sensors

MDPI

Article

Secrecy Coding Analysis of Short-Packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes

Bao Quoc Vuong [1,2,3,*], Roland Gautier [1], Anthony Fiche [1], Mélanie Marazin [1] and Cristina Despina-Stoian [1,4]

[1] Univ Brest, CNRS, Lab-STICC, CS 93837, 6 Avenue Le Gorgeu, CEDEX 3, 29238 Brest, France; roland.gautier@univ-brest.fr (R.G.); anthony.fiche@univ-brest.fr (A.F.); melanie.marazin@univ-brest.fr (M.M.); cristina.despina@mta.ro (C.D.-S.)
[2] School of Electrical Engineering, International University, Ho Chi Minh City 700000, Vietnam
[3] Vietnam National University, Ho Chi Minh City 700000, Vietnam
[4] Telecommunications and Information Technology Department, Military Technical Academy "Ferdinand I", 050141 Bucharest, Romania
* Correspondence: bao.vuong@univ-brest.fr

Abstract: This paper studies the secrecy coding analysis achieved by the self-jamming technique in the presence of an eavesdropper by considering a short-packet Full-Duplex (FD) transmission developed based on iterative blind or semi-blind channel estimation and advanced decoding algorithms. Indeed, the legitimate receiver and eavesdropper can simultaneously receive the intended signal from the transmitter and broadcast a self-jamming or jamming signal to the others. Unlike other conventional techniques without feedback, the blind or semi-blind algorithm applied at the legitimate receiver can simultaneously estimate, firstly, the Self-Interference (SI) channel to cancel the SI component and, secondly, estimate the propagation channel, then decode the intended messages by using 5G Quasi-Cyclic Low-Density Parity Check (QC-LDPC) codes. Taking into account the passive eavesdropper case, the blind channel estimation with a feedback scheme is applied, where the temporary estimation of the intended channel and the decoded message are fed back to improve both the channel estimation and the decoding processes. Only the blind algorithm needs to be implemented in the case of a passive eavesdropper because it achieves sufficient performances and does not require adding pilot symbols as the semi-blind algorithm. In the case of an active eavesdropper, based on its robustness in the low region of the Signal-to-Noise Ratio (SNR), the semi-blind algorithm is considered by trading four pilot symbols and only requiring the feedback for channel estimation processes in order to overcome the increase in noise in the legitimate receiver. The results show that the blind or semi-blind algorithms outperform the conventional algorithm in terms of Mean Square Error (MSE), Bit Error Rate (BER) and security gap (S_g). In addition, it has been shown that the blind or semi-blind algorithms are less sensitive to high SI and self-jamming interference power levels imposed by secured FD transmission than the conventional algorithms without feedback.

Keywords: security gap; channel coding scheme; physical layer security; self-jamming; feedback; blind channel estimation; semi-blind channel estimation

Citation: Vuong, B.Q.; Gautier, R.; Fiche, A.; Marazin, M.; Despina-Stoian, C. Secrecy Coding Analysis of Short-Packet Full-Duplex Transmissions with Joint Iterative Channel Estimation and Decoding Processes. *Sensors* **2022**, *22*, 5257. https://doi.org/10.3390/s22145257

Academic Editor: Qammer Hussain Abbasi

Received: 30 May 2022
Accepted: 12 July 2022
Published: 14 July 2022

1. Introduction

The development of future wireless technologies such as massive MIMO systems, machine type communications, millimeter wave transmissions, and especially the Internet of Things (IoT) has led to not only new challenges but also new opportunities in the 5G security domains [1]. In order to achieve enhanced security performances for the wireless communications, a better strategy is setting up based on the physical layer directly, which is a method that belongs to the information theory field. This category of security solutions, also known as Physical Layer Security (PLS), has recently emerged as a new security or

additional security layer, especially in 5G networks and beyond [2,3]. The wiretap channel was first introduced by Wyner in 1975 and became fundamental in characterizing PLS problems, where the intended transmitter sends a message to the legitimate receiver while the passive eavesdropper tries to listen and decode this message [4]. A decade later, Ozarow and Wyner introduced the second type of wiretap channel, known as wiretap channel II, where the active eavesdropper not only listens to the intended transmitter but also transmits a jamming signal to the legitimate receiver [5]. Therefore, the presence of an active eavesdropper can more strongly destroy the reception behavior of the legitimate receiver than that of the passive eavesdropper in the secrecy of wireless communication links [6]. As a metric of PLS, the security gap was first introduced in [7], which is calculated as the ratio of the Bit Error Rate (BER) on the linear scale or the difference of the BERs on the log scale achieved by the legitimate receiver and the eavesdropper to ensure that the legitimate receiver can reliably receive the intended message and to maintain security throughout transmission.

Due to the improved spectral efficiency, Full-Duplex (FD) communication systems that simultaneously transmit and receive information using the same time-frequency channel resource became an essential approach in 5G and beyond communication networks, especially in IoT transmissions and green communications [8,9]. However, Self-Interference (SI) cancellation is still the biggest challenge of any FD system due to the channel estimation error caused by the complexity of the SI channel, particularly in the case of short-frame transmission [10–12]. The presence of SI will reduce the Signal-to-Noise Ratio (SNR) at the receiver and leads to low overall performance. Considering the PLS in FD transmission, the security approaches involving the simultaneous transmission of the self-jamming or Artificial Noise (AN) have attracted a huge research interest due to their robustness promising performance [13,14]. The self-jamming technique is usually used to make the interception and the correct message decoding impossible for the eavesdroppers, even if they have equivalent or better channel conditions than the legitimate receiver. Therefore, the self-jamming approach has been widely studied and extended in numerous schemes to enhance the PLS, i.e., the FD transceiver can simultaneously receive the intended message and broadcast the AN to degrade the eavesdropper channel [15–17]. The AN technique is also used for secure transmission in cognitive wiretap networks with FD receivers [18] or FD relay systems [19]. Usually, the PLS mechanism related to the self-jamming and AN has been studied assuming that the eavesdropper cannot estimate the wiretap channel or jamming channel based on the known training pilots and transmitted power [20]. However, a large number of training pilots are required to be involved, and it is still not a satisfying solution in terms of time, bandwidth, and power consumption, especially for short-frame FD transmission, because the training requires a huge number of data symbols to obtain a good second-order statistic of the received signal. Furthermore, channel secrecy capacity and transmission message reliability can be a problem for communications with finite block length or short-packet [6]. Therefore, the PLS on short-packet transmission has recently become an open area to be focused on in 5G and beyond, especially for IoT transmissions and green communications.

Furthermore, new radio channel coding schemes such as 5G Quasi-Cyclic Low-Density Parity Check (QC-LDPC) codes can also be chosen for the PLS problem due to their higher error correction performance and powerful decoding for both on and below the reliability threshold [1,7], as well as sufficient performance in ultra-reliable Low Latency Communication (uRLLC) in short-packet 5G transmission systems [21]. In recent years, many researchers have focused on secrecy channel coding techniques in the wiretap channel [22–25]. In particular, the authors in [23] evaluated the reliability and security over the flat and fast-fading Gaussian wiretap channel for the construction of various LDPC codes with the puncturing and scrambling techniques. Furthermore, the authors in [26] used the McEliece coding method based on LDPC Code to guarantee both information reliability between intended users and the security metric with respect to eavesdroppers in PLS. The authors in [24] also studied the combination of LDPC codes and AN by designing

the scrambling matrix to reduce the probability of outage and improve PLS. Then, the authors in [25] proposed combining the LDPC codes at the transmitter and an iterative decoding algorithm at the receiver to reduce the security gap in the Gaussian wiretap channel. The results obtained show that their proposed scheme outperforms the punctured scheme in terms of the equivocation rate and the security gap. Last but not least, the authors in [27,28] proposed joint iterative blind and semi-blind algorithms for channel estimations and decoding processes in short-packet FD transmission. The results show that these algorithms outperform the conventional algorithms without feedback in terms of not only Mean Square Error (MSE) and BER performances but also processing time and computational complexity, which are suitable for IoT transmissions and green communications.

Therefore, in this paper, we propose and implement a new scheme that combines joint iterative channel estimation and decoding using 5G QC-LDPC codes with FD self-jamming of the legitimate receiver to enhance security and reliability, which means that the eavesdropper does not catch the information and the indented information is less affected or corrupted by the jamming signal, respectively, in two scenarios: a passive eavesdropper and an active eavesdropper. For the rest of this paper, the performance evaluations of the proposed algorithms are based on three metrics: MSE, BER, and security gap (S_g). The contributions of this paper can be summarized as follows:

- We evaluate a combination of self-jamming techniques with a joint iterative blind or semi-blind channel estimation and decoding for a FD short-packet transmissions in the cases of passive and active eavesdroppers, respectively;
- We characterize that the system developed based on the new proposed algorithms have better performance compared to the conventional algorithms without feedback in terms of security metrics;
- We point out that the legitimate receivers are less sensitive to self-interference as well as the jamming power from the eavesdropper in our approach.
- We emphasize that the proposed algorithms provides a higher robustness not only to the security and reliability factors but also to the power consumption by reducing the SNR at the legitimate receiver for decoding the message, which suits short-packet FD IoT transmissions and green communications.

The remainder of this paper is organized as follows. Section 2 briefly describes the general system model of the FD transceiver in the passive/active eavesdropper scenarios. The conventional schemes without feedback and security gaps are also mentioned in this section. Section 3 studies the application of the joint iterative blind channel estimation and decoding algorithm at the legitimate receiver in the case of passive eavesdroppers, with numerical results and comparisons with the conventional blind algorithm without feedback. Section 4 introduces the semi-blind algorithm for SI channel estimation and equalization processes in the legitimate receiver in case of active eavesdropper and simulation results. Finally, some highlights and conclusions will be discussed in Section 5. The notations in this paper are summarized in Table 1.

Table 1. List of Notations.

Notations	Meaning
K, N, R	Information length, code word length, and code rate
$\mathbf{x}_X$, $\mathbf{y}_X$	Transmitted signal vector and received signal vector at user X
$\mathbf{h}_{XY}$	Channel gain vector between X and Y
$\mathbf{h}_{XX}$	Self-interference channel gain vector at user X
$\mathbf{y}_{XX}$	Self-interference signal vector at user X
$\mathbf{y}_{XY}$	Receiving signal vector that transmitted from user X to user Y
$\hat{\mathbf{x}}$	Estimated signal vector
$\tilde{\mathbf{y}}$	Residual signal vector
$\mathbf{x}_{pilot}$	Pilot symbols vector
SNR_Y	Signal-to-noise ratio at user Y

Table 1. *Cont.*

Notations	Meaning
p_Y	Transmitting power of user Y
σ_Y^2	Noise power at user Y
$\mathbf{w}_Y$	Background noise at user Y
ρ_{XY}	Self-jamming power-to-noise ratio from user X to user Y
ρ_{YY}	SI power-to-noise ratio at user Y
λ	Forget factor of the RLS algorithm
i	Index of joint iterative iterations
j	Index of 5G QC-LDPC decoding iterations
k	Index of signal in the binary domain
n	Index of signal in the discrete time domain

2. Full-Duplex Transceiver with Passive/Active Eavesdropper Transmission System

2.1. General System Model

We consider a short-packet FD transmission wiretap channel between three users, such as user B (transmitter), user A (legitimate receiver), and user E (eavesdropper), as shown in Figure 1, where the transmitter is equipped with only one antenna for transmission while the receiver and the eavesdropper are attached with one transmitter and one receiver antenna each to simultaneously receive the intended information message and transmit self-jamming or jamming signals. The 5G QC-LDPC codes, which are considered fundamental codes for short-packet uplink and downlink transmissions [29–31], are used in all transceivers.

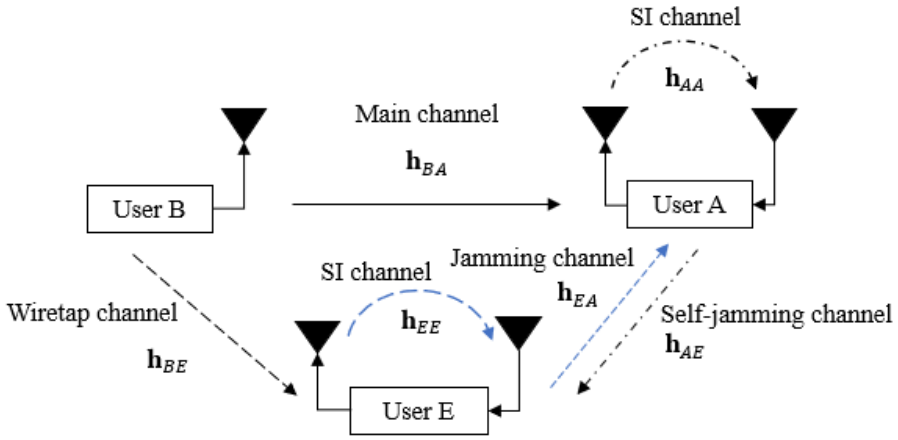

Figure 1. General system model.

At the transmitter, the (N, K) 5G QC-LDPC encoding process between the exponent parity check matrix $\mathbf{H}$ and the information bit sequence is based on the Gauss–Jordan elimination algorithm [32], where K and N denote the lengths of the information message and the code word message, respectively. Let us denote the channel gain between two users and the SI channel gain of itself as $\mathbf{h}_{XY}$ and $\mathbf{h}_{YY}$, respectively, in which $X \in \{A, B, E\}$ and $Y \in \{A, E\}$, where A, B, E represent user A, user B, and user E, respectively. In this paper, the SI channel is modeled as quasi-static Rayleigh fading in the digital domain due to the assumption that the Line-of-Sight (LoS) component is fully suppressed by antenna and analog cancellation techniques, whereas the residual SI is the Non-Line-of-Sight (NLoS) component [8,33]. Note that $\mathbf{h}_{XY}$ and $\mathbf{h}_{YY}$ are i.i.d complex Gaussian random variables with $\mathcal{CN}(0, 1)$ [34,35]. Moreover, the transmitted power of each user is denoted as p_X, where $X \in \{A, B, E\}$, and we further denote w_Y as the complex background noise at user Y with $\mathcal{CN}(0, \sigma_Y^2)$, where $Y \in \{A, E\}$. Based on the background noise as reference and without loss in generality, we further denote $\rho_{XY} = p_X/\sigma_Y^2$ and $\rho_{YY} = p_Y/\sigma_Y^2$ as the power-to-noise ratio provided by the self-jamming or jamming channel from user X to user Y and the SI channel at user Y, respectively. We also denote $SNR_A = p_B/\sigma_A^2$ and $SNR_E = p_B/\sigma_E^2$ as

the SNR at user A and user E, where σ_A^2 and σ_E^2 are the noise powers at user A and user E, respectively.

2.2. Conventional Schemes without Feedback

The conventional blind scheme without feedback and the semi-blind scheme without feedback have been studied in [27,28], respectively, and are presented in Figure 2. At the receiver side, the received signal $\mathbf{y}_A$ will pass through a Digital Self-Interference Cancellation (DSIC) process based on an adaptive filter with the Recursive Least Square (RLS) algorithm [36] to firstly estimate the SI channel and then reconstruct and cancel the SI component. Then, the residual signal will go to an equalizer to firstly estimate the intended channel and then obtain the equalized signal. In the semi-blind scheme without feedback, it is noted that the pilot symbols are attached to the information sequence at the transmitter side, and they are also used for the DSIC and equalizer processes. Then, they will be removed from the equalized signal, and this signal continuously goes to the demodulator to obtain the Log Likelihood Ratio (LLR) belief sequence. Finally, the Sum Product Algorithm (SPA) decoding algorithm [37,38] with an efficient message-passing schedule will be implemented in the 5G LDPC decoding process at user A and user E to reconstruct the binary input signal $\hat{\mathbf{x}}_{SoI}$ of user B. The principle of SPA involves the message repetitively passing from the check nodes to the symbol nodes for guessing the transmitted bits from each other at each iteration j until it reaches the maximum number of iterations, j_{max}. For the rest of this paper, this DSIC process and decoding scheme are called blind scheme without feedback or semi-blind scheme without feedback, respectively.

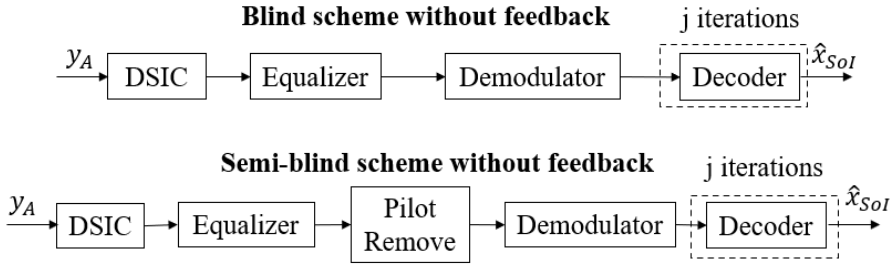

Figure 2. Conventional schemes without feedback.

In this paper, we assume the following hypotheses:

- In case of a passive eavesdropper, only blind channel estimation is used, where there is no knowledge about the channel state information at all communication users;
- In case of an active eavesdropper, both blind and semi-blind channel estimations, where all transceivers share a few pilot symbols, are mainly implemented;
- User E knows the parity check matrix **H** of user B and performs the SPA decoding mechanism; user E also uses an RLS algorithm in the DSIC process of user A in case of an active eavesdropper;
- Both user A and user E have equal computation capabilities, and the location of user E is close enough to user A to broadcast its jamming signal as well as to be attacked by the self-jamming signal from user A;
- The channel gains at the receiver and the eavesdropper are constant within a code word and change from one to another in fading channels;
- The impact of hardware impairments on the SI cancellation is not considered (which is outside the scope of this study but essential in practice). Moreover, the problem of the synchronization process between the transceivers is also not taken into account. Last but not least, the bit resolution of DAC/ADC is chosen to be high enough to bypass the effect of the quantization noise, i.e., larger than 6 bits for both DAC/ADC process. Alternatively, the oversampling should be applied in the ADC process if the green communication system and IoT applications are considered with low-bit ADC [39].

2.3. Security Gap

In the practical context of the wiretap channel when the short-packet is used for transmission, the typical BER performance criteria are usually used to ensure two aspects of performance such as reliability and secrecy conditions [23]. Let us denote BER_A and BER_E as the average BER of user A and user E, respectively. While $BER_{A,max}$ and $BER_{E,min}$ are the maximum BER that user A can achieve and the minimum BER that user E can obtain, respectively. The reliability condition holds when $BER_A \leq BER_{A,max}$, which means that the BER of user A should be maintained at a low value to enhance the reliability condition. Meanwhile, the security condition is achieved when $BER_E \geq BER_{E,min}$, which means that the BER of user E should remain at a sufficiently high value to guarantee the security.

According to [7,17], the security gap, which is the minimum difference of SNRs (in dB) required to guarantee the legitimate receiver security over the eavesdropper, is calculated as:

$$S_g(dB) = SNR_{A,min} - SNR_{E,max} \quad (1)$$

where $SNR_{A,min}$ is the minimum SNR corresponding to $BER_{A,max}$, where user A has to operate to make sure the BER is below some reliability thresholds, i.e., $BER_{A,max} = 10^{-5}$, which is a sufficient level for practical applications [23]. Similarly, $SNR_{E,max}$ is the maximum SNR corresponding to $BER_{E,min}$ in which the BER of user E can approximately reach a threshold, that is, $BER_{E,min} = 0.5$, which is called the security threshold because user E cannot exactly decode the information message in this region [7].

The graphical presentation of security gap is shown in Figure 3. In fact, the size of the security gap S_g indicates the minimum cost of the difference in SNRs between user A and user E that maintains the possibility of secure communication, the higher values of S_g will lead to a higher transmission cost. Therefore, the objective of this paper is to reduce the size of the security gap S_g as much as possible. In particular, the SNR of user A, $SNR_A = p_B/\sigma_A^2$ (dB), on the main channel must be small enough to ensure that user A can correctly decode the information message from user B assuming the lowest possible power. In contrast, the SNR of user E, $SNR_E = p_B/\sigma_E^2$ (dB), on the wiretap channel must be as large as possible to guarantee that the self-jamming broadcasting from user A still affects the decoding process of user E.

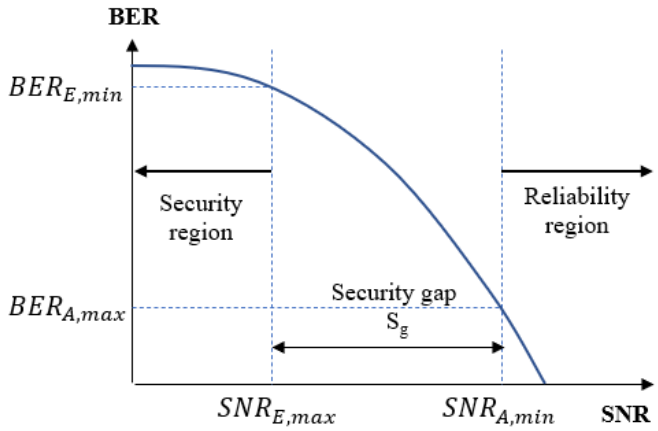

Figure 3. Security gap.

Next, we will consider the first case with passive eavesdropper and the presence of a blind feedback algorithm.

3. Case I: Passive Eavesdropper

3.1. Passive Eavesdropper System Model

The wiretap channel system models with the use of FD self-jamming and a passive eavesdropper are shown in Figures 4 and 5, where user A is operated in FD transmission mode to simultaneously receive the intended information message from user B and transmit

the self-jamming signal to destroy the decoding ability of user E, while user E just tries to listen and decode the message from user B. The transmission strategy of the proposed scheme is as follows. User B wants to send his encoded message $\mathbf{x}_B$ to the legitimate receiver user A through the main channel $\mathbf{h}_{BA}$, while passive eavesdropper user E tries to listen and decode user B's message through the wiretap channel $\mathbf{h}_{BE}$. The received signals in the digital domain at user A and user E are given by the following:

$$\begin{aligned} y_A[n] &= y_{BA}[n] + y_{AA}[n] + w_A[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BA})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AA})[n] + w_A[n]; \end{aligned} \tag{2}$$

$$\begin{aligned} y_E[n] &= y_{BE}[n] + y_{AE}[n] + w_E[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BE})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AE})[n] + w_E[n]; \end{aligned} \tag{3}$$

where $\mathbf{w}_A$ and $\mathbf{w}_E$ are the complex Gaussian background noise of the receiver channel of user A and user E, with $\mathcal{CN}(0, \sigma_A^2)$ and $\mathcal{CN}(0, \sigma_E^2)$, respectively, and $(*)$ is the convolution operation.

The legitimate receiver user A obtains the signal $\mathbf{y}_A$ and performs two possible decoding strategies to eliminate the SI component and obtain the estimation of the intended signal $\hat{\mathbf{x}}_{SoI}$. First, it may use a classical blind scheme without feedback where the DSIC and decoding processes are independent, as presented in Figure 4. Second, it can use a more efficient scheme based on joint iterative blind channel estimation and decoding through feedback, as shown in Figure 5, which we call the blind feedback scheme. At the same time, user E also tries to listen to the transmission over the wiretap channel and only performs the equalization process and the classical SPA decoding process to obtain the original signal $\mathbf{x}_B$.

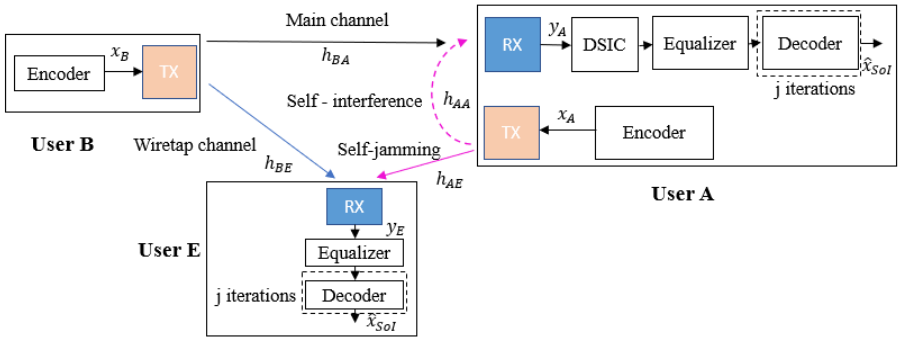

Figure 4. Blind scheme without feedback at user A in case of a passive eavesdropper.

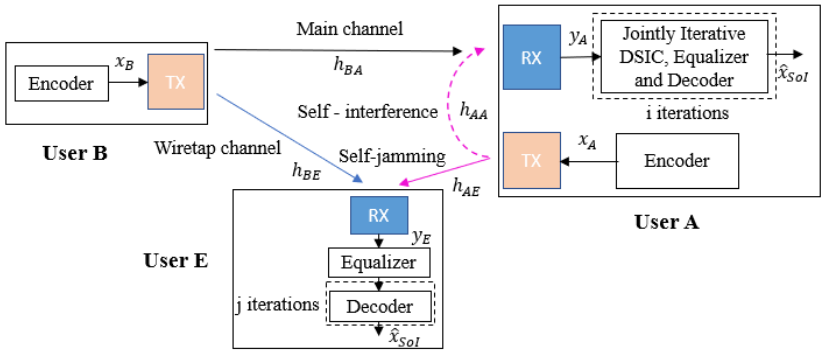

Figure 5. Blind feedback scheme at user A in case of a passive eavesdropper.

Next, we will briefly describe the joint iterative blind channel estimation and decoding processes, which were studied in [27].

3.2. Blind Feedback Scheme

The conventional scheme without feedback with the RLS algorithm and the SPA decoding algorithm is an optimal estimation [40] and decoding algorithm, but with a high computational complexity [41], because it requires an updated LLR sequence and decoding for each iteration. It is not suitable for short-packet FD transmission due to the high estimation error of the SI channel [10] and power consumption in IoT applications and green communications due to the high latency of the 5G QC-LDPC decoder [42,43]. To overcome these drawbacks, the authors in [27] proposed a joint iterative algorithm for blind channel estimation and decoding, named the blind feedback scheme. The fundamental process of the blind feedback scheme is that the SI cancellation, intended channel estimation, and decoding processes of the desired signal can benefit from each other through the temporary decoding and feedback loop. Hence, the proposed scheme will only consider one iteration of SPA decoding ($j_{max} = 1$) for each joint iteration i, called temporary decoding, and it will then perform the re-encoding, re-interleaving, and re-modulating to form a feedback loop of the intended signal in order to improve the SI cancellation process in the next joint iterations. This is continue until the system reaches the maximum number of joint iterations i_{max}. The proposed algorithm can not only decrease the processing time and computational complexity, but it can also improve the overall performance, which is illustrated in [27]. The flow chart of the proposed blind algorithm is described in Figure 6, which has four main steps and can be summarized as follows:

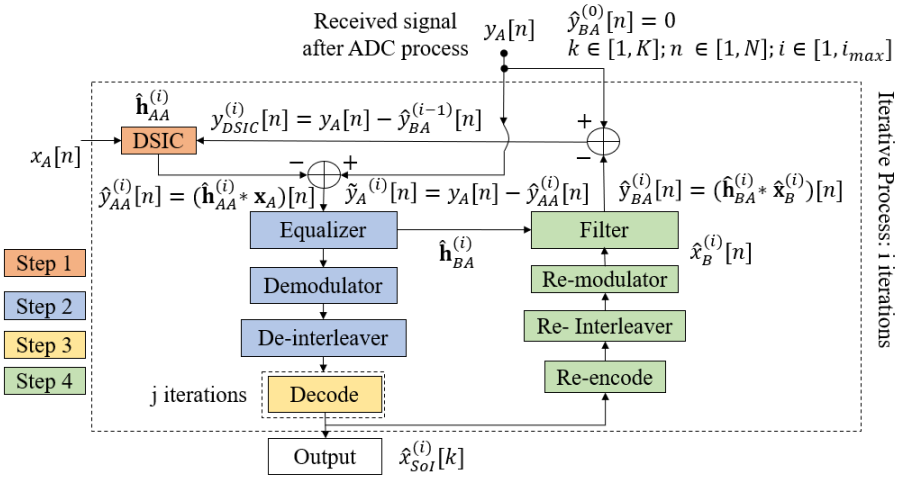

Figure 6. Joint iterative blind algorithm flowchart.

Step 1: The mixed signal $\mathbf{y_A}$ at the receiver side is firstly used to estimate the SI channel $\hat{\mathbf{h}}_{AA}$ and cancel the SI component based on the reference transmitted signal $\mathbf{x}_A$;

Step 2: The residual signal $\tilde{\mathbf{y}}_A$ received from Step 1 is continuously used to estimate the intended channel $\hat{\mathbf{h}}_{BA}$ and obtain the equalized signal by an equalizer. Here, the *blind* channel estimation method is applied with no knowledge of the transmitting signal from the transmitter. Then, this equalized signal goes to the demodulator and de-interleaver to obtain the LLR belief information sequence.

Step 3: In this step, the estimation of the binary intended signal is achieved by using 5G QC-LDPC decoding with the SPA algorithm.

Step 4: When the maximum number of joint iterations (i_{max}) is not reached, the temporary message obtained from the previous Step is re-encoded, re-interleaved, and re-modulated. Then, this signal is filtered with the estimation version of the intended channel $\hat{\mathbf{h}}_{BA}$ achieved in Step 2 to form the intended feedback signal $\hat{\mathbf{y}}_{BA}$. Consequently, the intended feedback signal is used to temporarily remove the intended component from the received signal in order to optimize the SI channel estimation process for the next joint iteration.

3.3. Simulation Specifications

To evaluate the secrecy performance of our proposed schemes, MSE, BER, and security gap S_g will be computed by using Monte Carlo simulations in MATLAB. For the rest of this paper, the MSE of the channel estimation in the intended receiver user A and the eavesdropper user E are given by [44]:

$$\text{MSE}_{XX} = | \mathbf{h}_{XX} - \hat{\mathbf{h}}_{XX} |^2, \tag{4}$$

and

$$\text{MSE}_{XY} = | \mathbf{h}_{XY} - \hat{\mathbf{h}}_{XY} |^2, \tag{5}$$

respectively.

For 5G QC-LDPC codes, the base graph matrix **BG2** [30] is implemented for all simulations. The SI channel and self-jamming or jamming channel are fixed with three taps based on Rayleigh distribution with $\mathcal{CN}(0, 1)$. The intended main channel and wiretap are fixed with four taps and the power of each tap is according to the ITU–R channel model [45]. These channels are generated independently in each transmission frame. The simulation parameters of this paper are summarized in Table 2.

Table 2. Simulation Specifications.

Parameter	Value
Number of transmission frames	10^6
Number of information bits and code word bits (K, N)	(128, 256)
Code rate R	1/2
Modulation scheme	QPSK
SI channel taps h_{AA}, h_{EE}	3
Self-jamming channel taps h_{AE}	3
Jamming channel taps h_{EA}	3
Main channel taps h_{BA}	4
Wiretap channel taps h_{BE}	4
Number of pilot symbols in semi-blind scheme	4
Index of iterations (i_{max}, j_{max}) for scheme with feedback	(4,1)
Index of iteration j_{max} for scheme without feedback	20

3.4. MSE Performances

3.4.1. MSE at the Legitimate Receiver User A

First, the MSEs of SI channel and main channel at user A are computed for different values of self-interference-to-noise ratio ρ_{AA}. For instance, Figure 7a,b show the MSEs of the SI channel versus SNR_A of the legitimate receiver user A in the blind without feedback and blind feedback schemes, respectively. Similarly, Figure 8a,b illustrate the MSEs of the main channel versus the SNR_A at user A in the blind without feedback and blind feedback schemes, respectively. It can be seen that MSEs increase significantly as the self-interference-to-noise ratio of user A (ρ_{AA}) increases, and the blind feedback scheme outperforms the scheme without feedback. It can also be observed that the increase in the self-interference-to-noise ratio of user A has less effect on the blind feedback scheme than the scheme without feedback. For example, maintaining MSE_{AA} at 10^{-3}, when ρ_{AA} increases from 0 to 30 dB, requires an increase of SNR_A only around 2.5 to 3 dB in the blind feedback scheme. However, it requires an increase of roughly 10 dB in the scheme without feedback. Therefore, the use of the blind feedback scheme can improve the channel estimation processes at user A significantly.

3.4.2. MSE at the Eavesdropper User E

Next, we also evaluate the MSE of the wiretap channel h_{BE} versus the signal-to-noise ratio at the eavesdropper user E (SNR_E) for various values of the self-jamming-to-noise ratio from user A, ρ_{AE}. Based on Figure 9, it can be clearly observed that user E cannot

estimate the wiretap channel well, especially in the case of a high value of the self-jamming-to-noise ratio of user A, i.e., when ρ_{AE} increases higher than 10 dB. This behavior is due to the lack of knowledge of the reference signal of the transmitter as well as the power of the self-jamming signal from user A, which is much greater than the power of the intended signal. So, we can conclude that user E cannot accurately estimate the wiretap channel in passive mode.

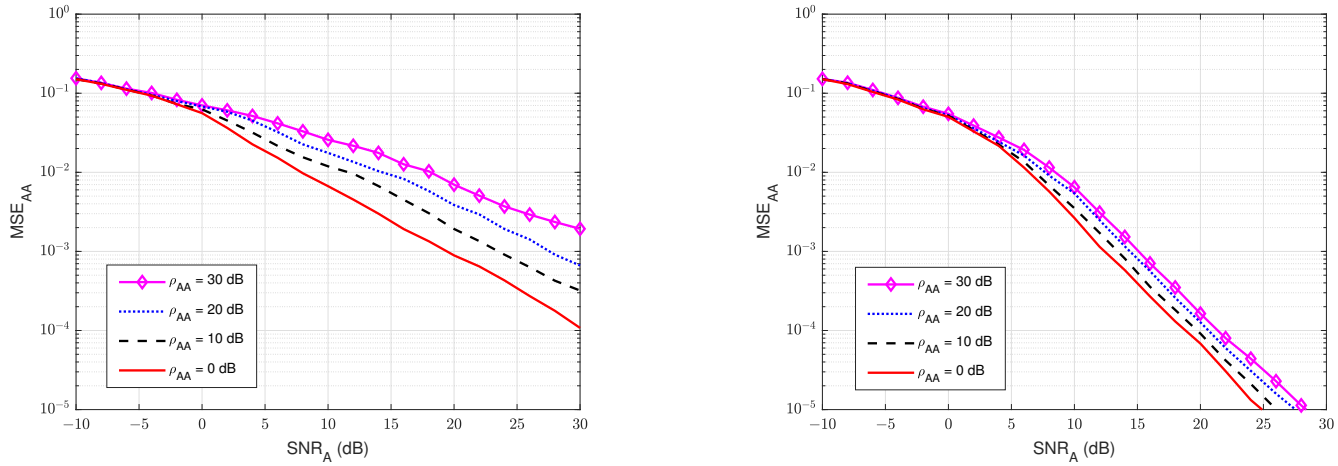

Figure 7. MSE_{AA} versus SNR_A in case of passive eavesdropper: (**a**) Blind without feedback; (**b**) Blind feedback.

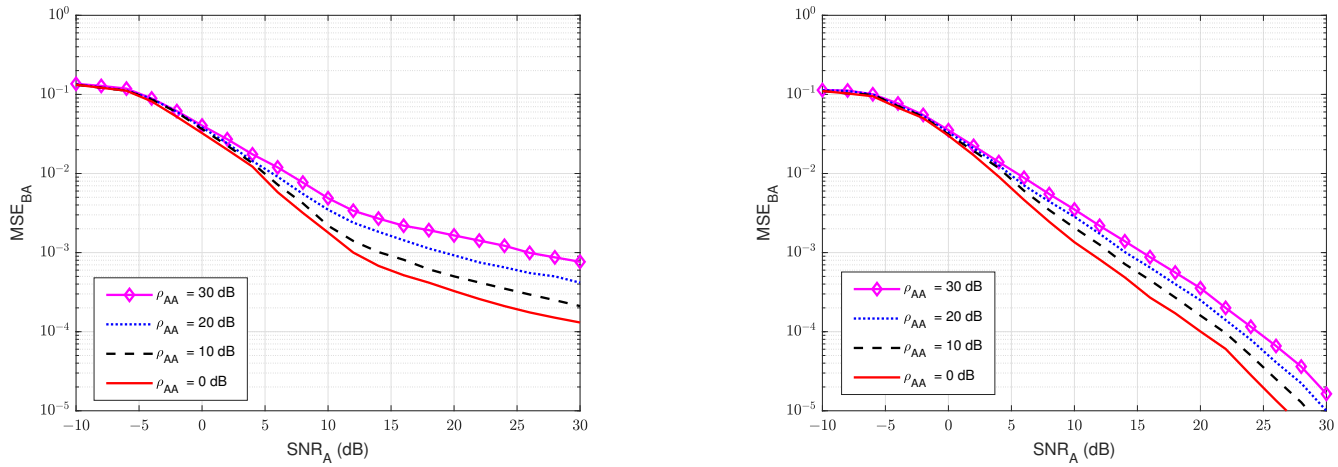

Figure 8. MSE_{BA} versus SNR_A in case of passive eavesdropper: (**a**) Blind without feedback; (**b**) Blind feedback.

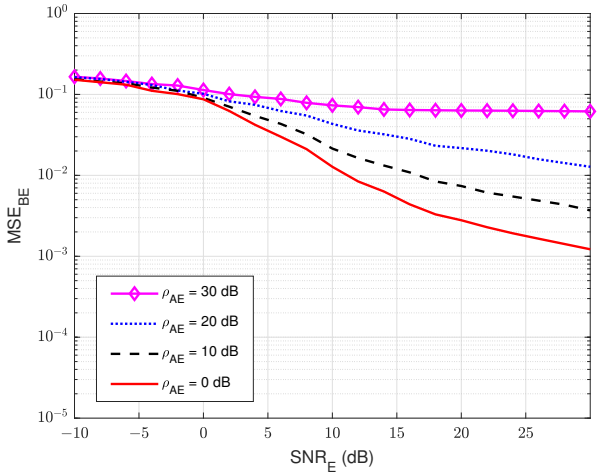

Figure 9. MSE_{BE} versus SNR_E in case of passive eavesdropper.

3.5. BER Performances

3.5.1. BER at the Legitimate Receiver User A

The BER performances versus the SNR_A of user A, for different values of the self-interference-to-noise ratio of user A (ρ_{AA}), are presented in Figure 10a,b for both the without feedback and blind feedback schemes, respectively. We can observe that the self-interference-to-noise ratio also significantly impacts the BER's performance, i.e., the BER increases as the ρ_{AA} increases, and the increase in the BER is bigger for larger SNR_A. It also shows an interesting result that when maintaining $BER_A = 10^{-5}$ and increasing the self-interference-to-noise ratio ρ_{AA} from 0 to 30 dB, the blind feedback scheme needs about 2 to 3 dB in SNR_A to obtain that BER, while the scheme without feedback requires more than 5 dB in SNR_A to achieve comparable results. Therefore, in the passive eavesdropper case, the increase in the self-interference-to-noise ratio has less effect on the blind feedback scheme in the BER performance at the legitimate receiver user A.

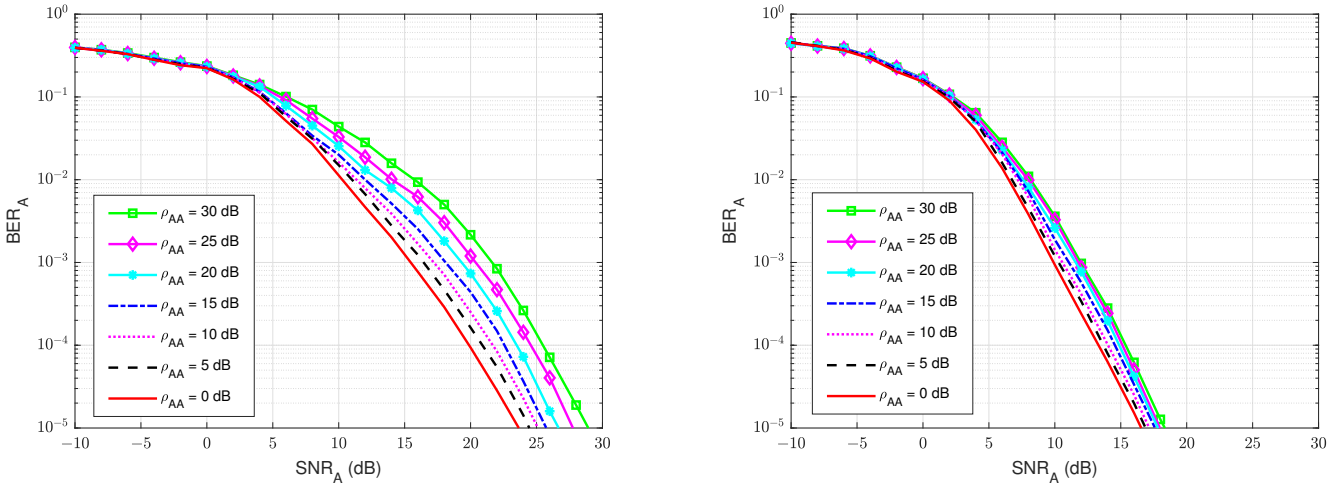

Figure 10. BER_A versus SNR_A in case of a passive eavesdropper: (**a**) Blind without feedback; (**b**) Blind feedback.

3.5.2. BER at the Eavesdropper User E

At the eavesdropper user E, the BER's performances versus SNR_E are also calculated to evaluate how much user E can decode the message sent from user B. For the rest of this paper, we have decided to keep the same BER ranges (10^0 to 10^{-5}) without focusing on

the useful ranges in order to allow for a visual comparison of the different schemes and especially the performance differences between legitimate user A and eavesdropper E. As shown in Figure 11, it is shown that the presence of a self-jamming signal from user A has a significant impact on the estimation and decoding processes of user E, regardless of the knowledge of the channel coding used for decoding. The best BER that user E can obtain is about $BER_E = 10^{-3}$ at $SNR_E = 30$ dB. Furthermore, when the self-jamming-to-noise ratio ρ_{AE} is greater than 15 dB, user E almost cannot decode the intended message from user B. It can be explained that user A can estimate the SI channel well and cancel the SI component because user A has its generated self-jamming signal $\mathbf{x}_A$ as reference. Moreover, applying the blind feedback scheme also improves the channel estimation and decoding processes, although user A also has no knowledge about the reference signal from user B. In contrast, user E has no knowledge about the reference signal of user B and the self-jamming signal of user A, and there is no interference cancellation mechanism applied; instead, it uses only the SPA decoding scheme to decode the intended message.

Therefore, user E cannot operate efficiently in the estimation and decoding processes. In summary, by applying the joint iterative estimation and decoding to the legitimate receiver, user A can significantly improve the secrecy reliability factor in FD wiretap transmission.

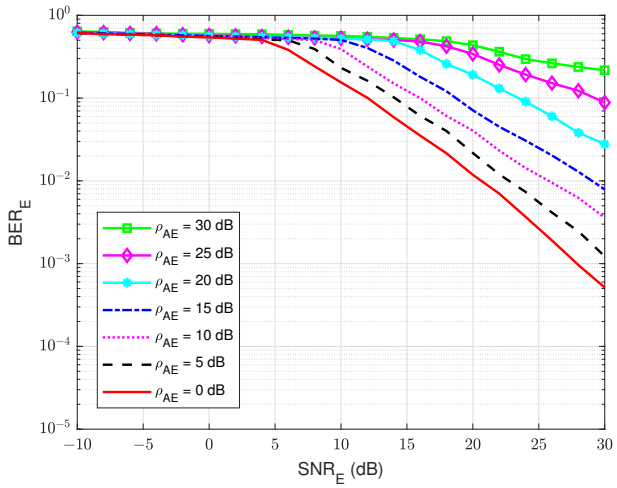

Figure 11. BER_E versus the SNR_E in case of a passive eavesdropper.

3.6. Security Gap Performance

On the one hand, there is an assumption concerning the relative positions of the various transmitters/receivers. In particular, for the case of user A and user E, it seems coherent and acceptable to consider that the powers of the background noises σ_A^2 and σ_E^2 are identical. On the other hand, under the assumption of channels without loss (unified mean deviations on all the paths) for $\mathbf{h}_{AA}$ and $\mathbf{h}_{AE}$, it is possible to simplify the notations and to denote in general the self-jamming power-to-noise ratio as ρ_{SJ} for both self-interference (ρ_{AA}) and self-jamming (ρ_{AE}) channels. Since, in these conditions, we have $\rho_{SJ} = \rho_{AA} = \rho_{AE}$. The security gap S_g is clearly related to the error rate achieved on the receiver side of user A and user E. In order to adapt to the practical applications, we set up $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$ for the maximum and minimum average errors that user A and user E can reach, respectively. Based on the results in Figures 10 and 11, the minimum SNR at the legitimate user A, the $SNR_{A,min}$ and the maximum SNR at the eavesdropper user E, and $SNR_{E,max}$ to obtain $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$, respectively, can be pointed out. Then, these values are recorded corresponding to different levels of the general self-jamming power-to-noise ratio ρ_{SJ}. Finally, the security gap S_g is calculated and summarized in Table 3.

Table 3. Security gap S_g in case of passive eavesdropper.

ρ_{SJ}	$SNR_{E,max}$	Without Feedback at User A		Blind Feedback at User A	
		$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	4.1	23.8	19.7	16.5	12.4
5	5.8	24.5	18.7	16.8	10.8
10	8.1	25.1	17	17.2	9.1
15	10.3	25.6	15.3	17.6	7.3
20	12.4	26.7	14.3	17.9	5.5
25	14.3	27.5	13.2	18.1	3.8
30	16.6	29	12.4	18.3	1.7

Figure 12 shows the security gap versus the various values of the self-jamming power-to-noise ratio (ρ_{SJ}) in the case of blind without feedback and blind feedback at user A. The result shows that the increase in the self-jamming power-to-noise ratio ρ_{SJ} leads to a decrease in the security gap S_g. For example, the security gap S_g can be dramatically reduced from 7 to 10 dB when the blind feedback scheme is applied. Therefore, it obtains an important goal of the PLS, which is to maintain the security gap as small as possible. In summary, the use of joint iterative blind estimation and decoding at the legitimate receiver user A significantly reduces the security gap S_g in FD wiretap transmission. Furthermore, when using the blind feedback scheme, the SNR_A of user A is reduced when performing channel estimation or decoding messages, compared with the blind scheme without feedback, which emphasizes that the system not only maintains security but also enhances power consumption by reducing the transmission power.

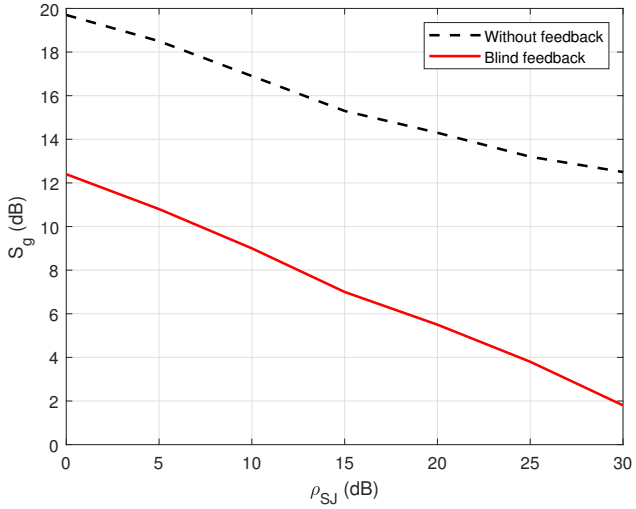

Figure 12. S_g versus ρ_{SJ} in the case of a passive eavesdropper.

In the next section, we will consider the second case, where user E can also send their jamming message to destroy the reception and decoding processes of user A, which we refer to as an active eavesdropper.

4. Case II: Active Eavesdropper

4.1. Active Eavesdropper System Model

The wiretap channel system model with the use of FD self-jamming and an active eavesdropper is shown in Figure 13.

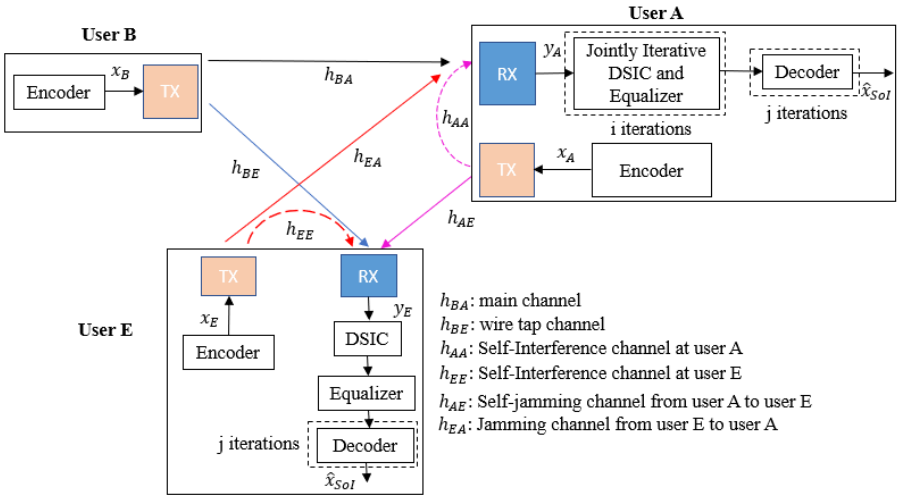

Figure 13. Wiretap Full-Duplex transmission with self-jamming in case of an active eavesdropper.

In this case, both user A and user E operate in the FD transmission mode to simultaneously receive the intended information message from user B and transmit the self-jamming or jamming signal to other users. In particular, user B wants to send his encoded message $\mathbf{x}_B$ to the legitimate receiver user A by the main channel, while the eavesdropper user E not only tries to listen to and decode user B's message by the wiretap channel but also simultaneously broadcasts their jamming signal to user A. Consequently, the received signals in the digital domain at user A and user E are given by:

$$\begin{aligned} y_A[n] &= y_{BA}[n] + y_{AA}[n] + y_{EA}[n] + w_A[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BA})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AA})[n] + (\sqrt{p_E}\mathbf{x}_E * \mathbf{h}_{EA})[n] + w_A[n]; \end{aligned} \tag{6}$$

and

$$\begin{aligned} y_E[n] &= y_{BE}[n] + y_{EE}[n] + y_{AE}[n] + w_E[n] \\ &= (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BE})[n] + (\sqrt{p_E}\mathbf{x}_E * \mathbf{h}_{EE})[n] + (\sqrt{p_A}\mathbf{x}_A * \mathbf{h}_{AE})[n] + w_E[n], \end{aligned} \tag{7}$$

respectively.

It can be seen that the signal-to-noise ratio at user A is reduced due to the impact of the jamming signal from user E, which leads to an increase in noise at the receiver of user A. Therefore, in addition to the proposed blind feedback scheme, the joint iterative SI channel estimation and equalization processes with the semi-blind algorithm, which have been studied in [28], should be used at user A in order to eliminate the SI component and estimate the intended signal $\hat{\mathbf{x}}_{SoI}$ because the proposed semi-blind algorithm shows its robustness in the low region of the SNR, compared to the blind algorithm. Indeed, the principle of this algorithm is to use at least four pilot symbols between the transceivers (which is a sufficient number of pilot symbols, as shown in [28]) to perform the channel estimation processes as well as the feedback loop. At the receiver side of user E, in order to distinguish the decoding behavior of the legitimate receiver (user A) and the eavesdropper (user E) and to also show the robustness of two proposed feedback schemes over the conventional schemes without feedback, user E will only use the blind scheme without feedback and the semi-blind scheme without feedback. In case of the semi-blind scheme without feedback, it is also assumed that four pilot symbols are observed by user E.

Next, we will briefly mention and summarize the joint iterative semi-blind channel estimation and equalization processes and name it the semi-blind feedback scheme.

4.2. Semi-Blind Feedback Scheme

In the case of a passive eavesdropper, it is shown that the performance is better when using the blind feedback scheme. However, in the case of an active eavesdropper, the

presence of a jamming signal from user E leads to significant destruction of the reception behavior of user A. Therefore, small sharing of known symbols or pilot symbols between user B and user A should be established to guarantee the reliability and security of transmissions.

The processing flowchart of the semi-blind algorithm is presented in Figure 14. In general, it is nearly similar to the joint iterative blind feedback algorithm in Section 3.2, except that the temporary decoding and encoding processes are skipped. Instead, the known pilot symbols, which are added to the information sequence on the transmitter side, are used to form the intended signal and the feedback loop. In particular, for $i = 1$ (first iteration of the iterative algorithm), a first SI cancellation and intended channel estimation are performed for all symbols in order to overcome a larger number of errors and achieve a sufficient level of convergence. When $i \in [2, i_{max}]$, the known pilot symbols $\mathbf{x}_{pilot} = 4$ (symbols) are used to form the feedback loop. When it reaches the maximum number of iterations ($i = i_{max}$), the algorithm is stopped, the SI component can be canceled, and the equalized signal can be fully achieved by the estimation versions of the SI channel and the intended channel. After that, the known pilot symbols are suppressed, and the equalized signal will undergo the demodulation, de-interleaver, and decoding processes to obtain the final decoded message. Here, it is noticed that the SPA decoding algorithm also performs only one iteration ($j_{max} = 1$) in the decoding step when the system achieves the best channel estimation ($i = i_{max}$).

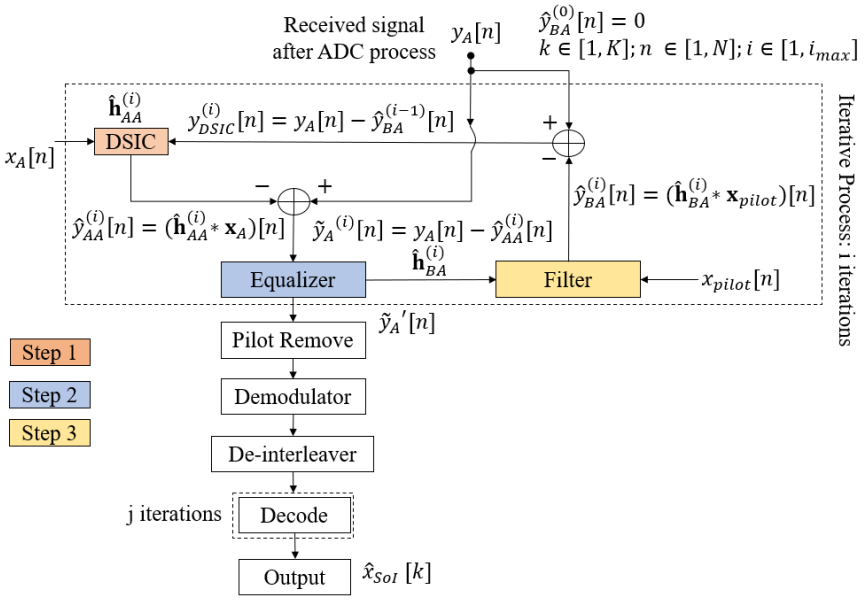

Figure 14. Joint iterative semi-blind algorithm flow chart.

The proposed semi-blind algorithm can be summarized in three steps:

Step 1: The received signal $\mathbf{y}_A$ is used to estimate the SI channel $\hat{\mathbf{h}}_{AA}$ and to cancel the SI component based on the reference transmitted signal $\mathbf{x}_A$;

Step 2: The residual signal $\tilde{\mathbf{y}}_A$ after step 1 will go to an equalizer to estimate the intended channel $\hat{\mathbf{h}}_{BA}$;

Step 3: Using pilot symbols $\mathbf{x}_{pilot}$ that are added to the information sequence on the transmitting side, a feedback loop is created with the estimation version of the intended channel $\hat{\mathbf{h}}_{BA}$ to form $\hat{\mathbf{y}}_{BA}$. This signal is passed to the subtraction process from the received signal and performs the next joint iterations.

Next, we will introduce the performance in terms of the MSE, BER, and security gap S_g in the case of an active eavesdropper.

4.3. Mean Square Error (MSE) Performance

4.3.1. MSE at the Legitimate Receiver User A

First of all, Figures 15 and 16 illustrate the MSEs of the SI channel and the main channel at user A for the blind feedback scheme and the semi-blind feedback scheme, respectively, versus SNR_A for different power values of the jamming-to-noise ratio ρ_{EA} broadcast from user E, while the self-interference-to-noise ratio at user A, ρ_{AA}, is fixed at 30 dB. It can be seen that the presence of the jamming signal from user E significantly impacts the SI channel estimation at user A, where it increases the noise level at the receiver side at user A, compared with the passive case. Indeed, the gain between each MSE's curve is bigger than in the passive case, whatever the algorithm used, which means that the system requires higher SNR_A to estimate the channel. Furthermore, the semi-blind feedback scheme outperforms the blind feedback scheme, i.e, it converges faster to the error floor and achieves better results than the blind feedback scheme because the traces of four pilot symbols is used. Therefore, using the semi-blind algorithm can improve the channel estimation processes and reduce the impact of the jamming signal from the eavesdropper.

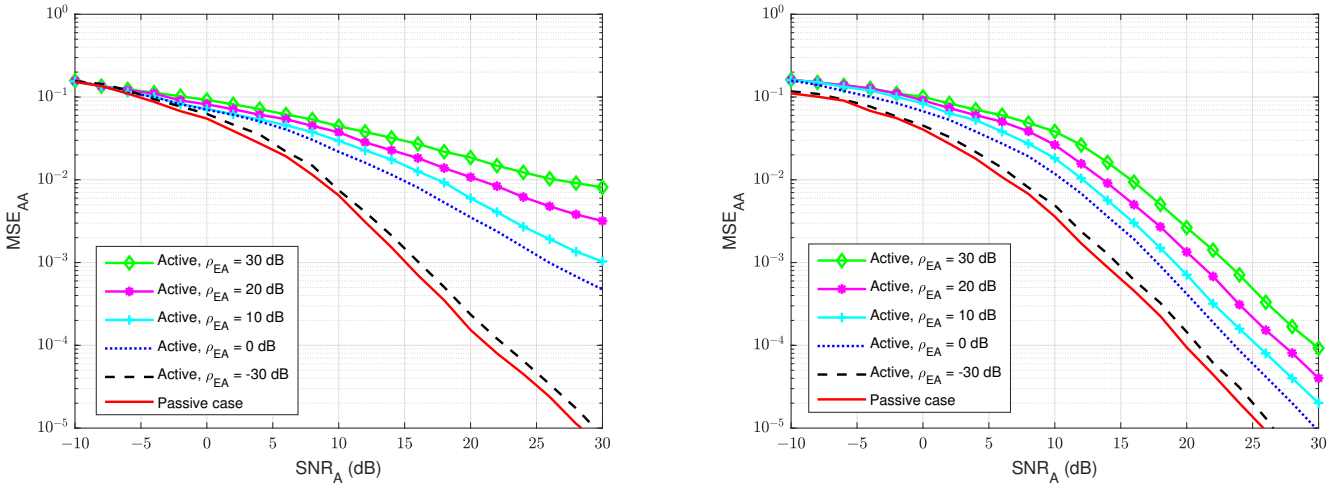

Figure 15. MSE_{AA} versus SNR_A, $\rho_{AA} = 30$ dB in case of active eavesdropper: (**a**) Blind feedback; (**b**) Semi-blind feedback.

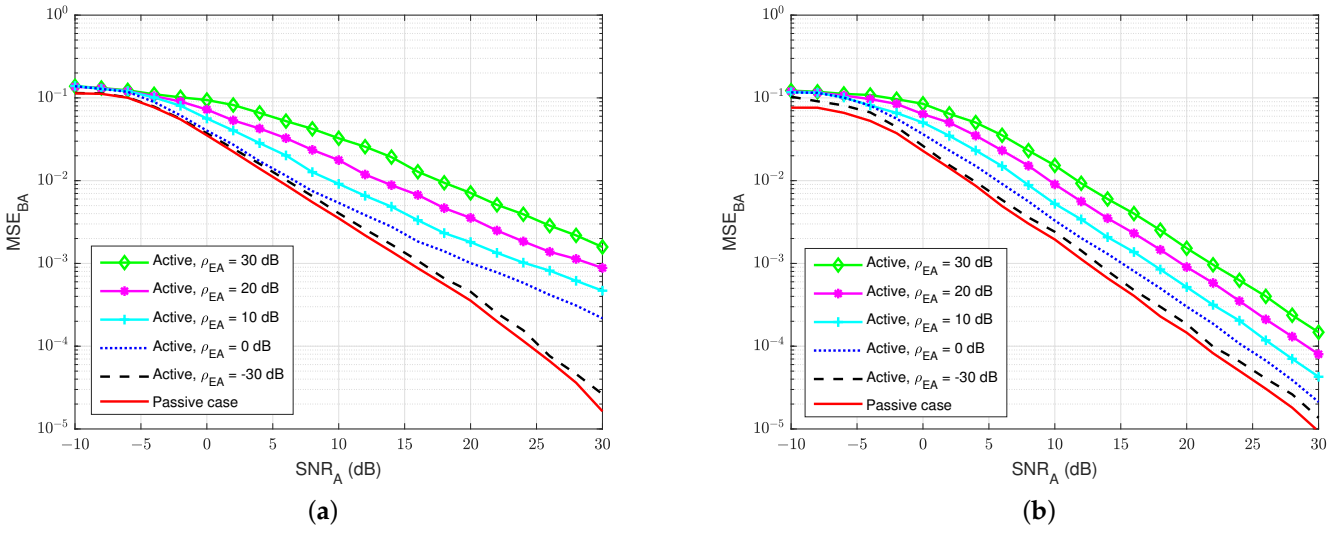

Figure 16. MSE_{BA} versus SNR_A, $\rho_{AA} = 30$ dB in case of an active eavesdropper: (**a**) Blind feedback; (**b**) Semi-blind feedback.

4.3.2. MSE at the Eavesdropper User E

Next, Figures 17 and 18 show the MSEs of the SI channel $\mathbf{h}_{EE}$ and the wiretap channel $\mathbf{h}_{BE}$ versus SNR_E at the eavesdropper user E for various values of the self-jamming-to-noise ratio from user A, ρ_{AE}. The self-interference-to-noise ratio at user E, ρ_{EE}, is fixed at 30 dB. It can be clearly observed that user E cannot estimate the wiretap channel and the SI channel well, especially if there is a high self-jamming-to-noise ratio from user A, i.e., ρ_{AE} increases higher than 20 dB. So, the self-jamming signal provided by user A significantly influences the receiver side of user E, where user E cannot perform the wiretap channel estimation well in active mode, although user E also knows the pilot symbols. Moreover, the power of the combination of the self-jamming of user A and the SI component at user E is also higher than the power level of the intended message from user B. Therefore, the blind scheme without feedback and the semi-blind scheme without feedback, which are applied to user E, cannot estimate the channels well.

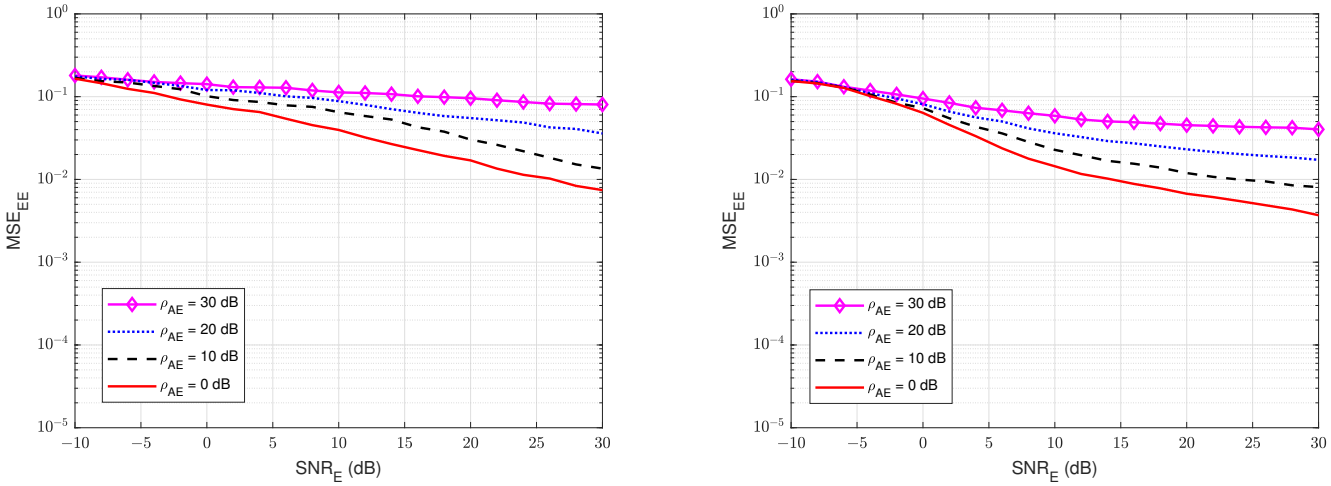

Figure 17. MSE_{EE} versus SNR_E, ρ_{EE} = 30 dB in case of an active eavesdropper. (**a**) Blind without feedback; (**b**) Semi-blind without feedback.

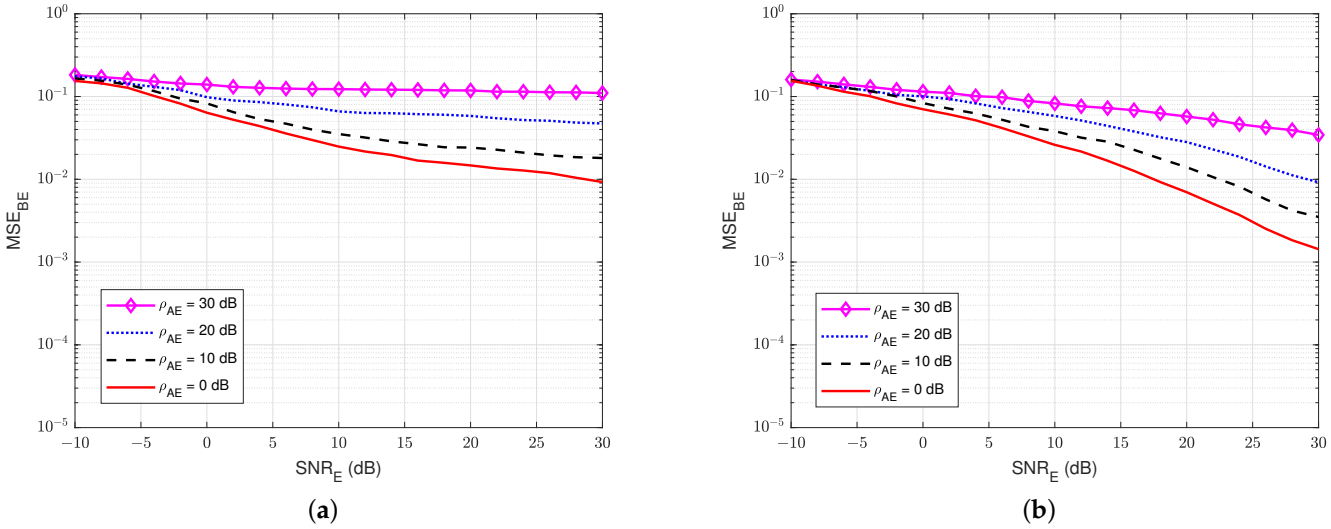

Figure 18. MSE_{BE} versus SNR_E, ρ_{EE} = 30 dB in case of an active eavesdropper: (**a**) Blind without feedback; (**b**) Semi-blind without feedback.

4.4. Bit-Error-Rate (BER) Performance

4.4.1. BER at the Legitimate Receiver User A

The BER performances versus SNR_A at user A for different values of the jamming-to-noise ratio from user E (ρ_{EA}) are illustrated in Figure 19a,b for both the blind feedback scheme and the semi-blind scheme at user A, respectively. The self-interference-to-noise ratio at user A (ρ_{AA}) is set at 30 dB. We can observe that the BER increases as the jamming-to-noise ratio of user E (ρ_{EA}) increases, and the increase in the BER is bigger for larger SNR_A values compared with the passive case. We can also remark that the semi-blind scheme is less sensitive to the jamming from user E than the blind feedback scheme, and it also converges faster to the error floor than the other. In particular, when maintaining $BER_A = 10^{-5}$ and increasing the jamming-to-noise ratio ρ_{EA} from 0 to 30 dB, the blind feedback scheme needs about 5 dB in SNR_A, while the semi-blind feedback scheme requires only 2.5 to 3 dB to reach that result. Therefore, the semi-blind feedback scheme is suitable in the case of an active eavesdropper because the increase in jamming power from the active user E has less influence on the BER performance at the legitimate receiver user A. In fact, it can considerably improve the reliability factor of secrecy in FD wiretap transmission in the case of an active eavesdropper.

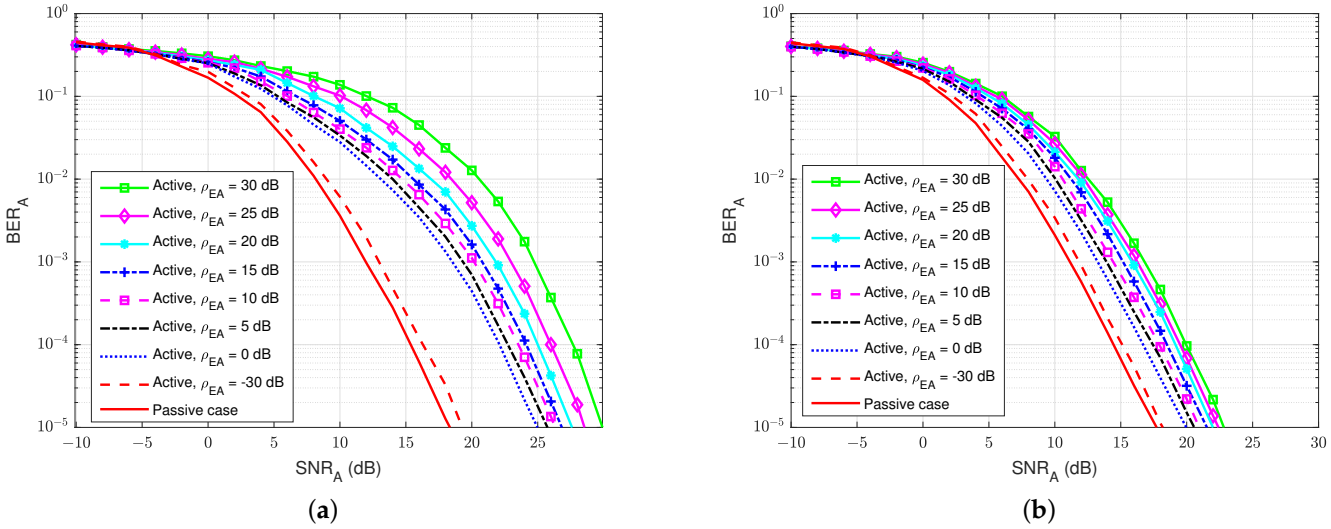

Figure 19. BER_A versus SNR_A, $\rho_{AA} = 30$ dB in case of an active eavesdropper: (**a**) Blind feedback; (**b**) Semi-blind feedback.

4.4.2. BER at the Eavesdropper User E

At the active eavesdropper user E, the BER performances versus SNR_E are also calculated to evaluate the amount of the message that user E can decode. As shown in Figure 20, it can be seen that the combination of both the jamming signal from user A and the self-interference component at user E themself has a major impact on the estimating and decoding process of user E. This is because the combined power of these two signals is larger than the power of the intended signal, and user E only uses the blind or semi-blind scheme without feedback for channel estimation and decoding, regardless of the knowledge of channel coding used for decoding and the four pilot symbols. The best BER that user E can obtain is about $BER_E = 10^{-2}$ at $SNR_E = 30$ dB, corresponding to the lowest level of the self-jamming-to-noise ratio from user A, $\rho_{AE} = 0$ dB. Consequently, when the power of the self-jamming signal from user A increases, user E needs a very large SNR_E to decode the intended message from user B.

Furthermore, Figure 21 shows the BER of user E versus the SNR_E for various values of the self-interference-to-noise ratio of itself, ρ_{EE}, while the self-jamming-to-noise ratio of user A, ρ_{AE} is fixed at 30 dB. It shows that if user E tries to increase the power of the jamming signal that is sent to user A, it leads to an increase in their BER because of the increase in the

self-interference-to-noise ratio ρ_{EE}. Although SI can be suppressed by the knowledge of the SI signal by the classical DSIC process, the interference from the self-jamming signal from user A still significantly impacts the blind scheme without feedback and the semi-blind scheme without feedback. It looks like the case of a passive eavesdropper when user E cannot suppress the interference from the jamming signal of user A well. However, the BER of user A is less sensitive to the increased power of user E, especially for the semi-blind feedback scheme, as shown in Figure 19.

Therefore, it can be concluded that user E cannot decode the message well, regardless of using the blind scheme without feedback or the semi-blind scheme without feedback.

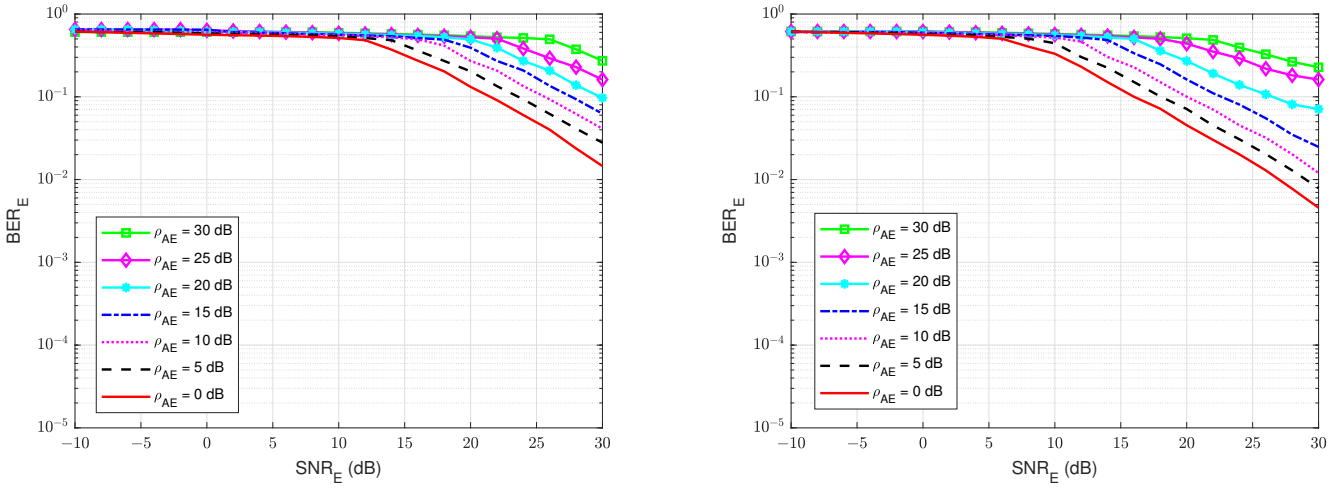

Figure 20. BER_E versus SNR_E, $\rho_{EE} = 30$ dB in case of an active eavesdropper: (**a**) Blind without feedback; (**b**) Semi-blind without feedback.

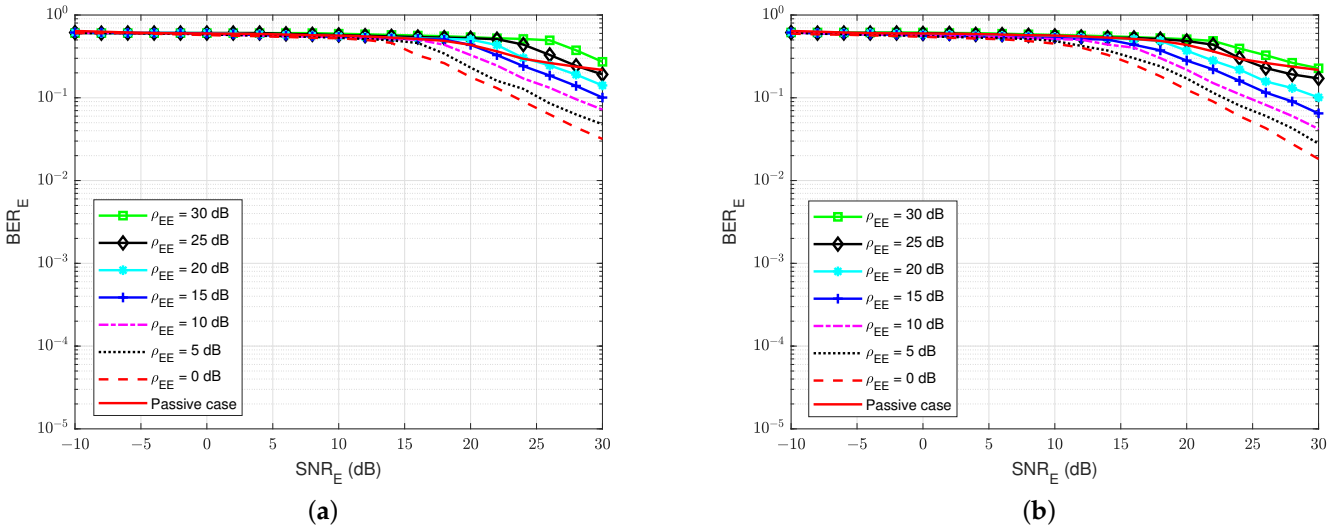

Figure 21. BER_E versus SNR_E, $\rho_{AE} = 30$ dB in case of an active eavesdropper: (**a**) Blind without feedback; (**b**) Semi-blind without feedback.

4.5. Security Gap Performance

Considering the same assumptions that have been made for background noises and propagation channels in the case of a passive eavesdropper in Section 3.6, it is also possible to simplify the notations and to denote in general the self-jamming power-to-noise ratio as ρ_{SJ} for both self-jamming (ρ_{AE}) and jamming (ρ_{EA}) channels. Since, in these conditions, we have $\rho_{SJ} = \rho_{AE} = \rho_{EA}$, adapting for practical applications, we also set $BER_{A,max} = 10^{-5}$

and $BER_{E,min} = 0.5$ for the maximum and minimum average errors that user A and user E can obtain, respectively. According to the results in Figures 19 and 20, in order to achieve $BER_{A,max} = 10^{-5}$ and $BER_{E,min} = 0.5$, the minimum SNR at the legitimate user A, $SNR_{A,min}$, and the maximum SNR at the eavesdropper user E, $SNR_{E,max}$, can be pointed out for different values of the general self-jamming power-to-noise ratio (ρ_{SJ}) and for different decoding schemes at user A and user E. Then, the security gap S_g is calculated based on $SNR_{A,min}$ and $SNR_{E,max}$ and summarized in Tables 4 and 5 when using the blind scheme without feedback and the semi-blind scheme without feedback at user E, respectively.

Table 4. The security gap when applying the blind scheme without feedback at user E.

ρ_{SJ}	Blind without Feedback at User E	Blind Feedback at User A		Semi-Blind Feedback at User A	
	$SNR_{E,max}$	$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	10.7	24.9	14.2	19.9	9.2
5	12.8	25.7	12.9	20.3	7.5
10	15.4	26.3	10.9	21	5.6
15	17.5	26.8	9.3	21.5	4
20	19.9	27.6	7.7	22	2.1
25	22.2	28.5	6.3	22.3	0.1
30	25.6	29.8	4.2	22.8	−2.8

Table 5. The security gap when applying the semi-blind scheme without feedback at user E.

ρ_{SJ}	Semi-Blind without Feedback at User E	Blind Feedback at User A		Semi-Blind Feedback at User A	
	$SNR_{E,max}$	$SNR_{A,min}$	S_g	$SNR_{A,min}$	S_g
0	6.2	24.9	18.7	19.9	13.7
5	8.2	25.7	17.5	20.3	12.1
10	10.8	26.3	15.5	21	10.2
15	13.4	26.8	13.4	21.5	8.1
20	16.1	27.6	11.5	22	5.9
25	18.2	28.5	10.3	22.3	4.1
30	21.5	29.8	8.3	22.8	1.3

Figure 22 shows the comparison of the security gap S_g with the various values of the general self-jamming power-to-noise ratio, ρ_{SJ}, between the application of the blind feedback scheme and the semi-blind feedback scheme on the decoding side of user A. It indicates that the increase in the self-jamming power-to-noise ratio ρ_{SJ} leads to a decrease in the security gap S_g for all cases. The proposed semi-blind feedback scheme also allows for reducing the security gap S_g from about 5 to 7 dB compared to the blind feedback scheme, regardless of the use of the blind or semi-blind scheme without feedback in user E. Therefore, it can keep the security gap as small as possible, which is the most important factor in PLS. Furthermore, the SNR_A of user A is reduced when performing channel estimation or decoding the message using the semi-blind feedback scheme, compared to the blind feedback scheme, which means that the system not only guarantees the security factor but also improves power consumption.

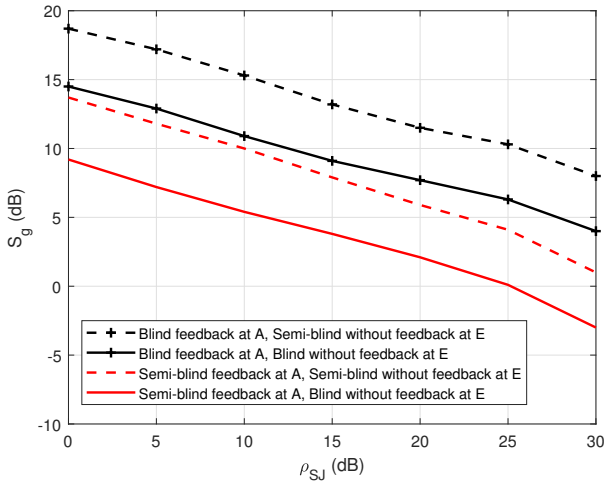

Figure 22. S_g versus ρ_{SJ} in case of an active eavesdropper.

5. Conclusions

The secrecy analysis of FD short-packet transmission in a wiretap channel for both passive and active eavesdroppers has been implemented, subject to the constraints of the MSE, BER, security gap S_g. This paper highlights that the presence of a jamming signal has a major effect on the reliability and security factors in PLS. To deal with this effect, a joint iterative SI channel estimation, propagation channel estimation, and decoding algorithm in FD transmissions via feedback were applied at the legitimate receiver, including blind feedback or semi-blind feedback schemes in the case of passive and active eavesdroppers, respectively. The numerical results presented show that the proposed algorithms, such as the blind feedback scheme in the passive case and the semi-blind feedback scheme in the active case, outperform the conventional algorithms without feedback, where the security gap S_g is significantly reduced. Moreover, it can be noticed that the blind feedback scheme in the case of a passive eavesdropper and the semi-blind feedback scheme in the case of an active eavesdropper are less sensitive to the increase in self-jamming power. Moreover, the SNR of the legitimate receiver is reduced when applying the proposed schemes to decode the intended message, which means that the system not only ensures the security factor well, but it also significantly improves the power consumption by reducing the transmitting power. It is also noted that the proposed blind and semi-blind algorithms have better performances in terms of processing time and computational complexity, which are shown in [27,28]. Therefore, the presence of joint iterative estimation and decoding with blind and semi-blind algorithms at the legitimate receiver is highly recommenced to enhance the security of FD wiretap transmission, especially in short-packet transmission-specific to IoT applications and green communications.

6. Future Works

In the near future, several interesting investigations should be established in the context of the physical layer security field, especially in FD short-packet transmission. First, the location of the eavesdropper will be considered to emphasize the outperformance of the proposed algorithm with the conventional algorithm. Moreover, a hardware implementation based on Software-Defined Radio (SDR) will be considered to emphasize the performance of the proposed schemes in realistic transmission scenarios for IoT applications and green communications.

Author Contributions: Conceptualization, B.Q.V., A.F. and R.G.; methodology, B.Q.V., A.F. and R.G.; software, B.Q.V. and C.D.-S.; validation, M.M., A.F. and R.G.; formal analysis, B.Q.V., A.F. and R.G.; investigation, B.Q.V., R.G. and A.F.; resources, B.Q.V. and C.D.-S.; data curation, B.Q.V. and A.F.; writing—original draft preparation, B.Q.V. and A.F.; writing—review and editing, B.Q.V., R.G., A.F., M.M. and C.D.-S.; visualization, B.Q.V., A.F. and M.M.; supervision, R.G. and M.M.; project administration, R.G.; funding acquisition, R.G., A.F. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research is jointly supported by the IBNM (Brest Institute of Computer Science and Mathematics), CyberIoT Chair of Excellence at the University of Brest (UBO), and the Brittany region—Pôle d'Excellence Cyber.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors would like to thank to the University of Brest (UBO), the Direction Europe and International (DEI), the IBNM (Brest Institute of Computer Science and Mathematics) CyberIoT Chair of Excellence, and the Brittany region—Pôle d'Excellence Cyber for their funding.

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

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	The Third-Generation Partnership Project
5G	The Fifth Generation
ADC	Analog-to-Digital Converter
BER	Bit Error Rate
DAC	Digital-to-Analog Converter
DSIC	Digital Self-interference Cancellation
FD	Full-Duplex
IoT	Internet of Things
ITU	International Telecommunication Union
LLR	Log Likelihood Ratio
LoS	Line-of-Sight
MSE	Mean Square Error
NLoS	Non-Line-of-Sight
PLS	Physical Layer Security
QC-LDPC	Quasi-Cyclic Low-Density Parity Check
QPSK	Quadature Phase Shift Keying
RF	Radio Frequency
RLS	Recursive Least Square
SDR	Software-Defined Radio
SI	Self-Interference
SPA	Sum Product Algorithm
uRLLC	Ultra-reliable Low-Latency Communication

References

1. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
2. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2012**, *58*, 1875–1888. [CrossRef]
3. Nguyen, B.V.; Jung, H.; Kim, K. Physical Layer Security Schemes for Full-Duplex Cooperative Systems: State of the Art and Beyond. *IEEE Commun. Mag.* **2018**, *56*, 131–137. [CrossRef]
4. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
5. Ozarow, L.H.; Wyner, A.D. Wire-Tap Channel II. *Bell Syst. Tech. J.* **1984**, *63*, 2135–2157. [CrossRef]

6. Arı, N.; Thomos, N.; Musavian, L. Active Eavesdropping in Short Packet Communication: Average Secrecy Throughput Analysis. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. [CrossRef]
7. Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.; Kwak, B.J. LDPC Codes for the Gaussian Wiretap Channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540. [CrossRef]
8. Ahmed, E.; Eltawil, A.M. All-Digital Self-Interference Cancellation Technique for Full-Duplex Systems. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 3519–3532. [CrossRef]
9. Khan, R.; Tsiga, N.; Asif, R. Interference Management with Reflective In-Band Full-Duplex NOMA for Secure 6G Wireless Communication Systems. *Sensors* **2022**, *22*, 2508. [CrossRef]
10. Liu, Y.; Zhu, X.; Lim, E.G.; Jiang, Y.; Huang, Y. Fast Iterative Semi-Blind Receiver for URLLC in Short-Frame Full-Duplex Systems With CFO. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 839–853. [CrossRef]
11. Zhang, J.; He, F.; Li, W.; Li, Y.; Wang, Q.; Ge, S.; Xing, J.; Liu, H.; Li, Y.; Meng, J. Self-Interference Cancellation: A Comprehensive Review from Circuits and Fields Perspectives. *Electronics* **2022**, *11*, 172. [CrossRef]
12. Chen, Y.; Ding, C.; Jia, Y.; Liu, Y. Antenna/Propagation Domain Self-Interference Cancellation (SIC) for In-Band Full-Duplex Wireless Communication Systems. *Sensors* **2022**, *22*, 1699. [CrossRef] [PubMed]
13. Wang, H.M.; Wang, C.; Ng, D.W.K. Artificial Noise Assisted Secure Transmission Under Training and Feedback. *IEEE Trans. Signal Process.* **2015**, *63*, 6285–6298. [CrossRef]
14. Silva, A.; Gomes, M.; Vilela, J.; Harrison, W. SDR Proof-of-Concept of Full-Duplex Jamming for Enhanced Physical Layer Security. *Sensors* **2021**, *21*, 856. [CrossRef] [PubMed]
15. Zheng, G.; Krikidis, I.; Li, J.; Petropulu, A.P.; Ottersten, B. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers. *IEEE Trans. Signal Process.* **2013**, *61*, 4962–4974. [CrossRef]
16. Li, W.; Ghogho, M.; Chen, B.; Xiong, C. Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis. *IEEE Commun. Lett.* **2012**, *16*, 1628–1631. [CrossRef]
17. Dryer, Z.; Nickerl, A.; Gomes, M.A.C.; Vilela, J.P.; Harrison, W.K. Full-Duplex Jamming for Enhanced Hidden-Key Secrecy. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
18. Shang, Z.; Zhang, T.; Cai, Y.; Yang, W.; Wu, H.; Zhang, Y.; Tao, L. Secure Transmission in Cognitive Wiretap Networks with Full-Duplex Receivers. *Appl. Sci.* **2020**, *10*, 1840. [CrossRef]
19. Li, Y.; Zhao, R.; Tan, X.; Nie, Z. Secrecy performance analysis of artificial noise aided precoding in full-duplex relay systems. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6. [CrossRef]
20. Yan, S.; Zhou, X.; Yang, N.; Abhayapala, T.D.; Swindlehurst, A.L. Secret Channel Training to Enhance Physical Layer Security With a Full-Duplex Receiver. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2788–2800. [CrossRef]
21. Sybis, M.; Wesolowski, K.; Jayasinghe, K.; Venkatasubramanian, V.; Vukadinovic, V. Channel Coding for Ultra-Reliable Low-Latency Communication in 5G Systems. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 1–5. [CrossRef]
22. Merhav, N. Encoding Individual Source Sequences for the Wiretap Channel. *Entropy* **2021**, *23*, 1694. [CrossRef]
23. Macro, B.; Nicola, M.; Giocomo, R.; Franco, C. Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels. *EURASIP J. Wirel. Commun. Netw.* **2015**, *15*, 232. [CrossRef]
24. Yang, Z.; Fan, Y.; Wang, A. Artificial noise and LDPC code aided physical layer security enhancement. In Proceedings of the 2014 International Conference on Information and Communications Technologies (ICT 2014), Nanjing, China, 15–17 May 2014; pp. 1–6.
25. Du, J. A Partially Coupled LDPC Coded Scheme for the Gaussian Wiretap Channel. *IEEE Commun. Lett.* **2020**, *24*, 7–10. [CrossRef]
26. Li, L.; Xing, Y.; Yao, X.; Luo, Y. McEliece Coding Method based on LDPC Code with Application to Physical Layer Security. In Proceedings of the 2021 7th International Conference on Computer and Communications (ICCC), Chengdu, China, 10–13 December 2021; pp. 2042–2045. [CrossRef]
27. Vuong, B.Q.; Gautier, R.; Fiche, A.; Marazin, M.; Ta, H.Q.; Nguyen, L.L. Joint Iterative Blind Self-Interference Cancellation, Propagation Channel Estimation and Decoding Processes in Full-Duplex Transmissions. *IEEE Access* **2022**, *10*, 22795–22807. [CrossRef]
28. Vuong, B.Q.; Gautier, R.; Ta, H.Q.; Nguyen, L.L.; Fiche, A.; Marazin, M. Joint Semi-Blind Self-Interference Cancellation and EqualisationProcesses in 5G QC-LDPC-Encoded Short-Packet Full-Duplex Transmissions. *Sensors* **2022**, *22*, 2204. [CrossRef] [PubMed]
29. Bae, J.H.; Abotabl, A.; Lin, H.P.; Song, K.B.; Lee, J. An overview of channel coding for 5G NR cellular communications. *Trans. Signal Inf. Process.* **2019**, *8*, e17. [CrossRef]
30. 3GPP. TS 38.212 NR- Multiplexing and Channel Coding. 2018. Available online: https://www.etsi.org/deliver/etsi_ts/138200_138299/138212/15.02.00_60/ts_138212v150200p.pdf (accessed on 29 June 2018).
31. Li, H.; Bai, B.; Mu, X.; Zhang, J.; Xu, H. Algebra-Assisted Construction of Quasi-Cyclic LDPC Codes for 5G New Radio. *IEEE Access* **2018**, *6*, 50229–50244. [CrossRef]
32. Clapham, C.; Jordan, N. *The Concise Oxford Dictionary of Mathematics*; Oxford University Press: Oxford, UK, 2013.

33. Everett, E.; Sahai, A.; Sabharwal, A. Passive Self-Interference Suppression for Full-Duplex Infrastructure Nodes. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 680–694. [CrossRef]
34. Koohian, A.; Mehrpouyan, H.; Nasir, A.A.; Durrani, S.; Blostein, S.D. Residual self-interference cancellation and data detection in full-duplex communication systems. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017.
35. Kim, T.; Kyungsik, M.; Park, S. Self-Interference Channel Training for Full-Duplex Massive MIMO Systems. *Sensors* **2021**, *21*, 3250. [CrossRef]
36. Haykin, S. *Adaptive Filter Theory*; Pearson: London, UK, 1993; Volume 29.
37. Sharon, E.; Litsyn, S.; Goldberger, J. An efficient message-passing schedule for LDPC decoding. In Proceedings of the 2004 23rd IEEE Convention of Electrical and Electronics Engineers in Israel, Tel-Aviv, Israel, 6–7 September 2004; pp. 223–226.
38. Zhang, X.; Siegel, P.H. Quantized iterative message passing decoders with low error floor for LDPC codes. *IEEE Trans. Commun.* **2014**, *62*, 1–14.
39. Vuong, B.Q.; Gautier, R.; Fiche, A.; Marazin, M. Full-Duplex Efficient Channel Codes for Residual Self-Interference/Quantization Noise Cancellation. In Proceedings of the IEEE 15th International Conference on Signal Processing and Communication Systems (ICSPCS), Sydney, Australia, 13–15 December 2021.
40. Despina-Stoian, C.; Digulescu-Popescu, A.; Alexandra, S.; Youssef, R.; Radoi, E. Comparison of Adaptive Filtering Strategies for Self-Interference Cancellation in LTE Communication Systems. In Proceedings of the 13th International Conference on Communications (COMM), Bucharest, Romania, 18–20 June 2020.
41. Mostari, L.; Taleb ahmed, A. High performance short-block binary regular LDPC codes. *AEJ Alex. Eng. J.* **2018**, *57*, 2633–2639. [CrossRef]
42. Iscan, O.; Lentner, D.; Xu, W. A Comparison of Channel Coding Schemes for 5G Short Message Transmission. In Proceedings of the 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
43. Hajiyat, Z.; Sali, A.; Mokhtar, M.; Hashim, F. Channel Coding Scheme for 5G Mobile Communication System for Short Length Message Transmission. *Wirel. Pers. Commun.* **2019**, *106*, 377–400. [CrossRef]
44. Masmoudi, A.; Le-Ngoc, T. A Maximum-Likelihood Channel Estimator for Self-Interference Cancelation in Full-Duplex Systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 5122–5132. [CrossRef]
45. ITU. *Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000*; International Telecommunication Union: Geneva, Switzerland, 1997.