

Article

Secure Information Transmission with Self Jamming SWIPT

Akashkumar Rajaram ^{1,2,3,*}, Rui Dinis ^{1,3} , Dushnatha Nalin K. Jayakody ^{2,4}  and Marko Beko ^{3,5} 

¹ Faculty of Science and Technology, New University of Lisbon, 2829-516 Caparica, Portugal; rdinis@fct.unl.pt

² School of Computer Science and Robotics, National Research Tomsk Polytechnic University, 634050 Tomsk, Russia; nalin@tpu.ru

³ COPELABS, Universidade Lusófona de Humanidades e Tecnologias, 1749-024 Lisboa, Portugal; beko.marko@ulusofona.pt

⁴ School of Engineering, Sri Lanka Technological Campus, 10500 Padukka City, Sri Lanka;

⁵ UNINOVA, Monte da Caparica, 2829-516 Caparica, Portugal

* Correspondence: a.rajaram@campus.fct.unl.pt

Received: 27 February 2020; Accepted: 25 March 2020; Published: 30 March 2020



Abstract: This article is focused on implementing simultaneous wireless information and power transmission as a physical layer security measure by using artificial noise. A series of high energy precoded symbols is simultaneously transmitted along with the information symbols over a Rayleigh frequency selective fading channel. The high energy precoded symbols act as an artificial noise for the eavesdroppers. The energy symbols are precoded on the basis of a legitimate user's channel matrix to form a null space vector, which eliminates the interference of energy symbols at the information symbol receiver antennas, while allowing the rectenna to harvest energy from the superimposed information and energy symbols. We analyze the secrecy rate and error rate performance at the receiver under different circumstances, and we show that the performance of the legitimate user can be improved by using the iterative block decision feedback equalization method at the receiver.

Keywords: simultaneous wireless information and power transmission (SWIPT); physical layer security; wiretap channel model; iterative block decision feedback equalization (IB-DFE)

1. Introduction

In a dense wireless communication network (WCN), both the energy and security reliability need to be assured. This represents a challenge in the case of a network with a huge number of nodes [1]. Thus, in order to keep up with the energy demands of the increasing number of network nodes, new radio frequency energy harvesting (EH) techniques like simultaneous wireless information and power transmission (SWIPT) are investigated for 5G networks [1–3]. Apart from harvesting energy by using SWIPT techniques, many other signal processing applications like channel estimation with SWIPT [4] and physical layer security (PLS) measures with the help of SWIPT technique were investigated in [5]. One of the most important techniques in improving PLS in a wiretap channel is using artificial noise (AN) in the communication channel to degrade the signal-to-noise plus interference ratio (SINR) of eavesdroppers; thereby improving the security of legitimate users [6]. The high energy signal that is used for harvesting energy in SWIPT can also be adopted for creating AN to improve PLS, as in [7]. The secrecy rate of legitimate users in a wiretap channel can be improved with the SINR degradation of eavesdroppers as in [8,9]. Furthermore, the secrecy rate for the multiple-input and multiple-output (MIMO) system model was established in [10]. To avoid the impact of AN on the legitimate receiver, AN is introduced in the null space of the legitimate receiver's channel matrix. Thereby, AN degrades

the SINR of eavesdroppers without compromising the quality of the legitimate users' signal [11]. However, the successful negation of AN is dependent on the channel state information (CSI) of the receiver at the legitimate transmitter and can be effectively used against very robust eavesdroppers as in [12,13]. This is considered as a challenge in the imperfect CSI condition [14,15]. Another challenge in using AN against eavesdroppers lies in the fact that a jamming attack depends on the channel correlation between the eavesdroppers and legitimate receiver; if the channel correlation is very high, then AN can be partially canceled out by the eavesdropper [16,17].

In this article, we use energy signals as a source of AN for secure communication, but also to harvest energy at the receiver. We consider the conventional MIMO system model with separate antennas for data and energy signal transmission and reception. AN is created by the transmitter by using channel precoding based on the CSI of the receiver. In this paper, we analyze the impact on channel precoding based on imperfect CSI. Furthermore, we also consider high channel correlation between eavesdroppers and the legitimate receiver as one of the challenges in the analysis. Our main contribution in this paper involves improving the error rate and secrecy rate performance of the legitimate receiver using iterative block decision feedback equalization (IB-DFE). IB-DFE is an efficient low complex receiver and performs better than non-iterative methods [18]. IB-DFE is effectively used with the single carrier frequency-division multiple access (SC-FDMA) transmission technique, and its performance was studied in detail [19–21]. IB-DFE can also be used to improve channel estimation at the transmitter side against imperfect CSI by using the robust superimposed pilot signal method for accurate channel estimation, as in [4,22]. For a fair comparison between the legitimate user and eavesdroppers, we also analyze the impact of imperfect CSI on the legitimate user's performance.

Throughout this article, matrices or vectors are denoted by bold letters, and scalar variables are denoted by italic letters. The variables associated with the frequency domain and time domain are denoted by capital letters and small letters, respectively. $(\cdot)^*$, $(\cdot)^T$, $(\cdot)^H$, $\|\cdot\|$, and $\mathbb{E}[\cdot]$ denote the conjugate, transpose, Hermitian, trace, and expectation operation, respectively.

2. System Model

The MIMO system model is shown in Figure 1. It is composed of three transmitting antennas and two receiving antennas, with a dedicated transmitting antenna and a receiving antenna for information transmission, denoted as \mathcal{T} and R , respectively. The other two transmitting antennas, $E1$ and $E2$, are used for energy transmission, and the rectenna \wp is used to harvest energy from the physical layer network coded (PLNC) signal. The eavesdropper is denoted as ζ . It is assumed that $E1$, $E2$, and \mathcal{T} are not spatially correlated. In Figure 1, based on the location of ζ , if ζ is very close to R , ζ is considered to have high channel correlation with R [16]. The system adopts the quadrature amplitude modulation (QAM) signal over the Rayleigh frequency selective fading channel by using SC-FDMA for simultaneously transferring information from \mathcal{T} and the high energy signal from $E1$ and $E2$ to both R and \wp . The frequency domain signals transmitted from \mathcal{T} , $E1$, and $E2$ are denoted as $X_I^{(k)}$, $X_{E1}^{(k)}$, and $X_{E2}^{(k)}$, respectively, where k represents the index of the symbol with $k = 0, 1, \dots, K$ and K is the total number of symbols in the respective signal stream. The frame structure of \mathbf{X}_I , \mathbf{X}_{E1} , and \mathbf{X}_{E2} is illustrated in Figure 2, where the time duration per symbol, block duration, and total time for all the blocks are denoted as T , T_l , and $T_l L$, respectively. A frame consists of L signal blocks where each signal block contains N symbols. The signal blocks are denoted as l , where $l = 0, 1, \dots, L$. We assume that $X_I^{(k)}$, $X_{E1}^{(k)}$, and $X_{E2}^{(k)}$ are transmitted with perfect time synchronization and in equal block size. The following system of equations is considered for a single block, and therefore, we set $l = 1$.

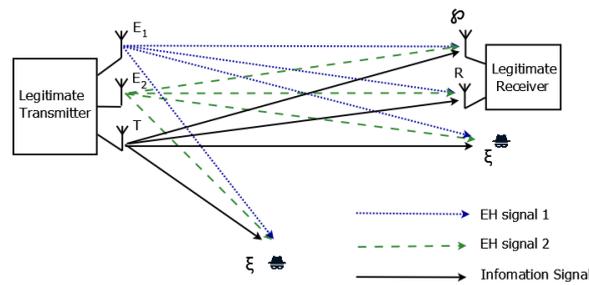
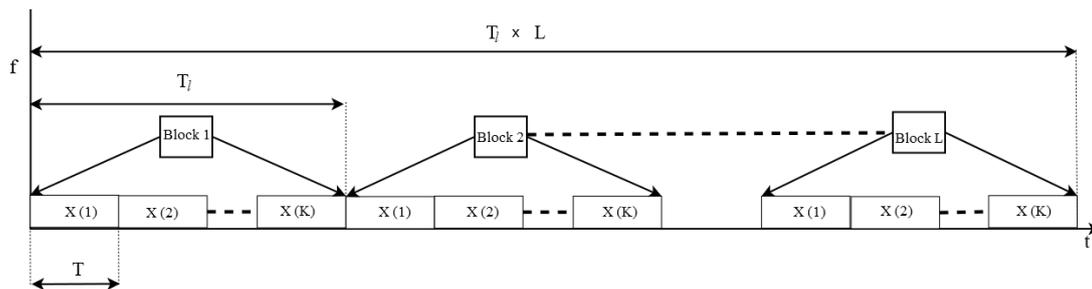


Figure 1. System model. EH, energy harvesting.



X - Data symbol, L - number of blocks

Figure 2. Frame structure of the proposed system, where T and T_l are the time duration of a symbol and a block, respectively.

S_{E1} , S_{E2} , and S_I are the unamplified versions of X_{E1} , X_{E2} , and X_I , respectively, and the power amplification levels of energy symbols and information symbols are at different levels. P_{E1} , P_{E2} , and P_I denote the transmit powers of X_{E1} , X_{E2} , and X_I , respectively. For the sake of simplicity, without loss of generality, we assume that $P_{E1} = P_{E2}$. The relationship between the power levels of energy and information symbols is given as:

$$\begin{aligned} X_I^{(k)} &= S_I^{(k)} P_I; \quad X_{E1}^{(k)} = S_{E1}^{(k)} P_{E1}; \quad X_{E2}^{(k)} = S_{E2}^{(k)} P_{E2}; \\ \beta &= \frac{2P_{E1}}{P_I}, \end{aligned} \tag{1}$$

where β is the ratio between the transmit power of the energy and information signal.

Throughout this paper, the channel coefficient for the channel link between two nodes, i.e., for example, nodes \mathcal{T} and R , is denoted as $H_{TR}^{(k)}$, where k represents the index of channel coefficient with respect to the transmitted symbol in the signal stream. Then, $H_{TR}^{(k)}$ is characterized as $H_{TR}^{(k)} \sim \mathcal{CN}(0, \sigma_{H,TR}^2)$, and its channel gain is given as $|H_{TR}^{(k)}|^2 \sim \text{Exp}\{\sigma_{H,TR}^2\}$, where $\sigma_{H,TR}^2$ is the variance of $H_{TR}^{(k)}$. Since all the channel links between the nodes are Rayleigh frequency selective fading channels, they follow similar notation and channel characterization as $H_{TR}^{(k)}$. Similarly, the channel coefficients corresponding to the channel link between $E1$ and R , $E2$ and R , \mathcal{T} and φ , $E1$ and φ , $E2$ and φ , \mathcal{T} and ζ , $E1$ and ζ , and $E2$ and ζ are denoted as $H_{E1R}^{(k)}$, $H_{E2R}^{(k)}$, $H_{T\varphi}^{(k)}$, $H_{E1\varphi}^{(k)}$, $H_{E2\varphi}^{(k)}$, $H_{T\zeta}^{(k)}$, $H_{E1\zeta}^{(k)}$, and $H_{E2\zeta}^{(k)}$, respectively. The received signals at R , φ , and ζ experience additive white Gaussian noise (AWGN) modeled as a zero mean complex Gaussian random variable, and their respective AWGNs are given as $N^{(k)} \sim \mathcal{CN}(0, \sigma_N^2)$, $W^{(k)} \sim \mathcal{CN}(0, \sigma_W^2)$, and $J^{(k)} \sim \mathcal{CN}(0, \sigma_J^2)$, respectively.

The system model exploits the CSI of $H_{E2R}^{(k)}$ and $H_{E1R}^{(k)}$ to cancel the interference of the energy signals to the information signal at R . $X_{E1}^{(k)}$ and $X_{E2}^{(k)}$ will be precoded to equalize $H_{E2R}^{(k)}$ and $H_{E1R}^{(k)}$, respectively. Unlike R , the eavesdropper ζ receives a highly distorted signal, which makes the decoding process difficult. In general, ζ can decode the information based on the estimated value of $X_{E1}^{(k)}$, $X_{E2}^{(k)}$,

$H_{E2R}^{(k)}$ and $H_{E1R}^{(k)}$. Furthermore, to reduce the accuracy of these estimated values at ζ , the EH signal should act as AN. Similar to ζ , \wp will receive the combination of all the transmitted signals as a PLNC signal. Furthermore, \wp can effectively take advantage of the PLNC signal for harvesting energy, and the received PLNC signal at \wp is given as:

$$Y_{\wp}^{(k)} = H_{E1\wp}^{(k)} X_{E1}^{(k)} + H_{E2\wp}^{(k)} X_{E2}^{(k)} + H_{T\wp}^{(k)} X_I^{(k)} + W^{(k)}. \tag{2}$$

The performance of this secure self jamming SWIPT technique is analyzed based on the secrecy rate and the bit error rate (BER). Here, three different scenarios are considered, and in all the scenarios, R and ζ are considered to have a CSI of \mathbf{H}_{TR} and $\mathbf{H}_{T\zeta}$, respectively. Here, both R and ζ do not have a CSI of \mathbf{H}_{E1R} and \mathbf{H}_{E2R} . The assumptions behind the three scenarios are explained as follows:

- A Scenario A: \mathcal{T} has the CSI of \mathbf{H}_{E1R} and \mathbf{H}_{E2R} . ζ is assumed to be far away from R , and ζ does not have channel correlation. In this scenario, ζ is denoted as $\zeta(a)$, and R is denoted as $R(a)$.
- B Scenario B: \mathcal{T} does not have the CSI of \mathbf{H}_{E1R} and \mathbf{H}_{E2R} , and \mathcal{T} estimates \mathbf{H}_{E1R} and \mathbf{H}_{E2R} . ζ is assumed to be very close to R , and their channel correlation is very high. In this scenario, ζ is denoted as $\zeta(b)$, and R is denoted as $R(b)$.
- C Scenario C: This scenario is similar to A where \mathcal{T} has the CSI of \mathbf{H}_{E1R} and \mathbf{H}_{E2R} , but here, ζ is assumed to be very close to R , and their channel correlation is very high. In this scenario, ζ is denoted as $\zeta(c)$. Based on the perfect CSI condition, R is the same in Scenario A and Scenario C.

Then, the received signal at $R(a)$ is given as:

$$Y_{R(a)}^{(k)} = \begin{cases} H_{TR}^{(k)} X_I^{(k)} + N^{(k)}; & \text{if } \mathcal{L}(\mathcal{V}^{(k)}) = 0, \\ H_{TR}^{(k)} X_I^{(k)} + N^{(k)} + H_{E1R}^{(k)} X_{E1}^{(k)} + H_{E2R}^{(k)} X_{E2}^{(k)}; & \text{otherwise,} \end{cases} \tag{3}$$

where $\mathcal{L}(\cdot)$ denotes the linear subspace of a vector and $\mathcal{V}^{(k)} = H_{E1R}^{(k)} X_{E1}^{(k)} + H_{E2R}^{(k)} X_{E2}^{(k)}$. Here, $H_{E1R}^{(k)} X_{E1}^{(k)}$ is the additive inverse of $H_{E2R}^{(k)} X_{E2}^{(k)}$, and this allows \mathcal{T} to nullify the interference of $X_{E1}^{(k)}$ and $X_{E2}^{(k)}$. To achieve $\mathcal{L}(H_{E1R}^{(k)} X_{E1}^{(k)} + H_{E2R}^{(k)} X_{E2}^{(k)}) = 0$, both $X_{E1}^{(k)}$ and $X_{E2}^{(k)}$ should be precoded based on the CSI of the EH signals; thereby, the inference of EH signals to $X_I^{(k)}$ can be reduced to a negligible level as in (3). The precoded $X_{E1}^{(k)}$ and $X_{E2}^{(k)}$ are given in Appendix A.1. Therefore, due to precoding, the SINR of $Y_{R(a)}$ at $R(a)$ does not experience any interference from EH signals, which is given as:

$$\Gamma_{R(a)} = \frac{\mathbb{E}[|\mathbf{X}_I^T \mathbf{H}_{TR}|^2]}{\mathbb{E}[|\mathbf{N}|^2]} = \frac{\sigma_{X,I}^2 \sigma_{H,TR}^2}{\sigma_N^2}, \tag{4}$$

where $\mathbb{E}[|\mathbf{X}_I|^2] = \sigma_{X,I}^2$. Thus, under the perfect channel condition, the EH signal does not affect the performance of the legitimate receiver R .

Irrespective of its location, ζ receives the signal with low SINR due to the EH signal interference. The received signal at $\zeta(a)$ is given as:

$$Y_{\zeta}^{(k)}(a) = H_{T\zeta}^{(k)} X_I^{(k)} + H_{E1\zeta}^{(k)} X_{E1}^{(k)} + H_{E2\zeta}^{(k)} X_{E2}^{(k)} + J^{(k)}, \tag{5}$$

where $Y_{\zeta}^{(k)}(a)$ is the PLNC signal, $H_{T\zeta}^{(k)} X_I^{(k)}$ is the useful information component, and the EH signal components ($H_{E1\zeta}^{(k)} X_{E1}^{(k)}$ and $H_{E2\zeta}^{(k)} X_{E2}^{(k)}$) are considered as interference to $X_I^{(k)}$. Hence, the SINR of $Y_{\zeta}^{(k)}(a)$ at $\zeta(a)$ is given as:

$$\Gamma_{\zeta(a)} = \frac{\mathbb{E}[|\mathbf{X}_I^T \mathbf{H}_{T\zeta}|^2]}{\mathbb{E}[|\mathbf{X}_{E1}^T \mathbf{H}_{E1\zeta}|^2] + \mathbb{E}[|\mathbf{X}_{E2}^T \mathbf{H}_{E2\zeta}|^2] + \mathbb{E}[|\mathbf{J}|^2]} = \frac{\sigma_{X,I}^2 \sigma_{H,T\zeta}^2}{\sigma_{H,E1\zeta}^2 \sigma_{X,E1}^2 + \sigma_{H,E2\zeta}^2 \sigma_{X,E2}^2 + \sigma_J^2}. \tag{6}$$

Note that the performance of the legitimate user is dependent on the perfect channel condition, which allows $E1$ and $E2$ to perform signal precoding using CSI. With the imperfect channel condition, the performance of R is dependent on a robust channel estimation technique as in [2,4]. The channel estimates of \mathbf{H}_{E1R} and \mathbf{H}_{E2R} are obtained by using training symbols from R to $E1$ and $E2$, respectively. The channel estimates of $H_{E1R}^{(k)}$ and $H_{E2R}^{(k)}$, respectively, are given as $\hat{H}_{E1R}^{(k)} = H_{E1R}^{(k)} + \epsilon_{E1R}^{(k)}$ and $\hat{H}_{E2R}^{(k)} = H_{E2R}^{(k)} + \epsilon_{E2R}^{(k)}$. Here, $\epsilon_{E1R}^{(k)}$ and $\epsilon_{E2R}^{(k)}$ are the channel estimation errors of $H_{E1R}^{(k)}$ and $H_{E2R}^{(k)}$, respectively. Then, the new precoded EH signals denoted as X'_{E1} and X'_{E2} are expressed in Appendix A.2. $\epsilon_{A,E1}^{(k)}$ and $\epsilon_{A,E2}^{(k)}$ are the precoding errors due to channel estimation error at $\epsilon_{E2R}^{(k)} A_{E1}^{(k)}$ and $\epsilon_{E1R}^{(k)} A_{E2}^{(k)}$, respectively.

Similarly, the received signal at $R(b)$ based on the impact of $\hat{H}_{E1R}^{(k)}$ and $\hat{H}_{E2R}^{(k)}$ is given as:

$$Y_{R(b)}^{(k)} = \begin{cases} H_{TR}^{(k)} X_I^{(k)} + N^{(k)} + \epsilon_{R(b),E1}^{(k)} + \epsilon_{R(b),E2}^{(k)}; & \text{if } \mathcal{L}(\mathcal{V}^{(k)}) = \epsilon_{R(b)}^{(k)}, \\ H_{TR}^{(k)} X_I^{(k)} + N^{(k)} + H_{E1R}^{(k)} X'_{E1} + H_{E2R}^{(k)} X'_{E2}; & \text{otherwise,} \end{cases} \quad (7)$$

where $\epsilon_{R(b),E1}^{(k)} = H_{E1R}^{(k)} \epsilon_{A,E2}^{(k)}$, $\epsilon_{R(b),E2}^{(k)} = H_{E2R}^{(k)} \epsilon_{A,E1}^{(k)}$, and $\epsilon_{R(b),E1}^{(k)}$ and $\epsilon_{R(b),E2}^{(k)}$ are the additional noise components of $Y_{R(b)}^{(k)}$ due to precoding error. Then, $\mathcal{L}(H_{E1R}^{(k)} X'_{E1} + H_{E2R}^{(k)} X'_{E2}) = \epsilon_{R(b)}^{(k)}$, where $\epsilon_{R(b)}^{(k)} = \epsilon_{R(b),E1}^{(k)} + \epsilon_{R(b),E2}^{(k)}$. The SINR of $Y_{R(b)}$ for the condition $\mathcal{L}(\mathcal{V}^{(k)}) = \epsilon_{R(b)}^{(k)}$ is given as:

$$\Gamma_{R(b)} = \frac{\mathbb{E}[|\mathbf{X}_I^T \mathbf{H}_{TR}|^2]}{\mathbb{E}[(\sum_{k=0}^{K-1} |\epsilon_{R(b),E1}^{(k)}|)^2] + \mathbb{E}[(\sum_{k=0}^{K-1} |\epsilon_{R(b),E2}^{(k)}|)^2] + \mathbb{E}[|\mathbf{N}|^2]} = \frac{\sigma_{X,I}^2 \sigma_{H,TR}^2}{\sigma_{\epsilon,R(b),E1}^2 + \sigma_{\epsilon,R(b),E2}^2 + \sigma_N^2}. \quad (8)$$

Note that, since R does not need to equalize $H_{E1R}^{(k)}$ and $H_{E2R}^{(k)}$, their respective channel estimation errors $\epsilon_{E1R}^{(k)}$ and $\epsilon_{E2R}^{(k)}$ are neglected in Equation (8).

The performance of $\zeta(b)$ is better than $\zeta(a)$ due to high channel correlations between $\mathbf{H}_{E1\zeta}$ and \mathbf{H}_{E1R} and also between $\mathbf{H}_{E2\zeta}$ and \mathbf{H}_{E2R} . Let us denote the channel correlation between $\mathbf{H}_{E1\zeta}$ and \mathbf{H}_{E1R} as ρ_{E1} . Furthermore, let us denote the channel correlation between between $\mathbf{H}_{E2\zeta}$ and \mathbf{H}_{E2R} as ρ_{E2} . ρ_{E1} and ρ_{E2} are expressed in Appendix B. The error due to ρ_{E1} and ρ_{E2} is denoted as $\epsilon_{\rho,E1}$ and $\epsilon_{\rho,E2}$, respectively. The channel precodings at $E1$ and $E2$ from the perspective of $\zeta(b)$, respectively, are given as:

$$\begin{aligned} X'_{E1} (1 + \epsilon_{\rho,E2}) &= (X_{E1}^{(k)} + \epsilon_{A,E1}^{(k)}) (1 + \epsilon_{\rho,E2}) = A_{E1}^{(k)} (H_{E2R}^{(k)} + \epsilon_{E2R}^{(k)}) (1 + \epsilon_{\rho,E2}), \\ X'_{E2} (1 + \epsilon_{\rho,E1}) &= (X_{E2}^{(k)} + \epsilon_{A,E2}^{(k)}) (1 + \epsilon_{\rho,E1}) = A_{E2}^{(k)} (H_{E1R}^{(k)} + \epsilon_{E1R}^{(k)}) (1 + \epsilon_{\rho,E1}). \end{aligned} \quad (9)$$

From the perspective of ζ , $(1 + \epsilon_{\rho,E2})$ and $(1 + \epsilon_{\rho,E1})$ are the impacts on X'_{E1} and X'_{E2} , respectively, which degrade the precoded EH signals and increase the precoding errors.

The received signal at $\zeta(b)$ is given as:

$$Y_{\zeta(b)}^{(k)} = \begin{cases} H_{T\zeta}^{(k)} X_I^{(k)} + J^{(k)} + \epsilon_{\zeta(b),E1}^{(k)} + \epsilon_{\zeta(b),E2}^{(k)}; & \text{if } \mathcal{L}(\mathcal{V}^{(k)}) = \epsilon_{\zeta(b)}^{(k)}, \\ H_{T\zeta}^{(k)} X_I^{(k)} + J^{(k)} + H_{E1R}^{(k)} X'_{E1} (1 + \epsilon_{\rho,E2}) + H_{E2R}^{(k)} X'_{E2} (1 + \epsilon_{\rho,E1}); & \text{otherwise.} \end{cases} \quad (10)$$

where $\varepsilon_{\zeta(b),E1}^{(k)} = \frac{H_{E1R}^{(k)}(X_{E1}^{(k)} + \epsilon_{A,E1}^{(k)})(1 + \epsilon_{\rho,E2})}{X_{E2}^{(k)}}$, $\varepsilon_{\zeta(b),E2}^{(k)} = \frac{H_{E2R}^{(k)}(X_{E2}^{(k)} + \epsilon_{A,E2}^{(k)})(1 + \epsilon_{\rho,E2})}{X_{E1}^{(k)}}$, and $\varepsilon_{\zeta(b),E1}^{(k)}$ and $\varepsilon_{\zeta(b),E2}^{(k)}$ are the additional noise components to $Y_{\zeta(b)}^{(k)}$. Then, $\mathcal{L}(H_{E1\zeta}^{(k)}X_{E1}^{(k)} + H_{E2\zeta}^{(k)}X_{E2}^{(k)}) = \varepsilon_{\zeta(b)}^{(k)}$, where $\varepsilon_{\zeta(b)}^{(k)} = \varepsilon_{\zeta(b),E1}^{(k)} + \varepsilon_{\zeta(b),E2}^{(k)}$. The SINR of $\mathbf{Y}_{\zeta(b)}$ for the condition $\mathcal{L}(\mathcal{V}^{(k)}) = \varepsilon_{\zeta(b)}^{(k)}$ is given as:

$$\Gamma_{\zeta(b)} = \frac{\mathbb{E}[|\mathbf{X}_I^T \mathbf{H}_{T\zeta}|^2]}{\mathbb{E}[(\sum_{k=0}^{K-1} |\varepsilon_{\zeta(b),E1}^{(k)}|^2)] + \mathbb{E}[(\sum_{k=0}^{K-1} |\varepsilon_{\zeta(b),E2}^{(k)}|^2)] + \mathbb{E}[|\mathbf{J}|^2]} = \frac{\sigma_{X,I}^2 \sigma_{H,T\zeta}^2}{\sigma_{\varepsilon,\zeta(b),E1}^2 + \sigma_{\varepsilon,\zeta(b),E2}^2 + \sigma_J^2}. \quad (11)$$

The best scenario for ζ is $\zeta(c)$, where, the precoding errors due to the channel estimation errors can be avoided at \mathcal{T} . However, there will be a precoding error due to $H_{E1R}^{(k)}(1 + \epsilon_{\rho,E1})$ and $H_{E2R}^{(k)}(1 + \epsilon_{\rho,E2})$. Hence, the precoded EH signals can be written as:

$$\begin{aligned} X_{E1}^{(k)}(1 + \epsilon_{\rho,E2}) &= A_{E1}^{(k)} H_{E2R}^{(k)}(1 + \epsilon_{\rho,E2}), \\ X_{E2}^{(k)}(1 + \epsilon_{\rho,E1}) &= A_{E2}^{(k)} H_{E1R}^{(k)}(1 + \epsilon_{\rho,E1}). \end{aligned} \quad (12)$$

Then, the received signal at $\zeta(c)$ is given as:

$$Y_{\zeta(c)}^{(k)} = \begin{cases} H_{T\zeta}^{(k)} X_I^{(k)} + N^{(k)} + \varepsilon_{\zeta(c),E1}^{(k)} + \varepsilon_{\zeta(c),E2}^{(k)}; & \text{if } \mathcal{L}(\mathcal{V}^{(k)}) = \varepsilon_{\zeta(c)}^{(k)}, \\ H_{T\zeta}^{(k)} X_I^{(k)} + N^{(k)} + H_{E1R}^{(k)} X_{E1}^{(k)}(1 + \epsilon_{\rho,E2}) + H_{E2R}^{(k)} X_{E2}^{(k)}(1 + \epsilon_{\rho,E1}); & \text{otherwise,} \end{cases} \quad (13)$$

where $\varepsilon_{\zeta(c),E1}^{(k)} = H_{E1R}^{(k)}(1 + \epsilon_{\rho,E2})$ and $\varepsilon_{\zeta(c),E2}^{(k)} = H_{E2R}^{(k)}(1 + \epsilon_{\rho,E1})$. Then, $\mathcal{L}(H_{E1\zeta}^{(k)}X_{E1}^{(k)} + H_{E2\zeta}^{(k)}X_{E2}^{(k)}) = \varepsilon_{\zeta(c)}^{(k)}$, where $\varepsilon_{\zeta(c)}^{(k)} = \varepsilon_{\zeta(c),E1}^{(k)} + \varepsilon_{\zeta(c),E2}^{(k)}$. The SINR of $\mathbf{Y}_{\zeta(c)}$ for the condition $\mathcal{L}(\mathcal{V}^{(k)}) = \varepsilon_{\zeta(c)}^{(k)}$ is given as:

$$\Gamma_{\zeta(c)} = \frac{\mathbb{E}[|\mathbf{X}_I^T \mathbf{H}_{T\zeta}|^2]}{\mathbb{E}[(\sum_{k=0}^{K-1} |\varepsilon_{\zeta(c),E1}^{(k)}|^2)] + \mathbb{E}[(\sum_{k=0}^{K-1} |\varepsilon_{\zeta(c),E2}^{(k)}|^2)] + \mathbb{E}[|\mathbf{J}|^2]} = \frac{\sigma_{X,I}^2 \sigma_{H,T\zeta}^2}{\sigma_{\varepsilon,\zeta(c),E1}^2 + \sigma_{\varepsilon,\zeta(c),E2}^2 + \sigma_J^2}. \quad (14)$$

For all the scenarios of ζ and $R(b)$, the channel precoding error is denoted as ϵ_A , and its variance is denoted as σ_A^2 . In this system model, both the channel estimate errors and the channel correlation errors are considered to be the sole contributors of ϵ_A , and ϵ_A proportionally increases with the increase in β . To form the generalized SINR equation, $\sigma_{H,TR}^2$ and $\sigma_{H,T\zeta}^2$ are assumed as one; then, the SINR of the received signal at R and ζ can be written as:

$$\Gamma = \frac{\sigma_{X,I}^2}{\sigma_N^2 + \beta \sigma_A^2}, \quad (15)$$

At a very high SINR of the information signal, σ_N^2 can be neglected. Then, Equation (15) can be written as:

$$\Gamma \approx \frac{\sigma_{X,I}^2}{\beta \sigma_A^2}. \quad (16)$$

Therefore, even at a very high SINR condition, $\beta \sigma_A^2$ can be used to degrade the performance of ζ . The secrecy of \mathbf{X}_I can be improved at $R(a)$ and $R(b)$ by increasing β under the condition that the σ_A^2 value in $\mathbf{Y}_{R(a)}$ and $\mathbf{Y}_{R(b)}$ is lesser than the σ_A^2 value in $\mathbf{Y}_{\zeta(a)}$, $\mathbf{Y}_{\zeta(b)}$, and $\mathbf{Y}_{\zeta(c)}$. Another observation from Equation (15) indicates that, if $\beta \geq 1$, then $\zeta(a)$ will always be in the negative SINR region.

2.1. Secrecy Rate Analysis

The secrecy rate analysis of this system model is based on the Gaussian wiretap channel secrecy capacity, which deduces the difference between Shannon’s capacity of R and ζ . The maximum

achievable secrecy rate is the secrecy capacity of R [8,9]. The secrecy capacity of $R(a)$ with respect to $\zeta(a)$ and the secrecy capacity of $R(a)$ with respect to $\zeta(c)$, respectively, are given (The notation for the secrecy rate of $R(a)$ with respect to $\zeta(c)$ is given as $\mathbb{C}_{(c),A}$, where (c) denotes $\zeta(c)$ and A denotes $R(a)$. A similar rule is followed for the other three secrecy rate notions.) as:

$$\begin{aligned} \mathbb{C}_{(a),A} &= \frac{\Delta f}{k} \sum_{k=0}^{K-1} \left(\log \left(\frac{1 + |H_{TR}^{(k)}|^2 \Gamma_{R(a)}}{1 + |H_{T\zeta}^{(k)}|^2 \Gamma_{\zeta(a)}} \right) \right), \\ \mathbb{C}_{(c),A} &= \frac{\Delta f}{k} \sum_{k=0}^{K-1} \left(\log \left(\frac{1 + |H_{TR}^{(k)}|^2 \Gamma_{R(a)}}{1 + |H_{T\zeta}^{(k)}|^2 \Gamma_{\zeta(c)}} \right) \right), \end{aligned} \tag{17}$$

where $2\Delta f$ is the bandwidth and Δf is the peak frequency deviation. The secrecy capacity of $R(b)$ with respect to $\zeta(a)$ and the secrecy capacity of $R(b)$ with respect to $\zeta(b)$, respectively, are given as:

$$\begin{aligned} \mathbb{C}_{(a),B} &= \frac{\Delta f}{k} \sum_{k=0}^{K-1} \left(\log \left(\frac{1 + |H_{TR}^{(k)}|^2 \Gamma_{R(b)}}{1 + |H_{T\zeta}^{(k)}|^2 \Gamma_{\zeta(a)}} \right) \right), \\ \mathbb{C}_{(b),B} &= \frac{\Delta f}{k} \sum_{k=0}^{K-1} \left(\log \left(\frac{1 + |H_{TR}^{(k)}|^2 \Gamma_{R(b)}}{1 + |H_{T\zeta}^{(k)}|^2 \Gamma_{\zeta(b)}} \right) \right). \end{aligned} \tag{18}$$

Here, the interference of the EH signals is used as the external noise to improve the maximum achievable secrecy rate of R , and by increasing β , the secrecy capacity can be improved in all scenarios. Even though β can reduce the capacity of $R(b)$ due to the amplification of channel estimation errors, since $\zeta(b)$ also has channel correlation error in addition to the channel estimate errors, β will improve R 's secrecy capacity.

2.2. Iterative Block Decision Feedback Equalization Receiver

In this system model, it is assumed that both R and ζ employ IB-DFE to improve the accuracy of the information estimate as proposed in [18]. The IB-DFE based estimate for $X_I^{(k)}$ at R is given as:

$$\tilde{X}_I^{(j,k)} = Y_I^{(k)} F^{(j,k)} - \tilde{X}_I^{(j-1,k)} B^{(j,k)}, \tag{19}$$

where $j = 0, 1, \dots, J$, j is the number of iterations followed in the IB-DFE receiver, $\tilde{X}_I^{(j-1,k)}$ is the previous iteration value of $\tilde{X}_I^{(j,k)}$, and $F^{(j,k)}$ is the iteration of the feedforward coefficient, given as:

$$F^{(j,k)} = \frac{\tilde{F}^{(j,k)}}{\frac{1}{K} \sum_{k=0}^{K-1} (\tilde{F}^{(j,k)} H_{TR}^{(j,k)})}, \tag{20}$$

where $\tilde{F}^{(j,k)}$ is written as:

$$\tilde{F}^{(j,k)} = \frac{H_{TR}^{(j,k)*}}{\left(\frac{\sigma_N^2}{\sigma_{X_I}^2} \right) + |H_{TR}^{(j,k)}|^2 (1 - (\rho^{(j-1)})^2)}, \tag{21}$$

and the correlation factor $\rho^{(j-1)} = \frac{\mathbb{E}[\hat{x}_i^{(j,n)} x_i^{(j,n*)}]}{\mathbb{E}[|x_i^{(j,n)}|^2]}$, where $x_i^{(j,n)}$ is time domain equivalent of $X_I^{(j,k)}$ and $\hat{x}_i^{(j,n)}$ is the extrinsic information of $x_i^{(j,n)}$. Furthermore, $\{X_I^{(j,k)}; k = 0, 1, \dots, K - 1\} = \text{DFT} \{x_i^{(j,n)} g_n; n = 0, 1, \dots, N - 1\}$, and if the n^{th} time domain is inside the cycle prefix, then g_n is either one or zero. The feedback co-efficient $B^{(j,k)}$ is written as:

$$B^{(j,k)} = F^{(j,k)} H_{TR}^{(j,k)} - 1. \tag{22}$$

In fact, the accuracy of $\tilde{X}_I^{(j,k)}$ increases with each iteration up to its saturation point. Similarly, the accuracy of the information estimate can be improved at R and ζ for all the scenarios except $\zeta(a)$. For $\zeta(a)$, $\tilde{X}_I^{(j,k)}$ is completely distorted by EH signals.

The performance of the IB-DFE receiver can be improved at $R(b)$ with improved feedforward input in the iteration. The feedforward estimate, $\tilde{F}^{(j,k)}$, is derived in Equation (21), and this estimate can be improved by including the impact of $\beta\sigma_A^2$ in the SINR of the information signal. Therefore, by using Equation (15) in (21), we get:

$$\tilde{F}^{(j,k)} = \frac{H_{TR}^{(j,k)*}}{\left(\frac{\sigma_N^2 + \beta\sigma_A^2}{\sigma_{x,I}^2}\right) + |H_{TR}^{(j,k)}|^2 (1 - (\rho^{(j-1)})^2)}. \quad (23)$$

Here, unlike the eavesdropper, $R(b)$ can take advantage of the available knowledge from the legitimate transmitter and improve the performance of $R(b)$; therefore, $R(b)$ with the improved feedback estimate can perform better than ζ .

3. Numerical Results

In this section, the BER performance of the legitimate user and eavesdropper in the system model is analyzed by using Monte Carlo simulations. The signal used the 2.4 GHz frequency band, $T = 4 \times 10^{-6}$, and it was considered that all the communication nodes including the eavesdroppers were operating in the non-line-of-sight channel condition. The secrecy rate was another performance metric of the legitimate user in the presence of the eavesdropper at various conditions and was analyzed through simulations. In the following simulations, the system adopted the 4-QAM signal with $K = 256$ and $L = 200$, and the IB-DFE receiver was used in R and ζ to improve their error rate performance. The channel estimate errors of the \mathbf{H}_{E1R} and \mathbf{H}_{E2R} links, i.e., ϵ_{E1R} and ϵ_{E2R} , respectively were assumed to be equal, i.e., $\epsilon_{E1R} = \epsilon_{E2R}$, and ϵ_{E1R} was either 0.02 or 0.1. We assumed that, under an exceptionally favorable circumstance, $\rho_{E1} = \rho_{E2} = 0.99$ and 0.98; this allowed $\zeta(b)$ and $\zeta(c)$ to perform better than $\zeta(a)$. In the following figures, the BER performance results by default illustrate the fourth iteration of the IB-DFE decoder unless it is specified as zero-forcing (ZF) decoding.

Figure 3 demonstrates the BER performance of $R(a)$ and $R(b)$. We see that the BER performance of $R(a)$ did not vary with the change in β , due to the successful channel precoding, which was based on the complete CSI of the EH signals, i.e., jamming signals. Furthermore, the results of $R(a)$ demonstrated that the performance of IB-DFE receiver and BER improved up to the fourth iteration. In the first iteration, without any feedforward and feedback values, the resultant BER of the first iteration was equal to the ZF decoding. For $R(b)$, the channel precoding error occurred due to ϵ_{E1R} , where $\epsilon_{E1R} = 0.02$ and 0.1, and the results demonstrated that due to the precoding error at the transmitter, the BER performance of $R(b)$ was poorer as compared to $R(a)$. When $\epsilon_{E1R} = 0.2$, up to $\beta = 4$, the performance of $R(b)$ was equivalent to that of $R(a)$, whereas for $\beta > 4$, the performance of $R(b)$ degraded with the increase in β . The precoding error increased proportionally with the increase in ϵ_{E1R} , and β acted as a multiplication factor in increasing the precoding error.

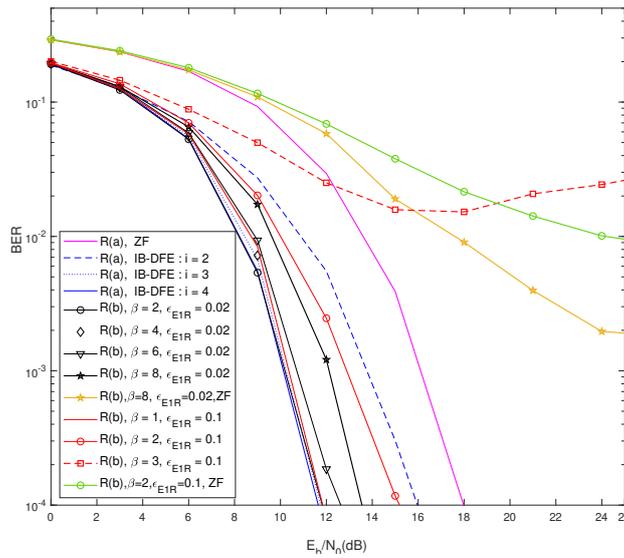


Figure 3. BER performance of $R(a)$ and $R(b)$. ZF, zero-forcing.

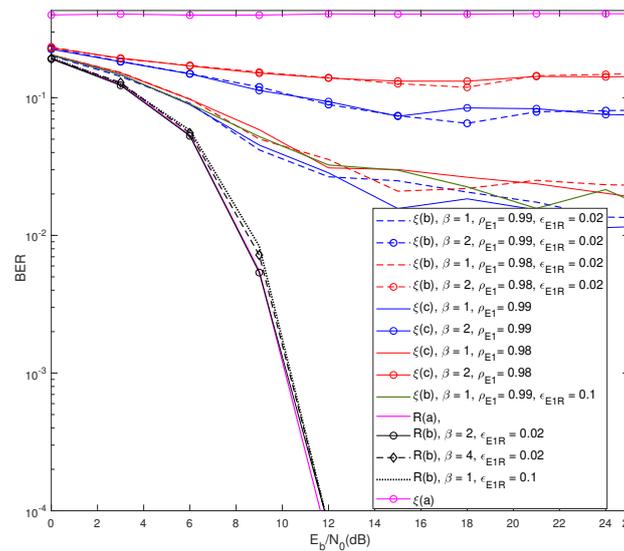


Figure 4. BER performance of ζ in all the scenarios with $\epsilon_{E1R} = 0.02$ in Scenario B.

Figure 4 demonstrates the BER performance of ζ in all the scenarios with the comparison to BER of R , and $\zeta(a)$ received an incompatible signal for decoding the information. Unlike $\zeta(a)$, with $\rho_{E1} = \rho_{E2} = 0.99$ and 0.98 , $\zeta(b)$ and $\zeta(c)$ could partially decode the signal, and their performance degraded with the decrease in ρ_{E1} as the precoding errors increased in turn. Due to high channel correlation between $\mathbf{H}_{E1\zeta}$ and \mathbf{H}_{E1R} and similarly between $\mathbf{H}_{E1\zeta}$ and \mathbf{H}_{E1R} , the jamming EH signals were partially canceled out in $\zeta(b)$ and $\zeta(c)$, allowing them to perform better than $\zeta(a)$. With $\epsilon_{E1R} = 0.02$, $\zeta(b)$ performed slightly more poorly as compared to $\zeta(c)$. Even though $\zeta(b)$ and $\zeta(c)$ could decode information in the high channel correlation condition, the BER results of R demonstrated that, by increasing β , the jamming signals could degrade the performance of ζ , while R suffered a negligible loss.

Figure 5 demonstrates the impact of the inclusion of $\beta\sigma_A^2$ in the IB-DFE receiver, and the results validated the advantage of using (23) over (21) in the iterative loop. R_i had significant SINR gain over $R(b)$ with the increase in β . At $\beta = 10$, R_i had 0.5 dBm SINR gain over $R(b)$, and when $\beta > 12$, R_i had more than 6 dBm SINR gain over $R(b)$. The results also illustrated the BER difference between the

best performance of $\zeta(c)$, i.e., $\zeta(c)$ with $\beta = 1$ and $\rho_{E1} = \rho_{E2} = 0.99$ versus the performance of R_i with $\beta = 13$.

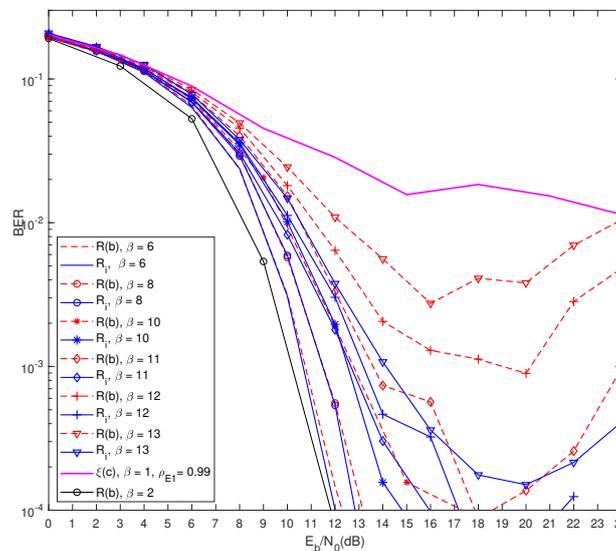


Figure 5. BER performance of $R(b)$ and R_i with $\epsilon_{E1R} = 0.02$, where R_i denotes $R(b)$ with an improved feedback loop in the IB-DFE receiver.

In Figure 6, we compare the BER performance of R_i in Rician fading and Rayleigh frequency flat fading channel conditions. For the simulation of Rician fading, we set $T = 4 \times 10^{-6}$ for 256 symbols; the multipath gain range was $0 : -3 : -45$; the Doppler shift was 50; and the k factor was 10. The results of Figure 6 demonstrate that the BER performance of R_i under both fading conditions had similar effects on the signal performance. The fading effects were relatively low due to the application of SC-FDMA, and the BER performance improved with the IB-DFE receiver.

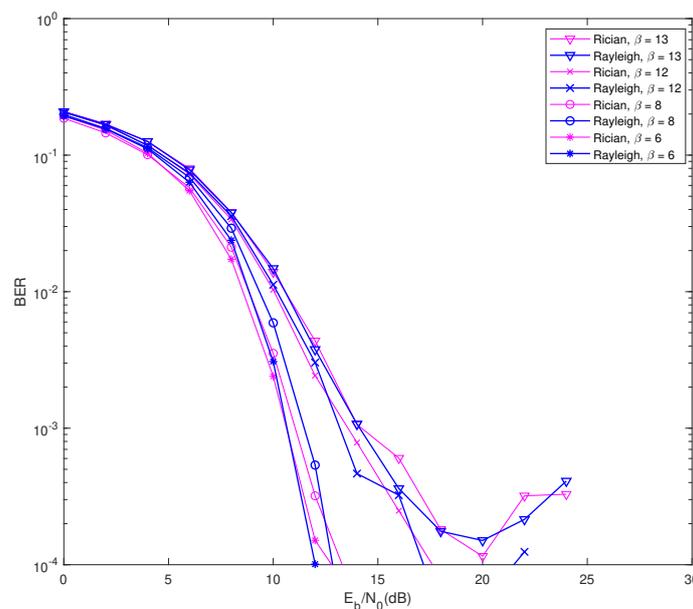


Figure 6. BER performance of R_i in Rician fading and Rayleigh fading conditions.

Figure 7 demonstrates the secrecy rate of $R(a)$ and $R(b)$ based on (17) and (18), respectively. Since $\zeta(a)$ was always in the negative SINR region, $C_{(a),A}$ had the best performance over $C_{(c),A}$, $C_{(a),B}$ and

$\mathbb{C}_{(b),B}$. For any given β value, $\mathbb{C}_{(c),A}$ always performed better than $\mathbb{C}_{(b),B}$ because in $\mathbb{C}_{(c),A}$, neither $\zeta(c)$ nor $R(a)$ experienced channel estimation error. The performance of $\mathbb{C}_{(a),B}$ and $\mathbb{C}_{(b),B}$ did not improve when the SINR was greater than 20 dBm because $R(b)$ experienced precoding error due to the channel estimate error of the EH signals, which was $\epsilon_{E1R} = 0.02$, and it was independent of the SINR of the information signal as observed in (15) and (16). The results of $\mathbb{C}_{(c),A}$ and $\mathbb{C}_{(a),B}$ proved that, at high SINR (i.e., greater than 20 dBm), $\mathbb{C}_{(c),A}$ could perform better than $\mathbb{C}_{(a),B}$, irrespective of ζ' 's condition. At low SINR (i.e., less than 20 dBm), the performance of $\mathbb{C}_{(a),B}$ as compared to $\mathbb{C}_{(c),A}$ was better because $R(b)$ took advantage of $\zeta(a)$'s poor performance, and this characteristic validated (15) and (16). Similar to the BER results, the secrecy rate performance of $\mathbb{C}_{(c),A}$ and $\mathbb{C}_{(b),B}$ was better when $\rho_{E1} = 0.98$ than their performance when $\rho_{E1} = 0.99$. The secrecy rate of $R(a)$ improved with the increase in β , but in the case of $R(b)$, contrary to the BER results, the secrecy rate degraded with the increase in β due to the channel estimate error. Unlike the secrecy rate results of $R(b)$, the impact of channel estimate error on the BER of $R(b)$ was reduced due to the implementation the IB-DFE receiver.

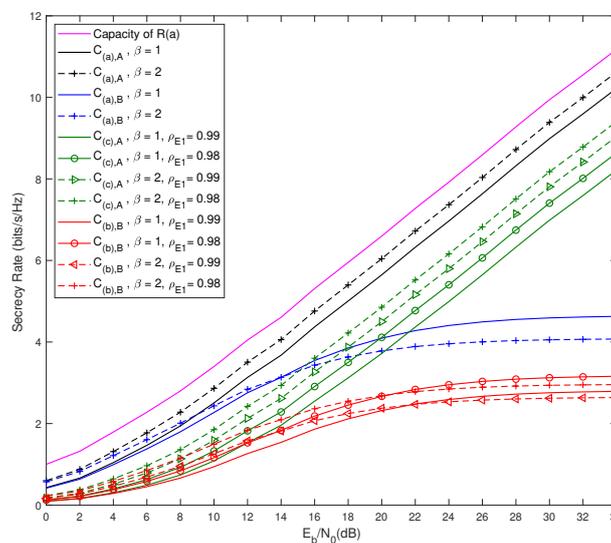


Figure 7. The secrecy rate of $R(a)$ and $R(b)$ and in Scenario B, $\epsilon_{E1R} = 0.02$.

4. Conclusions

In this paper, we implemented the SWIPT based self jamming physical layer security model, which relied on the channel precoding method to transmit information securely to the legitimate user. We considered different case studies by assuming that the eavesdropper had high channel correlation with the legitimate user. We also considered the possibility of channel estimate error (the channel link between jamming antennas to the legitimate user), which negatively affected the channel precoding. All the study cases were analyzed with the theoretical expressions supported by the simulation results.

The BER performance of the legitimate user and eavesdropper was improved by using the IB-DFE receiver, and we concluded that the channel precoding error could be further reduced at the legitimate user by taking advantage of all the available knowledge (i.e., including the variance of channel precoding error) in the IB-DFE receiver. Thus, the legitimate user could perform better than the eavesdropper, and the performance of the legitimate user improved over the eavesdropper with the increase in the jamming signal power. The secrecy rate analysis of legitimate user demonstrated that the performance of the legitimate user with the channel precoding error did not improve beyond 20 dBm SINR and slightly degraded with the increase in jamming signal power. In the case of perfect channel precoding, the secrecy rate performance of the legitimate user improved proportionally with the increase in SINR and with the increase in the jamming signal power.

Author Contributions: Conceptualization, A.R. and R.D.; investigation, A.R., M.B., and R.D.; software, A.R.; supervision, R.D. and D.N.K.J.; validation, D.N.K.J. and R.D.; visualization, A.R.; writing, original draft, A.R., M.B., D.N.K.J., and R.D.; writing, review and editing, A.R. and R.D. All authors read and agreed to the published version of the manuscript.

Funding: This work was supported by FCT/MCTES through national funds and when applicable co-funded EU funds under the project MASSIVE5G(PTDC/EEI-TEL/30588/2017), Copelabs (UIDB/04111/2020), and Instituto de Telecomunicações (UIDB/EEA/50008/2020). The research work was developed in part with Universidade Lusófona/ILIND funding and supported, in part, by the Russian Foundation for Basic Research (RFBR) Grant No. 19-37-50083\19.

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

Appendix A

The precoding vector for the legitimate receiver is given below.

Appendix A.1

The precoded EH signals at $R(a)$, denoted as $X_{E1}^{(k)}$ and $X_{E2}^{(k)}$, are given by:

$$\begin{aligned} X_{E1}^{(k)} &= A_{E1}^{(k)} H_{E2R}^{(k)}, \\ X_{E2}^{(k)} &= A_{E2}^{(k)} H_{E1R}^{(k)}, \end{aligned} \quad (\text{A1})$$

where $A_{E1}^{(k)}$ and $A_{E2}^{(k)}$ are the k^{th} entries of the precoding vectors \mathbf{A}_{E1} and \mathbf{A}_{E2} , respectively. The precoding vectors are chosen such that, under any SINR condition, $\mathcal{L}(H_{E1R}^{(k)} X_{E1}^{(k)} + H_{E2R}^{(k)} X_{E2}^{(k)}) = 0$.

Appendix A.2

The precoded EH signals at $R(b)$, denoted as $X'_{E1}{}^{(k)}$ and $X'_{E2}{}^{(k)}$, are given by:

$$\begin{aligned} X'_{E1}{}^{(k)} &= X_{E1}^{(k)} + \epsilon_{A,E1}^{(k)} = A_{E1}^{(k)} (H_{E2R}^{(k)} + \epsilon_{E2R}^{(k)}), \\ X'_{E2}{}^{(k)} &= X_{E2}^{(k)} + \epsilon_{A,E2}^{(k)} = A_{E2}^{(k)} (H_{E1R}^{(k)} + \epsilon_{E1R}^{(k)}), \end{aligned} \quad (\text{A2})$$

where $\epsilon_{A,E1}^{(k)}$ and $\epsilon_{A,E2}^{(k)}$ are the precoding errors due to $\epsilon_{E2R}^{(k)} A_{E1}^{(k)}$ and $\epsilon_{E1R}^{(k)} A_{E2}^{(k)}$, respectively.

Appendix B

The channel correlations (ρ_{E1} and ρ_{E2}) are given as:

$$\begin{aligned} \rho_{E1} &= \frac{\mathbb{E}[|\mathbf{H}_{E1R} \mathbf{H}_{E1\xi}^H|]}{\sqrt{\mathbb{E}[|\mathbf{H}_{E1R}|^2] \mathbb{E}[|\mathbf{H}_{E1\xi}|^2]}}, \\ \rho_{E2} &= \frac{\mathbb{E}[|\mathbf{H}_{E2R} \mathbf{H}_{E2\xi}^H|]}{\sqrt{\mathbb{E}[|\mathbf{H}_{E2R}|^2] \mathbb{E}[|\mathbf{H}_{E2\xi}|^2]}}. \end{aligned} \quad (\text{A3})$$

References

1. Jayakody, D.N.K.; Thompson, J.; Chatzinotas, S.; Durrani, S. *Wireless Information and Power Transfer: A New Green Communications Paradigm*; Springer: New York, NY, USA, 2017.
2. Perera, T.D.P.; Jayakody, D.N.K.; Sharma, S.K.; Chatzinotas, S.; Li, J. Simultaneous wireless information and power transfer (swipt): Recent advances and future challenges, *IEEE Commun. Surv. Tutor.* **2018**, *20*, 264–302. [[CrossRef](#)]
3. Rajaram, A.; Khan, R.; Tharranetharan, S.; Jayakody, D.; Dinis, R.; Panic, S. Novel SWIPT Schemes for 5G Wireless Networks. *Sensors* **2019**, *19*, 1169. [[CrossRef](#)] [[PubMed](#)]

4. Rajaram, A.; Jayakody, D.N.K.; Dinis, R.; Kumar, N. Receiver Design to Employ Simultaneous Wireless Information and Power Transmission with Joint CFO and Channel Estimation. *IEEE Access* **2019**, *7*, 9678–9687. [[CrossRef](#)]
5. Tang, X.; Cai, Y.; Yang, W.; Yang, W.; Chen, D.; Hu, J. Secure transmission of cooperative zero-forcing jamming for two-user SWIPT sensor networks. *Sensors* **2018**, *18*, 331. [[CrossRef](#)] [[PubMed](#)]
6. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M.; Li, J. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 196–248.
7. Ng, D.W.K.; Xiang, L.; Schober, R. Multi-objective beamforming for secure communication in systems with wireless information and power transfer. In Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London, UK, 8–11 September 2013; pp. 7–12.
8. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [[CrossRef](#)]
9. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [[CrossRef](#)]
10. Oggier, F.; Hassibi, B. The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 4961–4972. [[CrossRef](#)]
11. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [[CrossRef](#)]
12. Anjos, G.; Castanheira, D.; Silva, A.; Gameiro, A.; Gomes, M.; Vilela, J.P. Exploiting the Reciprocal Channel for Discrete Jamming to Secure Wireless Communications Against Multiple-Antenna Eavesdropper. *IEEE Access* **2018**, *6*, 1–10. [[CrossRef](#)]
13. Anjos, G.; Castanheira, D.; Silva, A.; Gameiro, A. Exploiting Reciprocal Channel Estimations for Jamming to Secure Wireless Communications. In Proceedings of the 2017 International Wireless Days Conference, Porto, Portugal, 29–31 March 2017.
14. Cumanan, K.; Xing, H.; Xu, P.; Zheng, G.; Dai, X.; Nallanathan, A.; Ding, Z.; Karagiannidis, G.K. Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks. *IEEE Access* **2017**, *5*, 3603–3611. [[CrossRef](#)]
15. He, B.; Zhou, X.; Abhayapala, T.D. Wireless physical layer security with imperfect channel state information: A survey. *arXiv* **2013**, arXiv:1307.4146.
16. Chou, T.; Draper, S.C.; Sayeed, A. M. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In Proceedings of the 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 2518–2522.
17. Zhang, B.; He, T.; Duong, Q.; Woods, R. On the Key Generation From Correlated Wireless Channels. *IEEE Commun. Lett.* **2017**, *21*, 961–964. [[CrossRef](#)]
18. Benvenuto, N.; Tomasin, S. Block iterative DFE for single carrier modulation. *Electron. Lett.* **2002**, *38*, 1144–1145. [[CrossRef](#)]
19. Silva, A.; Assunção, J.; Dinis, R.; Gameiro, A. Performance Evaluation of IB-DFE based Strategies for SC-FDMA Systems. *EURASIP J. Wirel. Commun. Netw.* **2013**, *2013*, 1–10. [[CrossRef](#)]
20. Castanheira, D.; Silva, A.; Dinis, R.; Gameiro, A. Efficient Transmitter and Receiver Designs for SC-FDMA Based Heterogeneous Networks. *IEEE Trans. Commun.* **2015**, *63*, 2500–2510. [[CrossRef](#)]
21. Silva, A.; Teodoro, S.; Dinis, R.; Gameiro, A. Iterative Frequency-Domain Detection for IA-Precoded MC-CDMA Systems. *IEEE Trans. Commun.* **2014**, *62*, 1240–1248. [[CrossRef](#)]
22. Dinis, R.; Lam, C.T.; Falconer, D. Joint frequency-domain equalization and channel estimation using superimposed pilots. In Proceedings of the 2008 Wireless Communications and Networking Conference, Las Vegas, NV, USA, 31 March–3 April 2008; pp. 447–452.

