electronics

MDPI

Article

A Physical Layer Security Technique for NOMA Systems with MIMO SC-FDE Schemes

João Madeira [1,*], João Guerreiro [2,3,*], Hugo Serra [3,*], Rui Dinis [3,4,*], Paulo Montezuma [3,4,*] and Luís Miguel Campos [5,*]

1 KT, Koala Tech LDA, 2825-182 Caparica, Portugal
2 UAL, Universidade Autónoma de Lisboa, 1169-023 Lisboa, Portugal
3 IT, Instituto de Telecomunicações, 1049-001 Lisboa, Portugal
4 FCT, Universidade Nova de Lisboa, 2829-516 Caparica, Portugal
5 PDMFC, Projecto Desenvolvimento Manutenção Formação e Consultadoria LDA., 1300-609 Alcântara, Portugal
* Correspondence: jf.madeira@campus.fct.unl.pt (J.M.); jfguerreiro@autonoma.pt (J.G.); hugoaaserra@gmail.com (H.S.); rdinis@fct.unl.pt (R.D.); pmc@fct.unl.pt (P.M.); luis.campos@pdmfc.com (L.M.C.)

Received: 11 December 2019; Accepted: 3 January 2020; Published: 1 February 2020

Abstract: Current wireless communication systems employ Multi-Input, Multi-Output (MIMO) techniques to increase spectral efficiency, at the cost of higher hardware complexity. Most of these systems continue to employ traditional Orthogonal Multiple Access (OMA) schemes, which are suboptimal when compared to Non-Orthogonal Multiple Access (NOMA) schemes. By combining NOMA with MIMO, it is possible to achieve higher spectral efficiencies. However, security in NOMA-MIMO systems remains a problem. In this paper, we study the physical layer security issues of a power based NOMA-MIMO system with a Singular Value Decomposition (SVD) scheme, employed along with Single Carrier with Frequency Domain Equalization (SC-FDE) techniques. We consider a scenario where there is an unintended eavesdropper attempting to listen to the messages being exchanged. It is shown that the higher the channel estimate correlation between transmitter and receiver, the higher the secrecy rate, particularly for a scenario where there is a Line-Of-Sight (LOS) between all users. Therefore, power based NOMA MIMO-SVD schemes, combined with SC-FDE, can be considered efficient options for highly secure MIMO communications.

Keywords: MIMO; NOMA; SC-FDE; physical layer security; SVD

1. Introduction

The increasing requirements for telecommunication systems have led to the research of Multiple-Input, Multiple-Output (MIMO) techniques, due to their large capacity gains over traditional single antenna system techniques [1]. In fact, these techniques have already been employed in recent standards, such as Wi-Fi [2] and LTE [3], and will be integrated in 5G systems [4].

In traditional Orthogonal Multiple Access (OMA) systems, radio resources are allocated to users in an orthogonal fashion (OFDMA, orthogonal CDMA, etc.), that is the uncoded messages meant for different users are never superimposed in the time and frequency domains. These systems, ideally, have no inter-user interference and require no additional processing for separating user's at the receiver. However, due to new demands to further increase spectrum efficiency, Non-Orthogonal Multiple Access (NOMA) schemes are quickly surging as solutions due to their higher spectrum efficiency [5,6], even for mmWave systems [7]. In a NOMA scheme, two or more users' messages are superimposed in the time and frequency domains, and user separation can be made in the power

domain, leading to the so-called power domain NOMA [8]. It is also possible to allocate users among clusters [9]; however, in this work, we assume only two users, which can be approximated as a single cluster scenario [10]. The detection of the different users usually resorts to Successive Interference Cancellation (SIC) techniques.

Although there is a great benefit in adopting NOMA schemes, the security requirements are higher than the ones of traditional OMA schemes. This is explained by the fact that, when performing the SIC process, a user may decode messages meant for other users. Therefore, NOMA schemes can greatly benefit from Physical Layer Security (PLS) schemes [11–14], which can be combined with upper layer security techniques to ensure the confidentiality of a user's message [15].

For this purpose, we chose to analyze the PLS characteristics of a Single Carrier (SC) NOMA-MIMO system employing Frequency Domain Equalization (FDE). Although there are many published works on PLS techniques, most of them focus on Orthogonal Frequency Division Multiplexing (OFDM) [16], and few are dedicated to SC systems. In [17], an SC system is analyzed, however, it does not consider a NOMA scenario, which poses additional security concerns. As is widely known, SC-FDE systems are appealing due to their lower Peak-to-Average Power Ratio (PAPR) when compared to multicarrier schemes. Moreover, when combined with non-linear iterative equalization techniques to mitigate Inter-Symbol Interference (ISI), such as Iterative Block-Decision Feedback Equalization (IB-DFE), they can achieve excellent performance, making this technique appealing for applications where there are strict energy efficiency requirements, as well as highly frequency selective channels. The security potential can be analyzed under various scenarios, such as in [18], where a friendly jammer and an eavesdropper were considered, or in [19], where a jammer and an eavesdropper worked together in an attempt to eavesdrop the system, or even through the use of artificial noise sequences at the transmitter [20]. This makes a direct comparison between these scenarios a challenging task. As such, in this work, we consider a simpler scenario with two independent eavesdroppers, which attempt to eavesdrop two different users.

In this work, we consider a novel Singular Value Decomposition (SVD) technique for separating user streams in MIMO-NOMA SC-FDE systems. More concretely, we analyze the security potential of this scheme in a scenario with an eavesdropper located near each user. Even in LOS scenarios, it is shown that the secrecy rate of the MIMO-NOMA system can be kept high if the multipath component's power is relatively high.

This paper is organized as follows: In Section 2, we characterize the MIMO-NOMA system with its intended receivers, B and C, and eavesdropper E, with varying positions and targets. Section 3 concerns the system capacity and presents secrecy rate calculations. Section 4 shows the simulated Bit Error Rate (BER) and secrecy rate for all transmitter-receiver sets. Lastly, Section 5 concludes this paper.

2. Materials and Methods

2.1. System Characterization

In this paper, we consider a three user system, where one user, the transmitter A, attempts to communicate with the other two users, receivers B and C. The receivers are separated by a large distance, d, with one receiver, B, being close to the transmitter, while C is placed far from the transmitter. The transmitter employs a power based NOMA scheme and transmits both users' signals at the same time. In addition, there is an eavesdropper near each user, attempting to listen to the messages being transmitted. A diagram summarizing this scenario can be seen in Figure 1. Although the transmitter's position may vary, it is assumed that the distance to all other users is always much greater than the wavelength of the transmitted signal. The transmitter employs T antennas, while the receivers and eavesdropper employ R antennas. In order to handle the highly frequency selective channel, we employ an SC-FDE technique, combined with an appropriate Cyclic Prefix (CP) larger than the maximum overall channel impulse response.

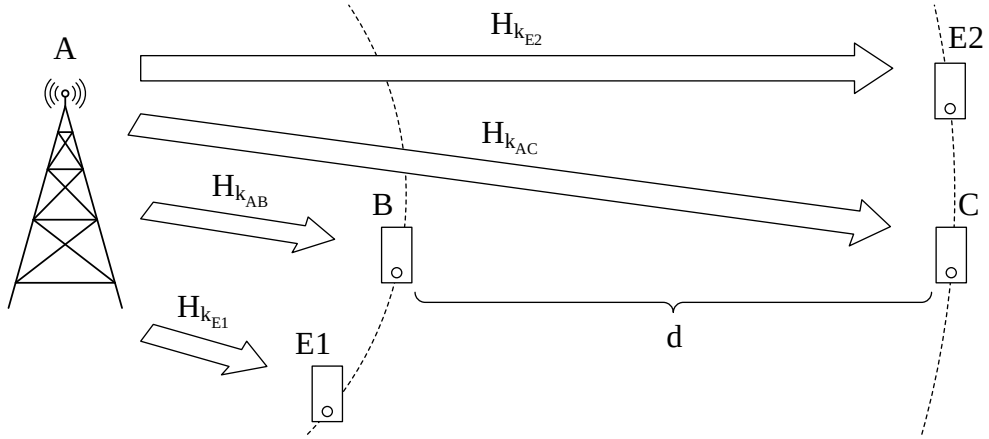

Figure 1. A diagram of the proposed NOMA scenario, with 3 users, 1 transmitting user and 2 receiving users, and 2 eavesdroppers.

The transmitter sends C data blocks, with $C \leq R$, and each data block is composed by the sum of two blocks of N Quadrature Phase Shift Keying (QPSK) symbols with differing power (the generalization to other constellations is straightforward [21]). Contrary to the single user system studied in [17], fir the power domain NOMA scenario of this work, we must define the symbols to be transmitted to both users. The data symbols transmitted for user B are denoted by the $C \times N$ matrix $\mathbf{s}_B$, with each data stream defined as an $N \times 1$ vector $\mathbf{s}_B^{(c)} = [s_{1_B}^{(c)}\ s_{2_B}^{(c)}\ \cdots\ s_{N_B}^{(c)}]$. In that context, $s_{n_B}^{(c)}$ represents the QPSK symbol at the n^{th} time instant of the c^{th} data stream. The frequency domain counterpart of the data to be transmitted is denoted by $\mathbf{S}_B$. The group of symbols associated with the k^{th} subcarrier are defined as $\mathbf{S}_{k_B} = [S_{k_B}^{(1)}\ S_{k_B}^{(2)}\ ..\ S_{k_B}^{(C)}]$. The symbols for User C are defined identically to the symbols for User B and denoted by $\mathbf{s}_C$, $\mathbf{s}_C^{(c)}$, $\mathbf{S}_C$, and $\mathbf{S}_{k_C}$, respectively. Under these conditions, the transmitted data at n^{th} time instant are defined as:

$$\mathbf{s}_n = \mathbf{s}_B + \mathbf{s}_C, \tag{1}$$

with a frequency domain counterpart defined as:

$$\mathbf{S}_k = \mathbf{S}_{k_B} + \mathbf{S}_{k_C}. \tag{2}$$

Since we are considering two receivers that are not co-located, we can define two channels, one from A to B and another from A to C. The frequency response for the k^{th} subcarrier of the channel from A to B is defined as:

$$\mathbf{H}_{k_{AB}} = \begin{bmatrix} H_{k_{AB}}^{(1,1)} & H_{k_{AB}}^{(1,2)} & \cdots & H_{k_{AB}}^{(1,T)} \\ H_{k_{AB}}^{(2,1)} & H_{k_{AB}}^{(2,2)} & \cdots & H_{k_{AB}}^{(2,T)} \\ \vdots & \vdots & \ddots & \vdots \\ H_{k_{AB}}^{(R,1)} & H_{k_{AB}}^{(R,2)} & \cdots & H_{k_{AB}}^{(R,T)} \end{bmatrix}, \tag{3}$$

and the frequency response for the k^{th} subcarrier of the channel from A to C is defined as:

$$\mathbf{H}_{k_{AC}} = \begin{bmatrix} H_{k_{AC}}^{(1,1)} & H_{k_{AC}}^{(1,2)} & \cdots & H_{k_{AC}}^{(1,T)} \\ H_{k_{AC}}^{(2,1)} & H_{k_{AC}}^{(2,2)} & \cdots & H_{k_{AC}}^{(2,T)} \\ \vdots & \vdots & \ddots & \vdots \\ H_{k_{AC}}^{(R,1)} & H_{k_{AC}}^{(R,2)} & \cdots & H_{k_{AC}}^{(R,T)} \end{bmatrix}. \tag{4}$$

In any MIMO system, the different channels must be separated, so as to avoid cross-channel interference. In this work, we employ a technique that combines precoding and decoding, which is based on the SVD in [22]. Calculating the SVD of the channel matrix requires Channel State Information (CSI) at both receivers and at the transmitter. This CSI can be obtained through the exchange of pilot sequences at the start of the transmission. In a Time Division Duplexing (TDD) system, this process is greatly simplified due to the reciprocity of the channel.

The SVD of each channel matrix is defined as:

$$\mathbf{H}_{k_{AB}} = \mathbf{U}_{k_{AB}} \mathbf{\Lambda}_{k_{AB}} \mathbf{V}_{k_{AB}}^{H}, \tag{5}$$

and:

$$\mathbf{H}_{k_{AC}} = \mathbf{U}_{k_{AC}} \mathbf{\Lambda}_{k_{AC}} \mathbf{V}_{k_{AC}}^{H}. \tag{6}$$

For simplicity's sake, we omit the channel identifier (i.e., AB or AC) when we are referring to any channel. We denote $\mathbf{U}_k$ as the $R \times R$ decoding matrix, $\mathbf{V}_k$ as the $T \times T$ precoding matrix, and $\mathbf{\Lambda}_k$ as an $C \times C$ diagonal matrix composed by the singular values of $\mathbf{H}_k$, which are sorted in descending order according to their power.

2.2. Transmission

In a power domain NOMA scheme, the data meant for each user are sent at the same time and over the same channel, with differing transmitting power. In this work, we define the ratio between the power of $\mathbf{S}_{k_B}$ and $\mathbf{S}_{k_C}$ as α.

It is widely known that the performance of a given stream in an SVD system depends on the singular value power of that stream. A simple scheme for averaging the performance of all streams was proposed in [23], which consisted of interleaving the data symbols before applying the precoding technique. The interleaving scheme can be different for each user, as it only affects the data symbols. Therefore, we define the interleaved symbols for Users B and C as $\mathbf{S}'_{k_B}$ and $\mathbf{S}'_{k_C}$, respectively.

Before transmitting data, there is an initial training sequence exchange between all users, so as to obtain the channel matrices with which to compute the SVD. The exchange begins with the farthest user, C, sending a training sequence meant for the transmitter, which is ignored by B. In the next step, B sends a training sequence meant for the transmitter as well. Lastly, the transmitter sends a training sequence, followed by the precoded data to all users. In all steps, there is an eavesdropper that listens to all of the exchanged sequences and computes its own channel estimates.

As described in [24], the channel matrices associated with the k^{th} subcarrier can be defined as:

$$\mathbf{H}_{k_{AB}} = \rho_{A1} \hat{\mathbf{H}}_{k_{A1}} + \boldsymbol{\epsilon}_k, \tag{7}$$

and:

$$\mathbf{H}_{k_{AC}} = \rho_{A2} \hat{\mathbf{H}}_{k_{A2}} + \boldsymbol{\epsilon}_k, \tag{8}$$

where $\hat{\mathbf{H}}_{k_{A1}}$ and $\hat{\mathbf{H}}_{k_{A2}}$ are the channel estimates used by the transmitter, ρ_{A1} and ρ_{A2} are correlation factors with the true channels, and $\boldsymbol{\epsilon}_k$ is the error associated with 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 a 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 $\rho_{A1} = \rho_{A2} = 1$, there is a perfect channel estimation, i.e., $\hat{\mathbf{H}}_{k_{AB}} = \mathbf{H}_{k_{A1}}$ and $\hat{\mathbf{H}}_{k_{AC}} = \mathbf{H}_{k_{A2}}$. We define the SVD of the channel estimates as:

$$\hat{\mathbf{H}}_{k_{A1}} = \hat{\mathbf{U}}_{k_{A1}} \hat{\mathbf{\Lambda}}_{k_{A1}} \hat{\mathbf{V}}_{k_{A1}}^{H}, \tag{9}$$

and:

$$\hat{\mathbf{H}}_{k_{A2}} = \hat{\mathbf{U}}_{k_{A2}} \hat{\mathbf{\Lambda}}_{k_{A2}} \hat{\mathbf{V}}_{k_{A2}}^{H}. \tag{10}$$

Using the result of SVD, the transmitter performs the precoding operation defined as:

$$\mathbf{X}_k = \hat{\mathbf{V}}_{k_A1}\mathbf{S}'_{k_B} + \sqrt{\alpha}\hat{\mathbf{V}}_{k_A1}\mathbf{S}'_{k_C}, \tag{11}$$

where $\mathbf{X}_k$ is the signal to be transmitted and α is the ratio between the power transmitted meant for User C and the power transmitted meant for User B. Since the precoding operation only utilizes the channel estimate of the close user, additional information must be sent to allow the far user to complete the SVD process. The transmitter sends a partial key $\mathbf{Q}_k$, which is defined as:

$$\mathbf{Q}_k = \hat{\mathbf{V}}^H_{k_A1}\hat{\mathbf{V}}_{k_A2}. \tag{12}$$

Since $\mathbf{Q}_k$ is a unitary matrix, then for the case of a system with $T = R = 2$, this matrix can be written as:

$$\mathbf{Q}_k = \begin{bmatrix} a & b \\ -b^* \exp(j\phi) & a^* \exp(j\phi) \end{bmatrix}, \tag{13}$$

where a and b are complex coefficients such that $|a|^2 + |b|^2 = 1$, and the determinant of this matrix is given by:

$$\det(\mathbf{Q}_k) = \exp(j\phi). \tag{14}$$

Under this decomposition, the transmitter must send four parameters that allow for the reconstruction of the original matrix. These parameters are $|a|$, $\arg(a)$, $\arg(b)$, and $\det(\mathbf{Q}_k)$, which are all real valued quantities that can be quantized with a low resolution, so as to reduce the overhead associated with the transmission of the partial key.

2.3. Reception

The received signal at User B can be defined as:

$$\mathbf{Z}_{k_B} = \mathbf{H}_{k_{AB}}\mathbf{X}_k + \mathbf{N}_k, \tag{15}$$

while the received signal at User C is defined as:

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

Before decoding the symbols, both receivers employ the Iterative Block-Decision Feedback Equalization (IB-DFE) technique [25] with soft decisions. This technique utilizes feedback from the soft decided symbols to improve the equalization and mitigate the intersymbol interference in frequency selective channels. Figure 2 shows a simplified diagram of this system. However, it should be noted that this 2userscheme must be slightly changed for our power domain NOMA scenario, mainly due to the SIC and partial key requirements at each receiver.

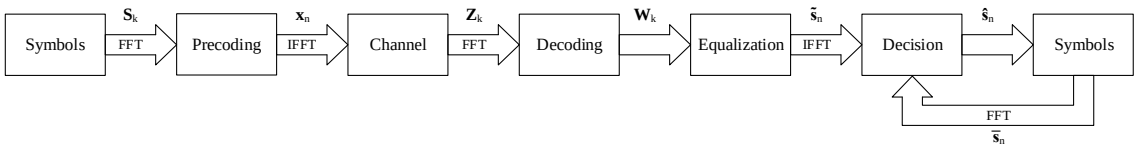

Figure 2. A diagram of the traditional SC system with precoding and decoding, employing an Iterative Block (IB)-DFE) receiver.

2.4. Receiver B

As described earlier, User B also computes a channel estimation, with the training sequence transmitted by A. We can express the channel as:

$$H_{k_{AB}} = \rho_B \hat{\mathbf{H}}_{k_B} + \boldsymbol{\epsilon}_k, \tag{17}$$

where ρ_B is a correlation factor with the true channel. It is not unreasonable to assume that there is a high correlation between the estimate of the receiver B and the transmitter; therefore, we can assume $\rho_{A1} = \rho_B \approx 1$. For simplicity, we assume that the error distribution of the channel estimate is the same for both A and B, though the generalization to other cases is straightforward. The SVD of the channel estimate at User B is written as:

$$\hat{\mathbf{H}}_{k_B} = \hat{\mathbf{U}}_{k_B} \hat{\mathbf{\Lambda}}_{k_B} \hat{\mathbf{V}}^H_{k_B}, \tag{18}$$

with $\hat{\mathbf{U}}_{k_B}$, $\hat{\mathbf{\Lambda}}_{k_B}$, and $\hat{\mathbf{V}}^H_{k_B}$ being the corresponding estimates of the matrices defined in (5).

As in conventional SVD techniques, the decoding is performed by multiplying the signal by the decoding matrix $\hat{\mathbf{U}}_{k_B}$, which is computed as:

$$\mathbf{W}'_{k_B} = \hat{\mathbf{U}}^H_{k_B} \mathbf{Z}_{k_B}, \tag{19}$$

where $\mathbf{W}'_{k_B}$ is a $C \times 1$ column vector with the interleaved, decoded symbols. This operation can be expanded as:

$$\begin{aligned} \mathbf{W}'_{k_B} &= \hat{\mathbf{U}}^H_{k_B} \mathbf{H}_{k_{AB}} \mathbf{X}_k + \hat{\mathbf{U}}^H_{k_B} \mathbf{N}_k \\ &= \hat{\mathbf{U}}^H_{k_B} \mathbf{H}_{k_{AB}} \mathbf{V}_{k_{A1}} (\mathbf{S}'_{k_B} + \sqrt{\alpha} \mathbf{S}'_{k_C}) + \hat{\mathbf{U}}^H_{k_B} \mathbf{N}_k \\ &= \hat{\mathbf{\Lambda}}_{k_{AB}} (\mathbf{S}'_{k_B} + \sqrt{\alpha} \mathbf{S}'_{k_C}) + \hat{\mathbf{U}}^H_{k_B} \mathbf{N}_k, \end{aligned} \tag{20}$$

with $\hat{\mathbf{\Lambda}}_{k_{AB}}$ corresponding to an estimate of the diagonal matrix composed by the singular values of the channel. Before performing equalization, however, the receiver must perform deinterleaving, to restore the original symbol order, yielding:

$$\mathbf{W}_{k_B} = \hat{\mathbf{\Lambda}}'_{k_{AB}} (\mathbf{S}_{k_B} + \sqrt{\alpha} \mathbf{S}_{k_C}) + \hat{\mathbf{U}}'^H_{k_B} \mathbf{N}'_k. \tag{21}$$

After the deinterleaving, each stream is affected by a frequency selective channel made up of the different singular values.

Before User B can detect its intended symbols, it must perform the SIC reception on the symbols intended for User C. In order to do so, it first performs detection on the stronger signal, which has a much higher Signal-to-Noise Ratio (SNR) than the wanted signal, making the detection simple.

The equalized signal is obtained by computing:

$$\tilde{\mathbf{S}}_{k_C} = \mathbf{F}_{k_{B1}} \mathbf{W}_{k_B}, \tag{22}$$

where the equalization factor $\mathbf{F}_{k_{B1}}$ is defined according to Minimum Mean Squared Error (MMSE) criterion as:

$$\mathbf{F}_{k_{B1}} = \frac{\hat{\mathbf{\Lambda}}'_{k_B}}{\hat{\mathbf{\Lambda}}'^2_{k_B} + \frac{1}{\sqrt{\text{ffSNR}}}}. \tag{23}$$

Subsequently, the receiver computes hard decisions of the transmitted symbols as:

$$\hat{\mathbf{S}}_{k_C} = \text{sign}\left(\text{Re}(\tilde{\mathbf{S}}_{k_C})\right) + j\,\text{sign}\left(\text{Im}(\tilde{\mathbf{S}}_{k_C})\right), \tag{24}$$

with $\hat{\mathbf{S}}_{k_C}$ being a hard decided estimate of the transmitted symbols meant for User C. Using this estimate, the receiver can perform detection on the intended symbols.

In the scenario where there is a nearby eavesdropper, E, attempting to listen to the message being sent to B, then it must attempt to estimate the channel between A and B. Since an eavesdropper cannot attempt to estimate this channel, it estimates two different channels, defined as:

$$\mathbf{H}_{k_{EB1}} = \rho_{EB1}\hat{\mathbf{H}}_{k_{EB1}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{25}$$

and:

$$\mathbf{H}_{k_{EB2}} = \rho_{EB2}\hat{\mathbf{H}}_{k_{EB2}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k, \tag{26}$$

where $\mathbf{H}_{k_{EB1}}$ is the channel between A and E, $\mathbf{H}_{k_{EB2}}$ is the channel between B and E, ρ_{EB1} and ρ_{EB2} are correlation coefficients with the true channels, and $\boldsymbol{\xi}_k$ is 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 $\rho_{EB1} = \rho_{EB2} < 1$. For simplicity's sake, we assume that $\rho_{EB1} = \rho_{EB2} = \rho_{EB}$. In order to increase the accuracy of the channel estimate, the receiver can compute the average of both intermediate channels, i.e.,

$$\mathbf{H}_{k_{AB}} = \frac{\mathbf{H}_{k_{EB1}} + \mathbf{H}_{k_{EB2}}}{2}. \tag{27}$$

Iterative Equalization

To reduce the ISI, the receiver and eavesdropper employ an iterative frequency domain equalization scheme based on the IB-DFE [25] and MMSE criterion, which performs both feedforward and feedback equalization at a subcarrier level. This equalization process can be repeated up to L times, which we fixed at $L = 4$ for this work.

The equalized symbols at the k^{th} subcarrier and l^{th} iteration are computed by:

$$\tilde{\mathbf{S}}_{k_B}^{(l)} = \mathbf{F}_{k_{B2}}^{(l)}\left(\mathbf{W}_{k_B} - \sqrt{\alpha}\hat{\boldsymbol{\Lambda}}_{k_B}^{'}\hat{\mathbf{S}}_{k_C}\right) - \mathbf{B}_{k_{B2}}^{(l)}\bar{\mathbf{S}}_{k_B}^{(l-1)}, \tag{28}$$

where $\mathbf{F}_{k_{B2}}^{(l)}$ is the feedforward factor, $\mathbf{B}_{k_{B2}}^{(l)}$ is the feedback factor, and $\bar{\mathbf{S}}_{k_B}^{(l-1)}$ are the soft decided symbols of the previous iteration (for $l = 1$, this is simply a null vector). The feedforward factor matrix is defined as:

$$\mathbf{F}_{k_{B2}}^{(l)} = \frac{\hat{\boldsymbol{\Lambda}}_{k_B}^{'}}{\left(1 - \left|\rho^{(l-1)}\right|^2\right)\hat{\boldsymbol{\Lambda}}_{k_B}^{'2} + \frac{1}{\text{SNR}}}, \tag{29}$$

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

$$\mathbf{B}_{k_B}^{(l)} = \mathbf{F}_{k_{B2}}^{(l)}\hat{\boldsymbol{\Lambda}}_{k_B}^{'} - \mathbf{I}. \tag{30}$$

2.5. Receiver C

The detection at User C is significantly different from the detection scheme employed in [17]. This is explained by the modifications required for the interleaving scheme and by the use of a partial key. As described earlier, User C also computes a channel estimation, with the training sequence transmitted by A. We can express the channel as:

$$H_{k_{AC}} = \rho_C\hat{\mathbf{H}}_{k_C} + \boldsymbol{\epsilon}_k. \tag{31}$$

where ρ_C is a correlation factor with the true channel. It is not unreasonable to assume that there is a high correlation between the estimate of the receiver C and the transmitter; therefore, we can assume $\rho_{A2} = \rho_C \approx 1$. For simplicity, we assume that the error distribution of the channel estimate is the same

for both A and C, though the generalization to other cases is straightforward. The SVD of the channel estimate at User C is written as:

$$\hat{\mathbf{H}}_{k_C} = \hat{\mathbf{U}}_{k_C} \hat{\mathbf{\Lambda}}_{k_C} \hat{\mathbf{V}}_{k_C}^H, \tag{32}$$

with $\hat{\mathbf{U}}_{k_C}$, $\hat{\mathbf{\Lambda}}_{k_C}$ and $\hat{\mathbf{V}}_{k_C}^H$ being the corresponding estimates of the matrices defined in (6).

As in conventional SVD techniques, the decoding is performed by multiplying the signal by the decoding matrix $\hat{\mathbf{U}}_{k_C}$, which is computed as:

$$\mathbf{W}'_{k_C} = \hat{\mathbf{U}}_{k_C}^H \mathbf{Z}_{k_C}, \tag{33}$$

where $\mathbf{W}'_{k_C}$ is a $C \times 1$ column vector with the interleaved, decoded symbols. This operation can be expanded as:

$$\begin{aligned} \mathbf{W}'_{k_C} &= \hat{\mathbf{U}}_{k_B}^H \mathbf{H}_{k_{AC}} \mathbf{X}_k + \hat{\mathbf{U}}_{k_C}^H \mathbf{N}_k \\ &= \hat{\mathbf{U}}_{k_C}^H \mathbf{H}_{k_{AC}} \mathbf{V}_{k_{A1}} (\mathbf{S}'_{k_B} + \sqrt{\alpha} \mathbf{S}'_{k_C}) + \hat{\mathbf{U}}_{k_C}^H \mathbf{N}_k \\ &= \hat{\mathbf{\Lambda}}_{k_{AC}} \mathbf{V}_{k_C}^H \mathbf{V}_{k_{A1}} (\mathbf{S}'_{k_B} + \sqrt{\alpha} \mathbf{S}'_{k_C}) + \hat{\mathbf{U}}_{k_C}^H \mathbf{N}_k, \end{aligned} \tag{34}$$

with $\hat{\mathbf{\Lambda}}_{k_{AC}}$ corresponding to an estimate of the diagonal matrix composed by the singular values of the channel. The received signal is then deinterleaved, so as to split the singular values amongst the streams, yielding:

$$\mathbf{W}_{k_C} = \hat{\mathbf{\Lambda}}'_{k_{AC}} \mathbf{V}'^H_{k_C} \mathbf{V}'_{k_{A1}} (\mathbf{S}_{k_B} + \sqrt{\alpha} \mathbf{S}_{k_C}) + \hat{\mathbf{U}}'^H_{k_C} \mathbf{N}'_k. \tag{35}$$

As was the case with Receiver B, this receiver performs the same iterative equalization, with the exception that it does not need to perform an initial first detection. The equalization is defined as:

$$\mathbf{Y}_{k_C}^{(l)} = \mathbf{F}_{k_C}^{(l)} \mathbf{W}_{k_C} - \mathbf{B}_{k_C}^{(l)} \bar{\mathbf{Y}}_{k_C}^{(l-1)}, \tag{36}$$

where $\mathbf{Y}_{k_C}^{(l)}$ is the equalized received signal at the k^{th} subcarrier and l^{th} iteration and $\bar{\mathbf{Y}}_{k_C}^{(l-1)}$ is the equalized signal estimate of the previous iteration (for $l = 1$, it is set to 0). However, unlike Receiver B, this receiver cannot complete the SVD on its own. Therefore, it makes use of the partial key $\hat{\mathbf{Q}}_k$, which is computed from the received parameters as:

$$\mathbf{Q}_k = \begin{bmatrix} \tilde{a} \exp j\tilde{\phi}_a & \tilde{b} \exp j\tilde{\phi}_b \\ -\tilde{b} \exp j(\tilde{\phi} - \tilde{\phi}_b) & \tilde{a} \exp j(\tilde{\phi} - \tilde{\phi}_a) \end{bmatrix}, \tag{37}$$

where $\tilde{a}$,$\tilde{\phi}_a$, $\tilde{\phi}_b$, and $\tilde{\phi}$ are the finite resolution quantized values transmitted by A and $\tilde{b}$ is obtained from $\tilde{b} = \sqrt{1 - \tilde{a}^2}$. Prior to applying the partial key, the equalized signal is interleaved, in order to match the SVD matrices. The equalized symbols estimates are expressed as:

$$\tilde{\mathbf{S}}_{k_C}^{\prime(l)} = \mathbf{Q}_k \mathbf{Y}_{k_C}^{\prime(l)}, \tag{38}$$

which are then deinterleaved into the equalized symbol estimates $\tilde{\mathbf{S}}_{k_C}^{(l)}$.

In the scenario where there is a nearby eavesdropper, E, attempting to listen to the message being sent to C, then it must attempt to estimate the channel between A and C. Since an eavesdropper cannot attempt to estimate this channel, it estimates two different channels, defined as:

$$\mathbf{H}_{k_{EC1}} = \rho_{EC1} \hat{\mathbf{H}}_{k_{EC1}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{39}$$

and:

$$\mathbf{H}_{k_{EC2}} = \rho_{EC2} \hat{\mathbf{H}}_{k_{EC2}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k, \tag{40}$$

where $\mathbf{H}_{k_{EC1}}$ is the channel between A and E, $\mathbf{H}_{k_{EC2}}$ is the channel between B and E, and ρ_{EC1} and ρ_{EC2} are correlation coefficients with the true channels. Since the eavesdropper does not know the channel, we can assume that $\rho_{EC1} = \rho_{EC2} < 1$. Once again, for simplicity's sake, we assume that $\rho_{EC1} = \rho_{EC2} = \rho_{EC}$. In order to increase the accuracy of the channel estimate, the receiver can compute the average of both intermediate channels, i.e.,

$$\mathbf{H}_{k_{AC}} = \frac{\mathbf{H}_{k_{EC1}} + \mathbf{H}_{k_{EC2}}}{2}. \tag{41}$$

2.6. Line-of-Sight Link Scenario

An additional scenario where there is LOS between the transmitter and all other users can be considered. In these conditions, the channel is defined as the sum of an LOS component (without fading effects) and several multipath rays (which are uncorrelated and have fading). In the worst case scenario, the eavesdropper can estimate the LOS component, albeit with a certain error; however, that is not feasible for the remaining multipath rays [26]. In this case, we define the channels as:

$$\mathbf{H}_{k_{AB},los} = \mathbf{D}_{k_{AB},los} + \mathbf{R}_{k_{AB},mp}, \tag{42}$$

and:

$$\mathbf{H}_{k_{AC},los} = \mathbf{D}_{k_{AC},los} + \mathbf{R}_{k_{AC},mp}, \tag{43}$$

where $\mathbf{D}_{k_{AB},los}$ and $\mathbf{D}_{k_{AC},los}$ are the low fading, highly correlated LOS components and $\mathbf{R}_{k_{AB},mp}$ and $\mathbf{R}_{k_{AC},mp}$ are the high fading multipath components of the respective channels. We then substitute these channels in (7), (8), (17), and (31) as:

$$\mathbf{H}_{k_{AB},los} = \rho_{A1}\hat{\mathbf{H}}_{k_{A1},los} + \boldsymbol{\epsilon}_k, \tag{44}$$

$$\mathbf{H}_{k_{AC},los} = \rho_{A2}\hat{\mathbf{H}}_{k_{A2},los} + \boldsymbol{\epsilon}_k, \tag{45}$$

$$\mathbf{H}_{k_{AB},los} = \rho_{B}\hat{\mathbf{H}}_{k_{B},los} + \boldsymbol{\epsilon}_k, \tag{46}$$

$$\mathbf{H}_{k_{AC},los} = \rho_{C}\hat{\mathbf{H}}_{k_{C},los} + \boldsymbol{\epsilon}_k. \tag{47}$$

The receivers' 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 for the eavesdropper estimating the closest user as:

$$\mathbf{D}_{k_{AB},los} = \frac{\mathbf{H}_{k_{EB1,los}} + \mathbf{H}_{k_{EB2,los}}}{2}, \tag{48}$$

where:

$$\mathbf{H}_{k_{EB1,los}} = \rho_{EB1}\hat{\mathbf{H}}_{k_{EB1,los}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{49}$$

and:

$$\mathbf{H}_{k_{EB2,los}} = \rho_{EB2}\hat{\mathbf{H}}_{k_{EB2,los}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k. \tag{50}$$

Likewise, the component for the eavesdropper estimating the farthest user is defined as:

$$\mathbf{D}_{k_{AC},los} = \frac{\mathbf{H}_{k_{EC1,los}} + \mathbf{H}_{k_{EC2,los}}}{2}, \tag{51}$$

where:

$$\mathbf{H}_{k_{EC1,los}} = \rho_{EC1}\hat{\mathbf{H}}_{k_{EC1,los}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k \tag{52}$$

and:

$$\mathbf{H}_{k_{EC2,los}} = \rho_{EC2}\hat{\mathbf{H}}_{k_{EC2,los}} + \boldsymbol{\xi}_k + \boldsymbol{\epsilon}_k. \tag{53}$$

In this scenario, the channel estimates $\hat{\mathbf{H}}_{k_{EB1,los}}$ and $\hat{\mathbf{H}}_{k_{EB2,los}}$, likewise with the channel estimates $\hat{\mathbf{H}}_{k_{EC1,los}}$ and $\hat{\mathbf{H}}_{k_{EC2,los}}$, only concern the LOS component between A and E and B and E or between A and E, and A and C, respectively. The difference between these estimates and the real channels will be proportional to the power of the multipath component. We define the ray power coefficient for both scenarios as:

$$\alpha_{RP} = \frac{P_R}{P_D + P_R}, \tag{54}$$

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.

2.7. Decision Feedback

The definitions in this section, unless otherwise stated, apply to all receivers. As is known, employing soft decisions in the feedback equalization greatly reduces the level of ISI. These soft decisions can be calculated through the log likelihood ratios (LLR) of the equalized signal, obtained by:

$$L_n^{(\mathrm{I},i)} = \frac{2}{\sigma_i^2}\mathrm{Re}\left(\tilde{s}_n^{(i)}\right), \tag{55}$$

and:

$$L_n^{(\mathrm{Q},i)} = \frac{2}{\sigma_i^2}\mathrm{Im}\left(\tilde{s}_n^{(i)}\right), \tag{56}$$

where:

$$\sigma_i^2 = \frac{1}{2}\mathbb{E}\left[\left|s_n - \tilde{s}_n^{(i)}\right|^2\right] \approx \frac{1}{2N}\sum_{n=0}^{N-1}\left|\hat{s}_n - \tilde{s}_n^{(i)}\right|^2. \tag{57}$$

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

$$\bar{s}_n^{(i)} = \tanh\left(\frac{L_n^{(\mathrm{I},i)}}{2}\right) + j\tanh\left(\frac{L_n^{(\mathrm{Q},i)}}{2}\right). \tag{58}$$

The estimated data symbols are obtained through the hard decision of the equalized symbols. For Receiver C, there is an additional step, which consists of, once again, interleaving the soft decided symbols and multiplying by the Hermitian of the partial key matrix, written as:

$$\bar{\mathbf{Y}}'^{(l)}_{k_C} = \mathbf{Q}_k^H \bar{\mathbf{S}}'^{(l)}_{k_C}. \tag{59}$$

The resulting matrix is then deinterleaved and applied in (36).

3. Secrecy Rate

To measure the security potential of this system, we utilize a figure of merit referred to as the secrecy rate [27]. The secrecy rate is expressed as the difference between the capacity of the proper channel, from A to B or A to C, and the eavesdropper channel, from A to E. For simplicity's sake, we use $\mathbf{X}_k$ and $\mathbf{Z}_k$ as placeholders for the signals in either receiver. The total capacity of the system is defined as the sum of the capacity of each sub-carrier, i.e.,

$$C = \sum_{k=1}^{N} C_k, \tag{60}$$

where C_k denotes the capacity of a single sub-carrier, defined according to [28]:

$$C_k = I(\mathbf{X}_k, \mathbf{Z}_k), \tag{61}$$

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

$$I(\mathbf{X}_k, \mathbf{Z}_k) = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_c|^2 \text{SNR}\right), \tag{62}$$

where λ_c is the c^{th} singular value of the corresponding channel.

Let us divide the analysis into two parts, the first being the proper transmitter/receiver pair, while the second is the transmitter/eavesdropper pair. For the scenario with A and B, we define the capacity as:

$$C_k^{AB} = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_c \rho_B|^2 \frac{\sigma_X^2}{\sigma_N^2 + \sigma_B^2}\right), \tag{63}$$

where σ_X and σ_N are the variances of $\mathbf{X}_k$ and $\mathbf{N}_k$, respectively, and σ_B^2 is the power of the interference associated with the imperfect channel estimation, given by:

$$2\sigma_B^2 = \mathbb{E}\left[\hat{\mathbf{\Lambda}}_{k_B}^I \hat{\mathbf{\Lambda}}_{k_B}^{IH}\right], \tag{64}$$

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

$$\hat{\mathbf{\Lambda}}_{k_B}^I = \hat{\mathbf{\Lambda}}_{k_B} - \text{diag}\left(\hat{\mathbf{\Lambda}}_{k_B}\right). \tag{65}$$

Likewise, the capacity of the system with the link from A to C is given by:

$$C_k^{AC} = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_c \rho_C|^2 \frac{\sigma_X^2}{\sigma_N^2 + \sigma_C^2}\right), \tag{66}$$

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

$$2\sigma_C^2 = \mathbb{E}\left[\hat{\mathbf{\Lambda}}_{k_C}^I \hat{\mathbf{\Lambda}}_{k_C}^{IH}\right], \tag{67}$$

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

$$\hat{\mathbf{\Lambda}}_{k_C}^I = \hat{\mathbf{\Lambda}}_{k_C} - \text{diag}\left(\hat{\mathbf{\Lambda}}_{k_C}\right). \tag{68}$$

Similarly, we can define the capacity of the eavesdropper as:

$$C_k^{AE} = \sum_{c=1}^{C} \log_2 \left(1 + |\lambda_{c_E} \rho_E|^2 \frac{\sigma_X^2}{\sigma_N^2 + \sigma_E^2}\right), \tag{69}$$

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:

$$2\sigma_E^2 = \mathbb{E}\left[\hat{\mathbf{\Lambda}}_{k_E}^I \hat{\mathbf{\Lambda}}_{k_E}^{IH}\right]. \tag{70}$$

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

$$\hat{\mathbf{\Lambda}}_{k_E}^I = \hat{\mathbf{\Lambda}}_{k_E} - \text{diag}\left(\hat{\mathbf{\Lambda}}_{k_E}\right). \tag{71}$$

With (63) and (69), we are able to obtain the total capacity by using (60). 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., for the link between and A and B, we have:

$$SR_B = C^{AB} - C^{AE}, \tag{72}$$

while for the link between A and C, we have:

$$SR_C = C^{AC} - C^{AE}. \tag{73}$$

4. Results and Discussion

This system was simulated under a variety of conditions utilizing Monte Carlo simulations. The frequency selective channel was characterized by 16 multipath rays with uncorrelated Rayleigh fading. Our analysis focused on the achievable secrecy rate for various levels and sources of channel errors and different system considerations, as well as on the BER at the users B and C. Unless otherwise mentioned, $\alpha = 18$ dB. Let us start with Figure 3, which shows the BER of the proposed system considering an 8×8 system with perfect CSI.

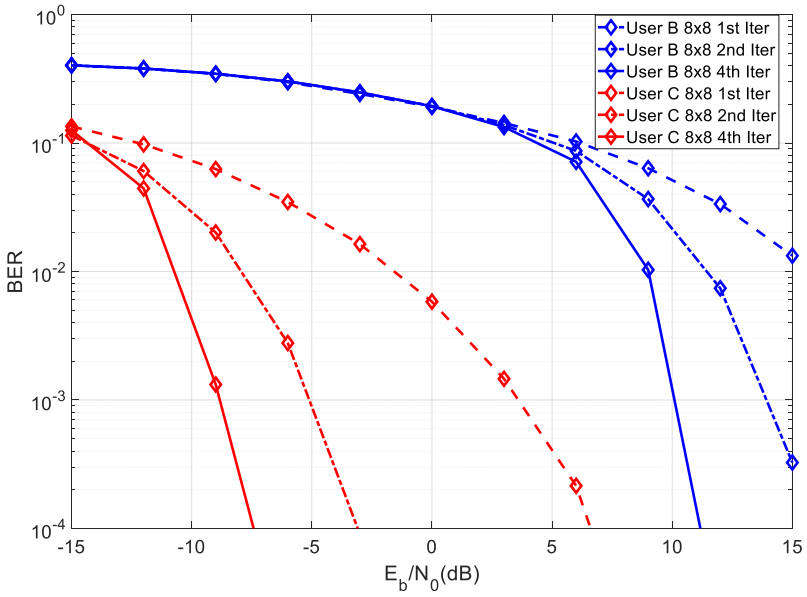

Figure 3. BER of both legitimate users for an 8×8 system.

From the figure, it can be seen that User C required an SNR of about 18 dB lower than User B, in order to achieve the same BER in the first iteration, which corresponded to the gain due to the higher transmit power. As mentioned before, the partial key $\mathbf{Q}_k$ must be quantized using a finite resolution, before being transmitted. Figure 4 shows the achievable BER results for a 2×2 system at User C for different quantization resolutions.

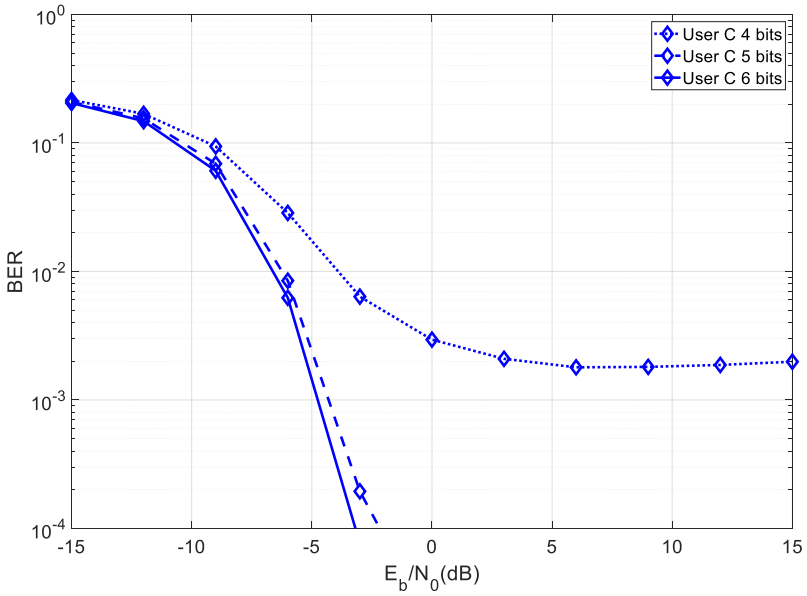

Figure 4. BER of a 2 × 2 system at User C, considering four IB-DFE iterations and different resolutions for quantization of the partial key $\mathbf{Q}_k$.

From the figure, it can be seen that this system required at least five bits of quantization to reach a target BER of 10^{-4}. Since the matrix $\mathbf{Q}_k$ could be reconstructed based on four parameters, then the total overhead associated with the transmission of the partial key had a length of 20 bits.

4.1. Secrecy Rate Results

Figure 5 shows a comparison of the secrecy rate for both channels considering both a SISO and MIMO configuration.

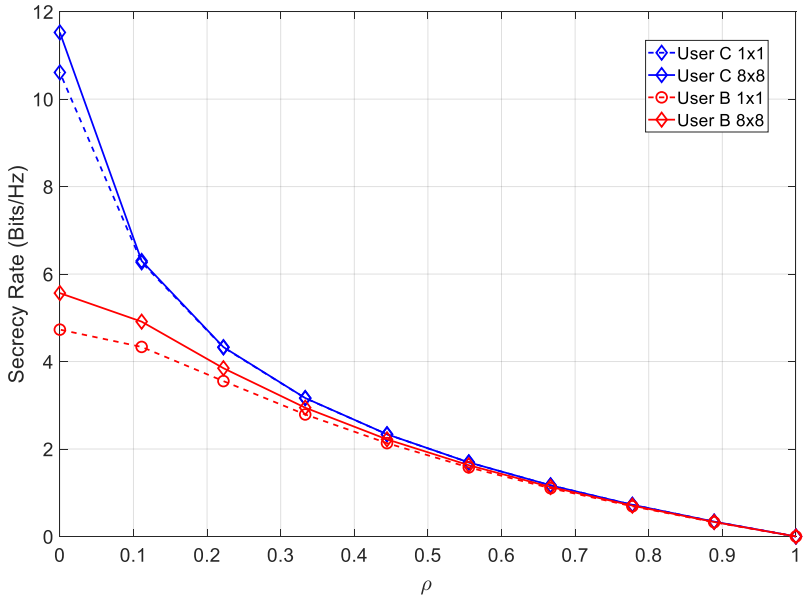

Figure 5. Secrecy rate for SISO and MIMO configurations considering perfect channel estimation. In this graph, ρ refers to either ρ_{EB} or ρ_{EC}, according to the user in question.

From the figure, it could be concluded that employing MIMO led to a higher achievable secrecy rate at lower values of ρ_{EB} and ρ_{EC}.

4.1.1. User B Results

Let us analyze the secrecy rate of the nearest user, beginning with Figure 6, which depicts the secrecy rate of User B under various channel estimation errors.

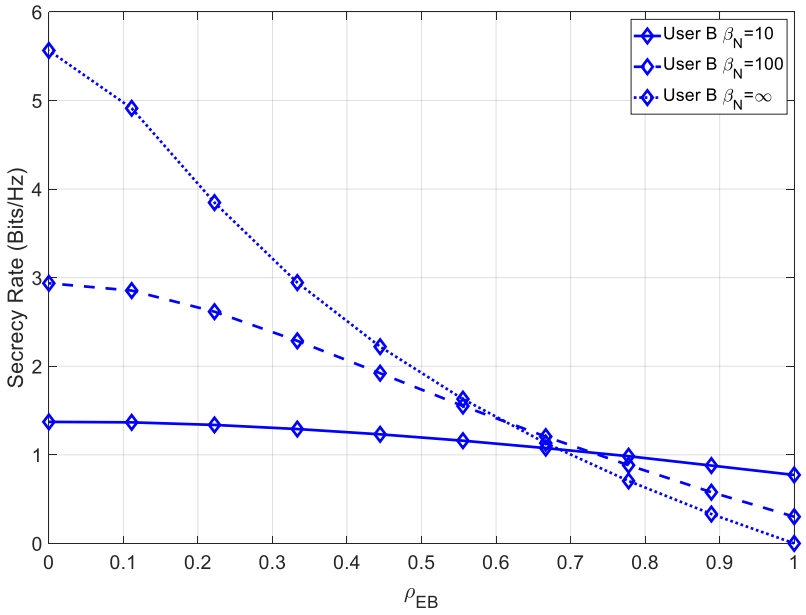

Figure 6. Secrecy rate of the 8×8 receiver B with different channel estimation errors.

It can be seen that minimizing the channel estimation error in the receiver was crucial to ensuring a high secrecy rate. For low values of ρ_{EB}, this receiver achieved significant levels of the secrecy rate. In Figure 7, we introduce a channel mismatch error.

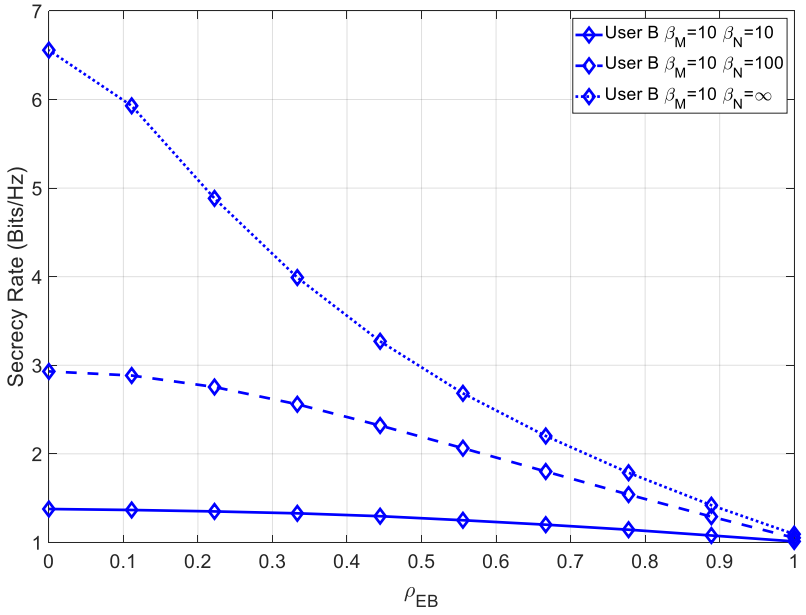

Figure 7. Secrecy rate of the 8×8 receiver B with different channel estimation errors and a permanent channel mismatch error.

It was observed that maximum achievable secrecy rate, for low values of ρ_{EB}, increased as the channel estimation error decreased. It should be noted that in this scenario, since the channel mismatch

error did not affect the intended receiver, the secrecy rate for high values of ρ_{EB} was also higher and could not be compensated by decreasing the channel estimation error.

4.1.2. Line-of-Sight at User B

In this scenario, there was an LOS with all users; therefore, we analyzed the impact of the power ratio α_{RP} on the attainable secrecy rate. In Figure 8, the secrecy rate for various values of α_{RP} is shown for User B.

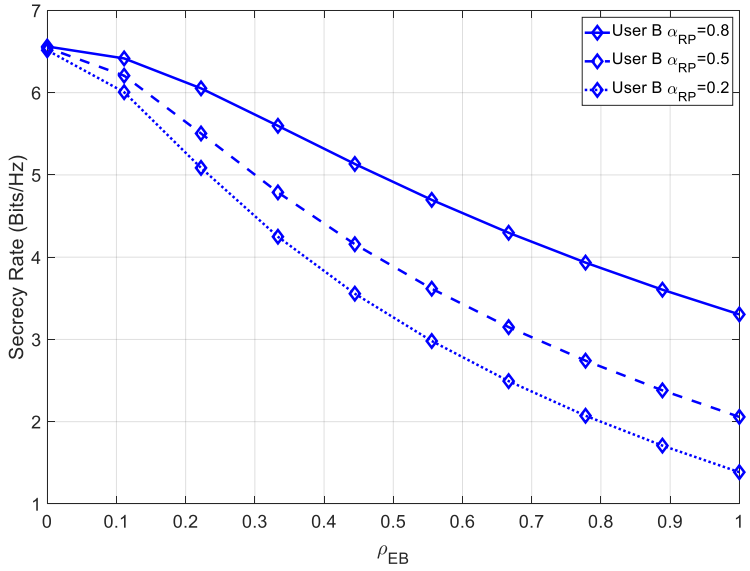

Figure 8. Secrecy rate of the 8×8 LOS receiver B with perfect channel estimation and varying ray power coefficient.

As expected, since the eavesdropper could not estimate the multipath component, the greater the value of α_{RP}, the more secure the system could be. Figure 9 shows the secrecy rate in a scenario where there was imperfect channel estimation.

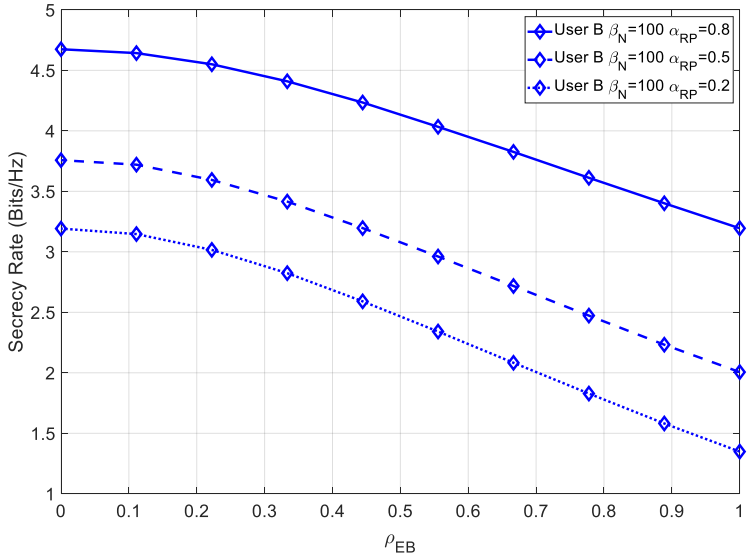

Figure 9. Secrecy rate of the 8×8 receiver B with channel estimation errors on both the receiver and eavesdropper, for various ray power coefficients.

It could be observed that the channel estimation severely degraded our secrecy rate; however, even for high values of ρ_{EB} and ρ_{EC}, the secrecy rate remained high, when compared with the non-LOS scenario, due to the multipath component. Figure 10 shows the impact of a channel mismatch error on the secrecy rate.

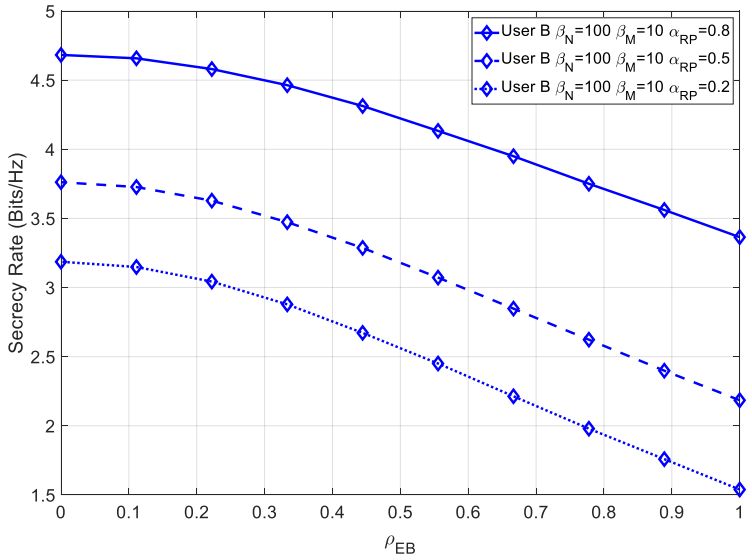

Figure 10. Secrecy rate of the 8×8 receiver B with channel estimation errors on both the receiver and eavesdropper, as well as a permanent channel mismatch error, for various ray power coefficients.

It could be concluded that the permanent channel mismatch error increased the secrecy rate for high values of ρ_{EB}, albeit the increase was relatively small, when compared with the non-LOS scenario. Since the lack of a multipath estimation produced a much more significant effect on the secrecy rate, then a further channel mismatch error had a smaller impact on the secrecy rate.

4.1.3. User C Results

Let us analyze the secrecy rate at the farthest user. In Figure 11, we compare the secrecy rate of User C under different levels of channel estimation error.

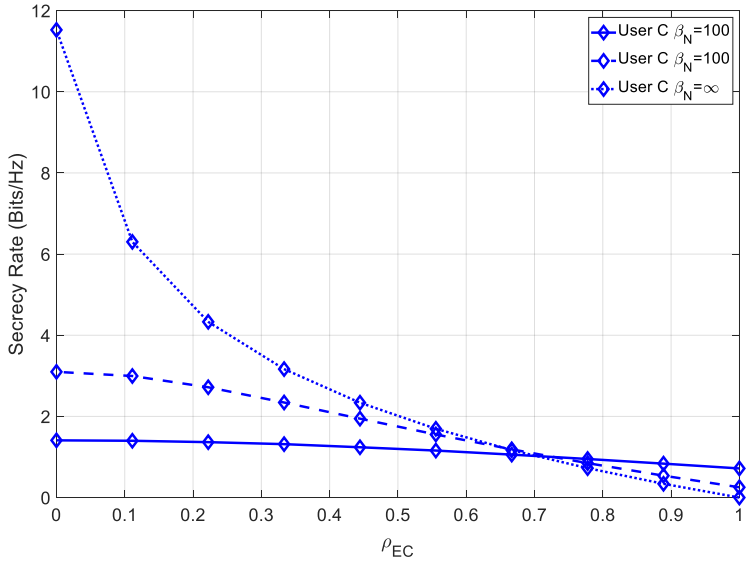

Figure 11. Secrecy rate of the 8×8 receiver C with different channel estimation errors.

In this case, the maximum achievable secrecy rate was higher than the one of User B, due to the increased capacity of the channel with a higher transmit power. The effect of minimizing the channel estimation error of the receiver was significantly more noticeable in this scenario, at low values of ρ_{EC}. In Figure 12, the secrecy rate of User C is simulated under imperfect channel estimation, as well as a channel mismatch error at the eavesdropper.

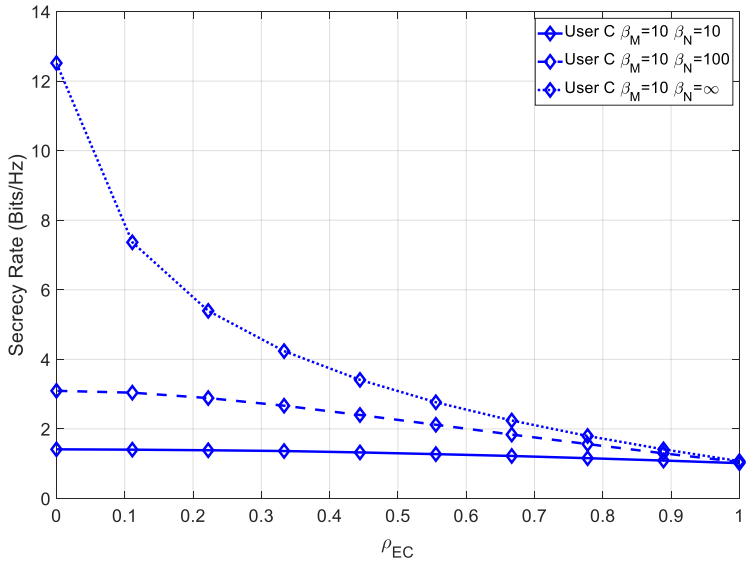

Figure 12. Secrecy rate of the 8×8 receiver C with different channel estimation errors and a permanent channel mismatch error.

It could be seen that, similarly to User B, this system achieved a higher maximum secrecy rate, at low values of ρ_{EC}, and a higher secrecy rate, even for high values ρ_{EC}.

4.1.4. Line-of-Sight at User C

In the LOS scenario, we analyzed the impact of the power ratio α_{RP} on the attainable secrecy rate for user C. In Figure 13, the secrecy rate for various values of α_{RP} is shown.

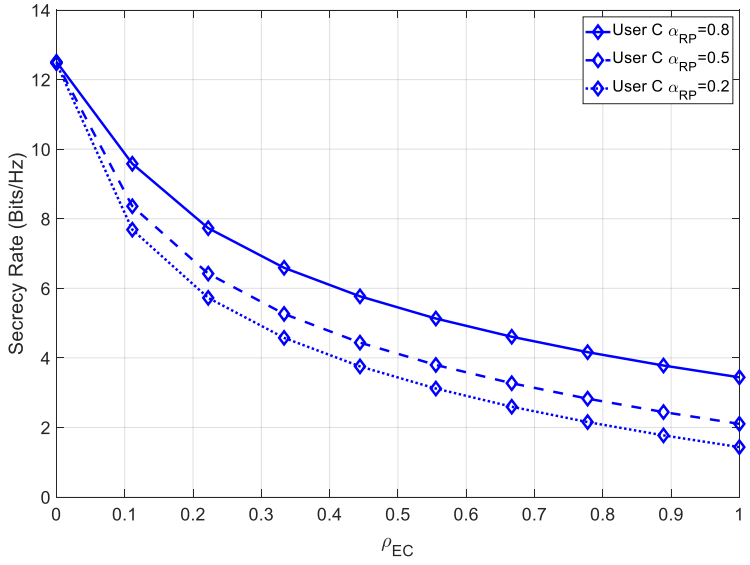

Figure 13. Secrecy rate of the 8×8 LOS receiver C with perfect channel estimation and varying ray power coefficient.

Similarly, for a higher contribution of the multipath component, the achievable secrecy increased. Since in this case, there was perfect channel estimation, then User C achieved a much higher maximum secrecy rate than User B, due to its higher channel capacity. Figure 14 shows the secrecy rate for various values of α_{RP}, in the presence of channel estimation errors.

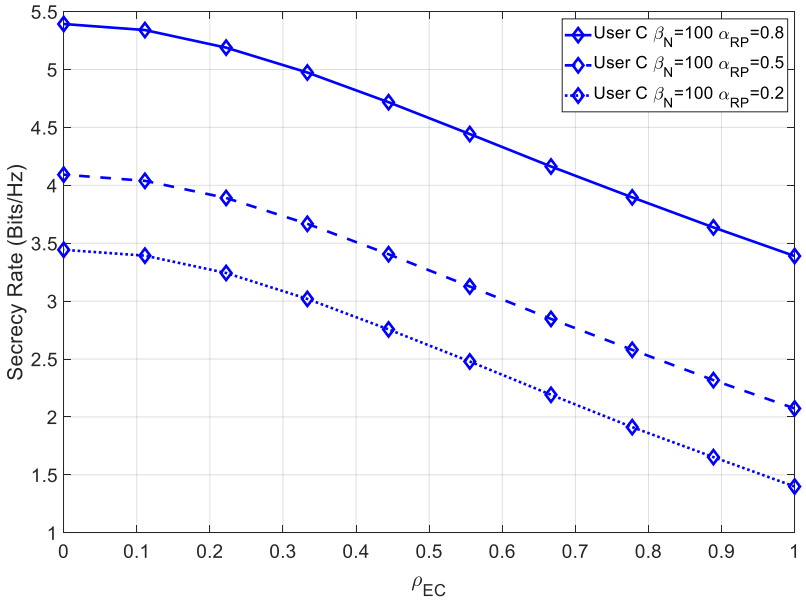

Figure 14. Secrecy rate of the 8 × 8 receiver C with channel estimation errors on both the receiver and eavesdropper, for various ray power coefficients.

In this case, the channel estimation error lowered the overall secrecy rate; however, the degradation was less severe for higher power multipath components. Moreover, it should be noted that User C's secrecy rate was degraded much more than User B's, as User C required very precise channel estimation. Figure 15 shows the secrecy rate for various values of α_{RP} and various sources of channel estimation errors.

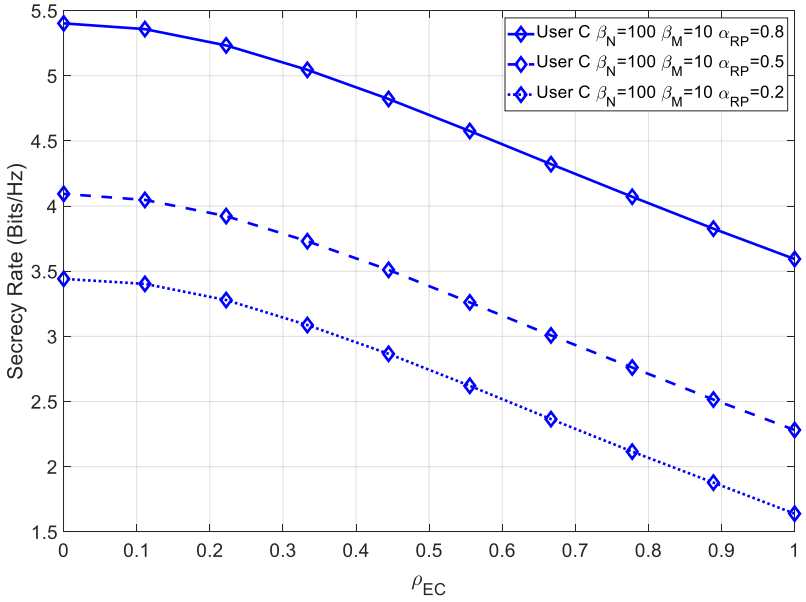

Figure 15. Secrecy rate of the 8 × 8 receiver C with channel estimation errors on both the receiver and eavesdropper, as well as a permanent channel mismatch error, for various ray power coefficients.

As is the case for User B, the increase in the secrecy rate at high ρ_{EC} was relatively small, compared to the NLOS scenario, as the LOS component contributed less in this scenario.

5. Conclusions

In this paper, we proposed a physical layer security level against eavesdroppers for a three user power domain MIMO-NOMA scheme based on SVD. The security potential of this scheme was studied, and it was shown that minimizing channel estimation errors and maximizing channel estimate correlations could lead to very high secrecy rates. Even in LOS scenarios, it was shown that the secrecy rate could be kept high if the multipath component's power was relatively high. Therefore, power domain MIMO-NOMA schemes based on SVD are an attractive option for highly secure NOMA 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 and editing, J.G. and H.S.

Funding: This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020, by Instituto de Telecomunicações under project PES3N POCI-01-0145-FEDER-030629 and by SECREDAS, which received funding from the Electronic Component Systems for European Leadership Joint Undertaking (ESCEL-JU) under Grant Agreement No. 783119.

Conflicts of Interest: The authors declare no conflict of interest.

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.
2. 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.
3. *3GPPP: Technical Specification Group Radio Access Network; Physical Layers Aspects for Evolved UTRA*; 3GPPP TR 25.814; 3GPPP:Valbonne, Frace, 2006.
4. 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.
5. Dai, L.; Wang, B.; Ding, Z.; Wang, Z.; Chen, S.; Hanzo, L. A Survey of Non-Orthogonal Multiple Access for 5G. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2294–2323.
6. Do, D.-T.; Le C.-B. Application of NOMA in Wireless System with Wireless Power Transfer Scheme: Outage and Ergodic Capacity Performance Analysis. *Sensors* **2018**, *18*, 3501.
7. Wang, B.; Dai, L.; Wang, Z.; Ge, N.; Zhou, S. Spectrum and Energy-Efficient Beamspace MIMO-NOMA for Millimeter-Wave Communications Using Lens Antenna Array. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2370–2382.
8. Islam, S.; Avazov, N.; Dobre, O.; Kwak, K. Power domain non-orthogonalmultiple access (NOMA) in 5G systems: Potentials and challenges. *IEEE Commun. Surv. Tuts.* **2017**, *19*, 721–742.
9. Liu, Y.; Xing, H.; Pan, C.; Nallanathan, A.; Elkashlan, M.; Hanzo, L. Multiple-Antenna-Assisted Non-Orthogonal Multiple Access. *IEEE Wirel. Commun.* **2018**, *25*, 17–23.
10. Zeng, M.; Yadav, A.; Dobre, O.A.; Tsiropoulos, G.I.; Poor, H.V. On the Sum Rate of MIMO-NOMA and MIMO-OMA Systems. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 534–537.
11. Liu, Y.; Qin, Z.; Elkashlan, M.; Gao, Y.; Hanzo, L. Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1656–1672.
12. He, B.; Liu, A.; Yang, N.; Lau, V.K.N. On the Design of Secure Non-Orthogonal Multiple Access Systems. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2196–2206.
13. Li, S.; Qinghe, D. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy*, vol. 20, pp. 730, Sep. 2018.
14. Do, D.-T.; Van Nguyen, M.-S.; Hoang, T.-A.; Voznak, M. NOMA-Assisted Multiple Access Scheme for IoT Deployment: Relay Selection Model and Secrecy Performance Improvement. *Sensors* **2019**, *19*, 736.

15. Vaezi, M.; Schober, R.; Ding, Z.; Poor, H.V. Non-Orthogonal Multiple Access: Common Myths and Critical Questions. *IEEE Wirel. Commun.* **2019**, *26*, 174–180.
16. Zhang, M.; Liu, Y.; Zhang, R. Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3085–3096.
17. Madeira, J.; Guerreiro, J.; Dinis, R.; Montezuma, P.; Campos, L.M, On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes. *Sensors* **2019**, *19*, 4757.
18. Saini, R.; Jindal, A.; De, S. Jammer-Assisted Resource Allocation in Secure OFDMA with Untrusted Users. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1055–1070.
19. Gabalou, V.F.; Maham, B. Jamming game for secure OFDMA systems. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
20. Zeng, M.; Nguyen, N.; Dobre, O.A.; Poor, H.V. Securing Downlink Massive MIMO-NOMA Networks with Artificial Noise. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 685–699.
21. 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.
22. Lebrun, G.; Gao, J.; Faulkner, M. MIMO transmission over a time-varying channel using SVD. *IEEE Trans. Wirel. Commun.* **2005**, *4*, 757–764.
23. Madeira, J.; Guerreiro, J.; Dinis, R. Iterative frequency domain detection and compensation of nonlinear distortion effects for MIMO systems. *Phys. Commun.* **2019**, *37*, 100869 .
24. 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.
25. 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.
26. Zhu, Y.; Wang, L.; Wong, K.; Heath, R.W. Physical Layer Security in Large-Scale Millimeter Wave Ad Hoc Networks. *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Dec. 2016.
27. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *Safeguarding 5G Wirel. Commun. Networks Using Phys. Layer Secur.* **2015**, *53*, 20–27.
28. Telatar, I. Capacity of multi-antenna Gaussian channels. *Eur. Trans. Telecommun.* **1999**, *10*, 585–595.