacity of a single sub-carrier, defined as [3]

$$C_k = I(\mathbf{X}_k, \mathbf{Z}_k), \tag{33}$$

where $I(\mathbf{X}_k, \mathbf{Z}_k)$ is the mutual information between the transmitted signal and the received signal, which can be computed by

$$I(\mathbf{X}_k, \mathbf{Z}_k) = H(\mathbf{Z}_k) - H(\mathbf{Z}_k|\mathbf{X}_k), \tag{34}$$

with $H(\mathbf{Z}_k)$ being the differential entropy of $\mathbf{Z}_k$ and $H(\mathbf{Z}_k|\mathbf{X}_k)$ being the conditional differential entropy of $\mathbf{Z}_k$ given $\mathbf{X}_k$. Since we know that $\mathbf{X}_k$ is independent from $\mathbf{N}_k$, we can simplify $H(\mathbf{Z}_k|\mathbf{X}_k) = H(\mathbf{N}_k)$ and define both entropies as

$$H(\mathbf{Z}_k) = \log_2 \left((\pi e)^C \det \left(\mathbf{H}_k \mathbf{R}_X \mathbf{H}_k^H + \mathbf{R}_N \right) \right), \tag{35}$$

and

$$H(\mathbf{N}_k) = \log_2 \left((\pi e)^C \det \left(\mathbf{R}_N \right) \right), \tag{36}$$

where $\mathbf{R_X} = \sigma_X^2 \mathbf{I}$ and $\mathbf{R_N} = \sigma_N^2 \mathbf{I}$, with σ_X^2 and σ_N^2 corresponding to the variances of $\mathbf{X}_k$ and $\mathbf{N}_k$, respectively. By substituting (35) and (36) in (34), we can write

$$I(\mathbf{X}_k, \mathbf{Z}_k) = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_c|^2 \text{SNR} \right). \tag{37}$$

Since we have two different transmitter-receiver pairs, we can, likewise, define two different system capacities. Let us start by defining the system capacity associated with the link from A to B (i.e., the capacity of the intended receiver), which is given by

$$C_k^{AB} = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_c \rho_B|^2 \frac{\sigma_X^2}{\sigma_N^2 + \sigma_B^2} \right), \tag{38}$$

where σ_B^2 is the power of the interference associated with the imperfect channel estimation, given by

$$2\sigma_B^2 = \mathbb{E}\left[\hat{\mathbf{\Lambda}}_{k_B}^I \hat{\mathbf{\Lambda}}_{k_B}^{IH} \right], \tag{39}$$

with $\hat{\mathbf{\Lambda}}_{k_B}^I$ denoting a matrix comprised of the interference in the receiver, which can be computed as

$$\hat{\mathbf{\Lambda}}_{k_B}^I = \hat{\mathbf{\Lambda}}_{k_B} - \text{diag}\left(\hat{\mathbf{\Lambda}}_{k_B} \right). \tag{40}$$

Similarly, we can define the capacity of the eavesdropper as

$$C_k^{AE} = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_{c_E} \rho_E|^2 \frac{\sigma_X^2}{\sigma_N^2 + \sigma_E^2} \right), \tag{41}$$

where ρ_E is a simplification defined as $\rho_E = \rho_{E1} = \rho_{E2}$, and σ_E^2 is the interference power due to the imperfect channel estimation, which is larger than σ_B^2, and is computed as

$$2\sigma_E^2 = \mathbb{E}\left[\hat{\mathbf{\Lambda}}_{k_E}^I \hat{\mathbf{\Lambda}}_{k_E}^{IH} \right]. \tag{42}$$

Likewise, $\hat{\mathbf{\Lambda}}_{k_E}^I$ is the interference matrix computed as

$$\hat{\mathbf{\Lambda}}_{k_E}^I = \hat{\mathbf{\Lambda}}_{k_E} - \text{diag}\left(\hat{\mathbf{\Lambda}}_{k_E} \right). \tag{43}$$

With (38) and (41), we are able to obtain the total capacity by using (32). Moreover, we are also able to compute the secrecy rate, defined by the difference between the intended receiver's capacity and the eavesdropper's capacity, i.e.,

$$SR = C^{AB} - C^{AE}. \tag{44}$$

3. Results and Discussion

In this section we present a set of performance results regarding the BER and secrecy rate of the considered point-to-point MIMO system with, unless otherwise mentioned, $T = 8$ transmit

antennas and $R = 8$ receive antennas. These performance results involve scenarios with and without a LOS component and are obtained through Monte Carlo simulations. Unless otherwise stated, the block size is $N = 256$.

3.1. NLOS Scenario

We begin by analyzing the impact of the ρ_E factor in the receiver's performance. This can be observed in Figure 4, where we measure BER of the eavesdropper for different ρ_E values.
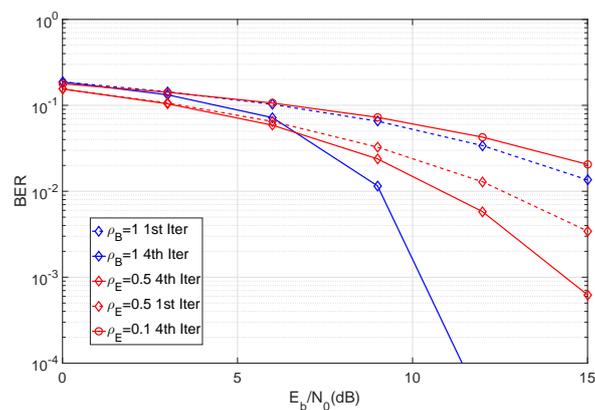
Figure 4. Comparison of BER for different values of ρ_E, with $\beta_N = \beta_M = \infty$.

From the figure, it can be observed that the system performance can be severely degraded at low levels of ρ_E. In accordance with our system definition, it is not unreasonable to assume that the eavesdropper will operate with small values of ρ_E. In the next set of results, we compute the secrecy rate of the system under different conditions. Figure 5 shows the secrecy rate as a function of ρ_E, considering different MIMO configurations.
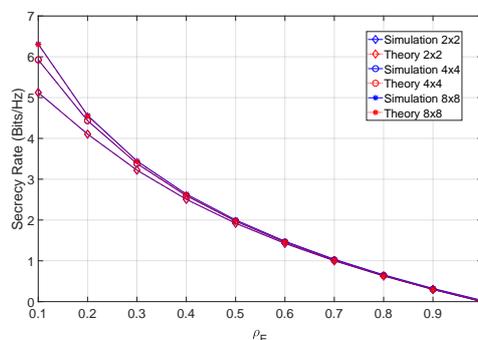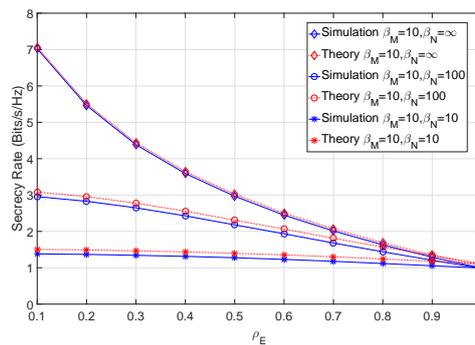

Figure 5. Secrecy rate of the system for an SNR of 12 dB and different MIMO configurations.

From the figure it can be concluded that, with perfect CSI, the maximum attainable secrecy rate increases with the number of antennas of both users. Figure 6 shows the secrecy rate of an 8×8 system, considering different values of β_N (i.e., considering different channel estimation errors on both receivers), at an SNR of 12 dB.

As expected, the addition of a channel estimation error negatively impacts the secrecy rate of the system, particularly for lower values of ρ_E. In Figure 7, we have introduced the channel mismatch error, represented by β_M, in addition to the channel estimation error and SNR of the previous simulations.
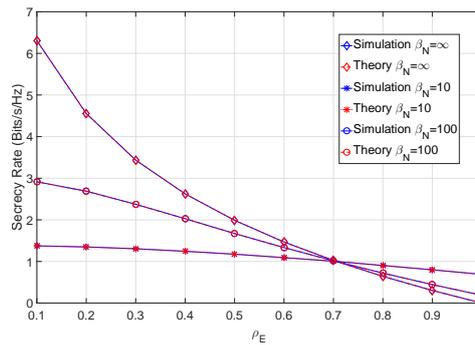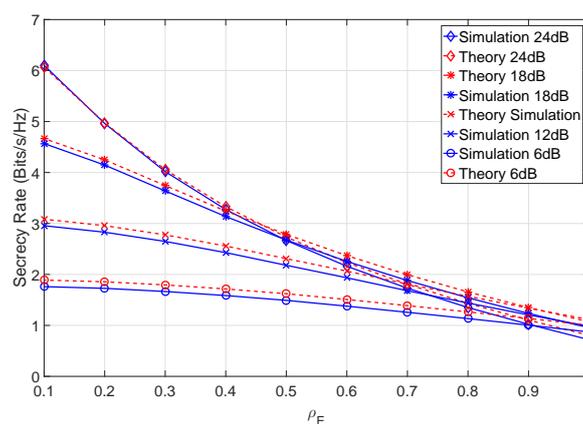
Figure 6. Secrecy rate of the system for an SNR of 12 dB and various levels of channel estimation error on both sides.

Figure 7. Secrecy rate of the system for an SNR of 12 dB and $\beta_M = 10$ with various levels of channel estimation error.

From the figure, it can be seen that when the channel estimation error assumes low levels, the secrecy rate increases. It should also be noted that even for high values of ρ_E, the secrecy rate is higher than in a scenario with no channel mismatch error. This is expected due to the mismatch error affecting only the eavesdropper's capacity. In addition, a relatively small difference between the theoretical and simulated results can be observed. This arises due to the residual error of the Gaussian approximation. Figure 8 combines various levels of SNR for the same levels of channel estimation and mismatch errors.
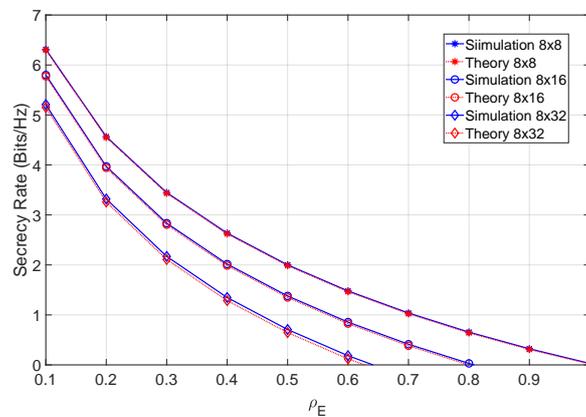

Figure 8. Secrecy rate of the system for different levels of SNR and with $\beta_N = 100$ and $\beta_M = 10$.

From the figure, it can be noted that a higher SNR leads to a higher secrecy rate, as expected, with the secrecy rate gain increasing further for smaller values of ρ_E.

3.2. Multiple Eavesdroppers Scenario

Let us now consider the existence of K eavesdroppers performing joint estimation and equalization. As mentioned before, this scenario is approximated by a single eavesdropper employing KR antennas, for $K > 1$. Figure 9 shows the secrecy rate of the system for $K = 1, 2$ and 4.

Figure 9. Secrecy rate of the system for various numbers of eavesdroppers, at 12 dB SNR.

From the figure, it can be seen that increasing the number of eavesdroppers leads to a lower attainable secrecy rate. This fact is not limited to the scenario without errors, as can be observed in the scenario with channel mismatch in Figure 10.
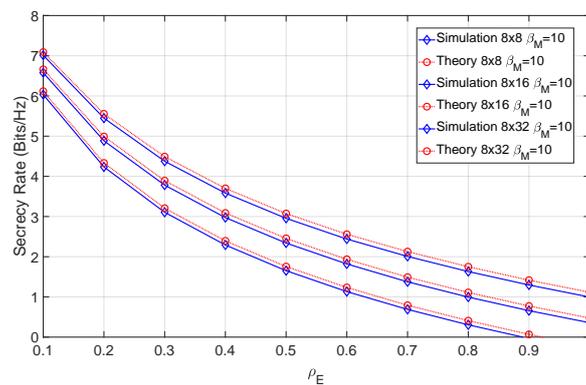
Figure 10. Secrecy rate of the system for various numbers of eavesdroppers and $\beta_M = 10$, at 12 dB SNR.

From this figure, it can be noted that by considering more eavesdroppers and/or antennas, the impact of the channel mismatch error can be reduced (or even eliminated).

3.3. LOS Scenario

In addition to varying ρ_E and the error factors, let us evaluate the secrecy rate of a scenario where we also vary the ray power ratio between multipath component and main LOS component. Figure 11 shows the secrecy rate with no errors, considering different values of ρ_E and different ray power coefficients α_{RP}.

From the figure it can be observed that the higher the ray power ratio, the higher the achievable secrecy rate. In fact, this is somewhat expected, since the component that the eavesdropper can estimate contributes less to the total channel power. Let us now consider a scenario with imperfect CSI. Figure 12 shows the secrecy rate when the SNR is 12 dB and different values of α_{RP} are considered.
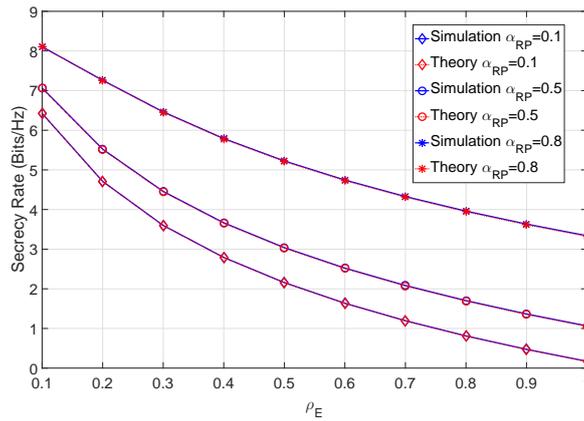
Figure 11. Secrecy rate of the system for various ray power ratios with $\beta_N = \infty$.
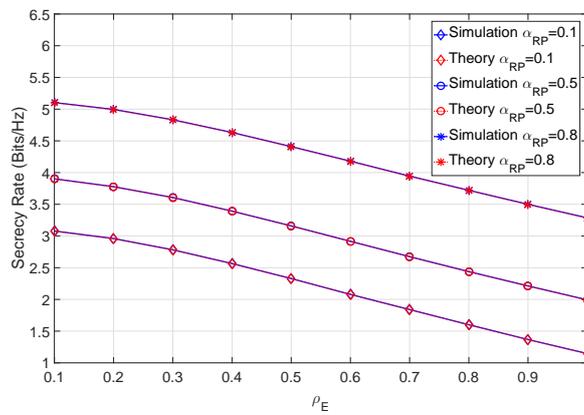

Figure 12. Secrecy rate of the system for various ray power ratios with $\beta_N = 100$ at 12 dB SNR.

The unknown multipath component introduces a permanent error in the eavesdropper, which accounts for the higher secrecy rate at $\rho_E = 1$, similar to the mismatch error. In Figure 13, we have introduced the mismatch error to the previous scenario.
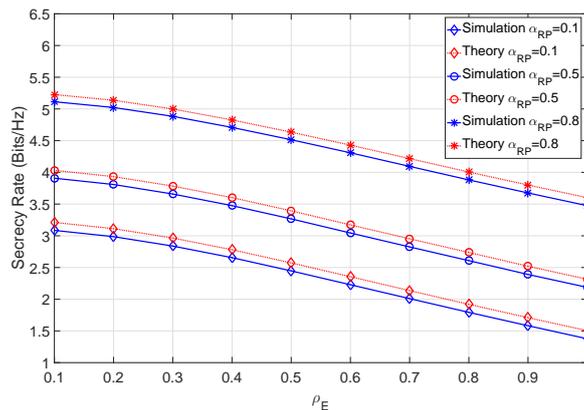

Figure 13. Secrecy rate of the system for various ray power ratios with $\beta_N = 100$ and $\beta_M = 10$ at 12 dB SNR.

We verify that the mismatch error leads to an overall increased secrecy rate at all power ratios, since by varying this ratio, only the eavesdropper's channel estimate and the corresponding capacity is affected.

4. Conclusions

In this paper, we proposed a physical security level against eavesdroppers which is based on MIMO-SVD schemes along with SC-FDE techniques. The security potential was studied, and it was shown that the secrecy rate can increase sharply as the distance between eavesdropper and transmitter or receiver increases. It was also demonstrated that in LOS scenarios, the secrecy rate increased with the multipath component's power. Therefore, MIMO-SVD schemes combined with SC-FDE tecnhiques can be an efficient option for highly secure MIMO communications.

Author Contributions: Conceptualization, R.D.; Funding acquisition, P.M. and L.M.C.; Investigation, J.M.; Project administration, P.M. and L.M.C.; Software, J.M.; Supervision, R.D.; Writing—original draft, J.M.; Writing—review & editing, J.G.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Foschini, G.; Gans, M. On limits of wireless communications in a fading environment when using multiple antennas. *Wirel. Pers. Commun.* **1998**, *6*, 311–335. [CrossRef]
2. Wolniasky, P.; Foschini, G.; Golden, G.; Valenzuela, R. V-Blast: An architecture for realizing very high data rates over rich-scattering wireless channel. In Proceedings of the 1998 URSI International Symposium on Signals, Systems, and Electronics, Pisa, Italy, 29 September–2 October 1998.
3. Telatar, I. Capacity of multi-antenna Gaussian channels. *Eur. Trans. Telecommun.* **1999**, *10*, 585–595. [CrossRef]
4. Xue, Y.; Zhang, J.; Jin, S.; Gao, X. On achievable rate of massive MIMO multiple access channels via virtual representation. *Phys. Commun.* **2016**, *20*, 133–140. [CrossRef]
5. Paulraj, A.J.; Gore, D.A.; Nabar, R.U.; Bolcskei, H. An overview of MIMO communications—A key to gigabit wireless. *Proc. IEEE* **2004**, *92*, 198–218. [CrossRef]
6. 3GPPP. *Physical Layers Aspects for Evolved UTRA*; TR 25.814 3GPPP: Valbonne, France, 2006.
7. Boccardi, F.; Heath, R.W.; Lozano, A.; Marzetta, T.L.; Popovski, P. Five disruptive technology directions for 5G. *IEEE Commun. Mag.* **2014**, *52*, 74–80. [CrossRef]
8. Ali, B.; Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* **2018**, *18*, 817. [CrossRef]
9. Shiu, Y.; Chang, S.Y.; Wu, H.; Huang, S.C.-H.; Chen, H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
10. Melki, R.; Noura, H.; Mansour, M.; Chehab, A. A survey on OFDM physical layer security. *Phys. Commun.* **2019**, *32*, 1–30. [CrossRef]
11. Mucchi, L.; Nizzi, F.; Pecorella, T.; Fantacci, R.; Esposito, F. Benefits of Physical Layer Security to Cryptography: Tradeoff and Applications. In Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sochi, Russia, 3–6 June 2019; pp. 1–3.
12. Pan, F.; Pang, Z.; Luvisotto, M.; Xiao, M.; Wen, H. Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions. *IEEE Ind. Electron. Mag.* **2018**, *12*, 18–27. [CrossRef]
13. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
14. Gopala, P.; Lai, L.; El Gamal, H. On the secrecy capacity of fading channels. *IEEE Trans Inf. Theory* **2008**, *54*, 5059–5067. [CrossRef]
15. Romero-Zurita, N.; Ghogho, M.; McLernon, D. Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation. *Phys. Commun.* **2011**, *4*, 313–321. [CrossRef]
16. Ankarali, Z.; Arslan, H. Cyclic feature suppression for physical layer security. *Phys. Commun.* **2017**, *25*, 588–597. [CrossRef]

17. Renna, F.; Laurenti, N.; Poor, H.V. Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1354–1367. [CrossRef]

18. Wu, C.; Lan, P.; Yeh, P.; Lee, C.; Cheng, C. Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1687–1700. [CrossRef]

19. Madeira, J.; Guerreiro, J.; Dinis, R. Iterative Frequency-Domain Detection for MIMO Systems with Strong Nonlinear Distortion Effects. In Proceedings of the IEEE 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICuMT '2018), Moscow, Russia, 5–9 November 2018

20. Lebrun, G.; Gao, J.; Faulkner, M. MIMO transmission over a time-varying channel using SVD. *IEEE Trans. Wirel. Commun.* **2005**, *4*, 757–764. [CrossRef]

21. Daniels, R.C.; Heath, R.W., Jr. Modeling ordered subcarrier SNR in MIMO-OFDM wireless links. *Phys. Commun.* **2011**, *4*, 275–285. [CrossRef]

22. Yang, H.; Marzetta, T.L. Performance of conjugate and zero-forcing beamforming in large-scale antenna systems. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 172–179. [CrossRef]

23. Kang, M.; Alouini, M. A comparative study on the performance of MIMO MRC systems with and without cochannel interference. *IEEE Trans. Commun.* **2004**, *52*, 1417–1425. [CrossRef]

24. Benvenuto, N.; Tomasin, S. Block iterative DFE for single carrier modulation. *Electron. Lett.* **2002**, *38*, 1144–1145. [CrossRef]

25. Busari, S.A.; Huq, K.M.S.; Mumtaz, S.; Rodriguez, J. Terahertz Massive MIMO for Beyond-5G Wireless Communication. In Proceedings of the 2019 IEEE International Conference on Communications (ICC 2019), Shanghai, China, 20–24 May 2019; pp. 1–6.

26. Aly, R.M.; Zaki, A.; Badawi, W.K.; Aly, M.H. Time Coding OTDM MIMO System Based on Singular Value Decomposition for 5G Applications. *Appl. Sci.* **2019**, *9*, 2691. [CrossRef]

27. Khandaker, M.R.A.; Masouros,C.; Wong, K. Constructive Interference Based Secure Precoding: A New Dimension in Physical Layer Security. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2256–2268. [CrossRef]

28. Dinis, R.; Montezuma, P.; Souto, N.; Silva, J. Iterative Frequency-Domain Equalization for general constellations. In Proceedings of the 2010 IEEE Sarnoff Symposium, Princeton, NJ, USA, 12–14 April 2010; pp. 1–5.

29. Guerreiro, J.; Dinis, R.; Montezuma, P.; da Silva, M.M. On the Achievable Performance of Nonlinear MIMO Systems. *IEEE Commun. Lett.* **2019**, *23*, 1725–1729. [CrossRef]

30. Ahrens, A.; Benavente-Peces, C.; Aboltins, A. Performance comparison of SVD- and GMD-assisted MIMO systems. In Proceedings of the Advances in Wireless and Optical Communications (RTUWO), Riga, Latvia, 5–6 November 2015; pp. 5–12.

31. Guerreiro, J.; Dinis, R.; Montezuma, P. Analytical Performance Evaluation of Precoding Techniques for Nonlinear Massive MIMO Systems With Channel Estimation Errors. *IEEE Trans. Commun.* **2018**, *66*, 1440–1451. [CrossRef]

32. Zhang, J.; Yuen, C.; Wen, C.-K.; Jin, S.; Wong, K.-K.; Zhu, H. Achievable ergodic secrecy rate for MIMO SWIPT wiretap channels. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 453–458.

33. Benvenuto, N.; Dinis, R.; Falconer, D.; Tomasin, S. Single Carrier Modulation With Nonlinear Frequency Domain Equalization: An Idea Whose Time Has Come-Again. *Proc. IEEE* **2010**, *98*, 69–96. [CrossRef]

34. Bustin, R.; Liu, R.; Poor, H.V.; Shamai, S. An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*. [CrossRef]

35. Oggier, F.; Hassibi, B. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 4961–4972. [CrossRef]

36. Obeed, M.; Mesbah, W. Efficient algorithms for physical layer security in two-way relay systems. *Phys. Commun.* **2018**, *28*, 78–88. [CrossRef]