Efficient Blind and Semi-Blind Approaches on Encoded Wiretap Full-Duplex Transmissions

Bao Quoc Vuong, Roland Gautier, Anthony Fiche, Mélanie Marazin

Efficient Blind and Semi-Blind Approaches on Encoded Wiretap Full-Duplex Transmissions

Bao Quoc Vuong[1,2], Roland Gautier[3], Anthony Fiche[3] and Mélanie Marazin[3],
[1] School of Electrical Engineering, International University, Ho Chi Minh City 700000, Vietnam
[2] Vietnam National University, Ho Chi Minh City 700000, Vietnam
[3] Univ Brest, CNRS, Lab-STICC, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France
Email: vqbao@hcmiu.edu.vn; {roland.gautier, anthony.fiche and melanie.marazin}@univ-brest.fr

***Abstract*—This paper investigates the secrecy coding analysis of encoded wiretap Full-Duplex transmission respected to various eavesdropper positions. To limit the effect of interference and self-jamming/jamming signals sending by the legitimate receiver and eavesdropper, a combination of joint iterative blind/semi-blind channel estimation, decoding algorithms and self-jamming techniques is used. In fact, these algorithms employ a feedback loop to estimate and reduce SI components while also estimating the propagation channel and decoding the messages. The results reveal that blind/semi-blind algorithms give a better solution than conventional without feedback algorithms by significantly reducing and giving smaller security gap. Furthermore, they are less sensitive to the eavesdropper's movement by maintaining security gap in an acceptable level. The results also indicate that the suggested algorithms have a capability to notably decrease the self-jamming power required at the authorized receiver to obtain the same security level. It shows a robustness in several factors such as security, reliability and power consumption, which is suitable for short-packet Internet of Things transmissions and green communications.**

***Index Terms*—Security gap, 5G QC-LDPC codes, physical layer security, self-jamming, blind/semi-blind algorithms.**

I. Introduction

In recent years, significant researches have been dedicated to enhance new techniques and new security solutions in wireless communication, particularly in 5G networks & beyond [1]. Indeed, they have explored the use of Physical Layer Security (PLS), which exploits the properties of the communication channel itself to provide security. Most of these works are based on the classical wiretap channel with a passive eavesdropper, which was initially proposed by Wyner in 1975 [2] and the wiretap channel II with the active eavesdropper, which was created by Ozarow and Wyner [3]. In PLS area, security gap is one of the security metric, which was first proposed in [4] and measures by the difference of Bit Error Rate (BER) on log scale between the receiver and eavesdropper channels. This interval is typically used to ensure both reliably and security characteristics throughout the transmission.

Nowadays, due to the spectrum efficiency by using the same time and frequency resources for both transmission and reception, Full-Duplex (FD) transmissions with fully suppression of residual Self-Interference (SI) have become a crucial scheme in 5G & Beyond, especially in short-packet transmissions [5]. In the field of PLS, the deployment of FD self-jamming or Artificial Noise (AN) at the receiver for security reasons has been thoroughly investigated and developed further due to its robustness and favorable performance. This holds true even when the channel condition of the unauthorized receiver is equal to or superior to that of the authorized receiver [6]–[8]. Furthermore, for communications with finite block length or short-packet, the secrecy capacity of the channel and the reliability of transmission messages might be considered as an issue [9]. As a result, the application of PLS to short-packet transmission has emerged as a recent topic of interest for research.

Moreover, due to excellent error correction performance in various wireless communication scenarios, secrecy channel coding techniques have received a lot of attention in recent years, particularly 5G Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes [10], which are acted as standard codes for 5G transmissions [11]. Indeed, the authors in [12], [13] investigated various LDPC codes constructions and AN signal with the puncturing, scrambling matrix and decoding approaches to evaluate the reliability and security over Gaussian wiretap channel. In [14]–[16], the authors suggested a couple of iterative algorithms that combine blind and semi-blind techniques for estimating channels and decoding procedures in order to evaluate the secrecy metric in short-packet FD transmission. It shows that their approaches outperform conventional methods by reducing significantly the secrecy gap, and achieve low power consumption. However, the distances between the transceivers, which can be seen as an important factor in PLS, are not taken into account in these works.

Therefore, in this paper, we will consider the combination of joint iterative blind/semi-blind algorithms and FD self-jamming at the legitimate receiver to improve the security and reliability metrics and also enhance the power consumption with respect to various eavesdropper's locations. The contributions of this paper are:

- We demonstrate that the proposed system performs better results than conventional without feedback systems in both passive and active eavesdroppers;
- We emphasize that the proposed system is less sensitive to eavesdropper's motion by limiting the increase of security gap;
- We show that the proposed system can greatly minimize self-jamming power that emitted by legitimate receiver

regardless of eavesdropper's locations, which is suitable for the power consumption factor in IoT transmissions.

The rest of this paper is structured as follows. In Section II, an overview system model is presented. The proposed feedback schemes, the model of eavesdropper's locations and security gap are also indicated. In Section III, numerical results and discussions are provided involving passive and active eavesdropper scenarios, respectively. Lastly, Section IV will present some key insights and conclusions.

II. System Model and Problem Formulation

A. System Model

Considering a wiretap transmission model between three users: Alice (A) as a transmitter, Bob (B) as a legitimate receiver and Eve (E) as an eavesdropper, respectively. Alice is attached with one antenna for broadcasting its intended message $\mathbf{x}_A$ to other users, while Bob and Eve are equipped with two antennas for operating in FD mode, allowing them to instantaneously receive information messages $(\mathbf{y}_B, \mathbf{y}_E)$ and transmit self-jamming/jamming signals $(\mathbf{x}_B, \mathbf{x}_E)$, as shown in Fig. 1.

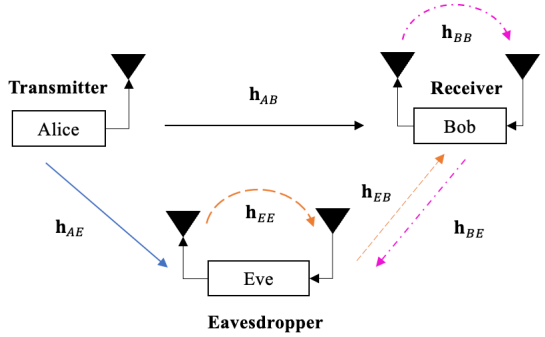


Fig. 1: System model.

At the transmitter of all transceivers, the input message is encoded by using (N, K) 5G QC-LDPC codes, where N and K denote the length of code word message and information message, respectively. The channel gain between two users is denoted as $\mathbf{h}_{XY}$ in which $X \in \{A, B, E\}$ and $Y \in \{B, E\}$ and is further formulated with respect to the distances as $\mathbf{h}_{XY} = \sqrt{d_{XY}^{-\phi}}\mathbf{g}_{XY}$, where d_{XY} is the distance between two users, $\mathbf{g}_{XY}$ is the fading coefficients and ϕ is path-loss exponent. Moreover, these channels are modeled as i.i.d. complex Gaussian random variables with $\mathcal{CN}(0, d_{XY}^{-\phi})$ [17]. It also denotes that $\mathbf{h}_{YY}$ is the channel gain of SI channel at user Y as quasi-static Rayleigh distribution in digital domain, with $Y \in \{B, E\}$, and it is modeled as i.i.d complex Gaussian random variables with $\mathcal{CN}(0, 1)$ [18]. Furthermore, let us denote p_X as the transmitted power of each user, where $X \in \{A, B, E\}$ and w_Y as the complex background noise at user Y with $\mathcal{CN}(0, \sigma_Y^2)$, where $Y \in \{B, E\}$. Considering the background noise as reference, we further denote $\rho_{XY} = \sqrt{d_{XY}^{-\phi}}p_X/\sigma_Y^2$ and $\rho_{YY} = p_Y/\sigma_Y^2$ as self-jamming to noise ratio provided by the self-jamming channel from user X to user Y and self-interference to noise ratio given by the SI channel at user Y, respectively. We also denote the $SNR_Y = p_A\sqrt{d_{AY}^{-\phi}}/\sigma_Y^2$ as the Signal to Noise Ratio (SNR) at user Y, where d_{AY} is the distance between Alice and user Y and $Y \in \{B, E\}$ corresponding to Bob and Eve, respectively. The received signals at Bob and Eve, are respectively given by Equation (1) and Equation (2) in case of passive eavesdropper and Equation (3) and Equation (4) in case of active eavesdropper.

On the receiver side, the Recursive Least Square (RLS) algorithm [19] is used to firstly estimate and then cancel the SI component in Digital Self-Interference Cancellation (DSIC) process. The residual signal continuously passes through an equalizer to get equalized signal. Then, this signal will continue the process in two cases, named blind and semi-blind without feedback schemes, and denoted as BWoFB and SBWoFB schemes, respectively, as shown in Figure 2. The difference is that the extra pilot symbols, that adding into the message sequence at the transmitter, are eliminated in the case of semi-blind without feedback scheme before the signal continues to the demodulator to obtain the belief sequence. Finally, the traditional decoding method as Sum Product Algorithm (SPA) [20] with m_{max} iterations is used to achieve the binary sequence of the input message from Alice.

B. Proposed Blind/Semi-blind Feedback Algorithm

In [14], [15], a couple of iterative algorithms that combine blind and semi-blind techniques for estimating channels and decoding procedures have been proposed to improve the overall performance, reduce computational complexity as well as decoding latency, called as blind and semi-blind feedback schemes, and denoted as BFB and SBFB schemes, respectively. The flowcharts of these schemes are shown in Fig. 3 and Fig. 4, respectively. In these two feedback schemes, the processes at the receiver can benefit from each other through feedback loop, hence improving overall performance. The blind method with unknown broadcast signal from Alice, in particular, includes four basic steps, which are as follows:

Step 1: Using $\mathbf{x_B}$ as the reference, we can firstly estimate $\hat{\mathbf{h}}_{BB}$ and then cancel the SI component $\hat{\mathbf{y}}_{BB}$ from the received signal $\mathbf{y_B}$. Consequently, the residual signal $\tilde{\mathbf{y}}_B$ is produced after this process;

Step 2: Without Alice's knowledge, an equalizer is implemented to simultaneously estimate the main channel $\hat{\mathbf{h}}_{AB}$ and obtain the equalized signal $\mathbf{y}'_B$, respectively. Then the demodulator and de-interleaver processes are apply in order to achieve the belief sequence for decoding process.

Step 3: After that, the intended message from Alice is decoded by using the conventional SPA algorithm. It is noticed that only one iteration ($m_{max} = 1$) is used in this step.

Step 4: If the number of joint iterations has not been achieved the maximum value ($k < k_{max}$), the desired feedback signal $\hat{\mathbf{y}}_{AB}$ will be created by a temporary feedback loop. In particular, the temporary message obtained from Step 3 is repeatedly re-encoded, re-interleaved, re-modulated, and filtered with $\hat{\mathbf{h}}_{AB}$ that produced in Step 2. Finally, the SI channel estimation process in the next joint iteration can be significantly improved by subtracting the feedback signal from the received signal.

$$y_B[n] = (\sqrt{p_A}\mathbf{x}_A * \sqrt{d_{AB}^{-\phi}}\mathbf{g}_{AB})[n] + (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BB})[n] + w_B[n]; \tag{1}$$

$$y_E[n] = (\sqrt{p_A}\mathbf{x}_A * \sqrt{d_{AE}^{-\phi}}\mathbf{g}_{AE})[n] + (\sqrt{p_B}\mathbf{x}_B * \sqrt{d_{BE}^{-\phi}}\mathbf{g}_{BE})[n] + w_E[n]; \tag{2}$$

$$y_B[n] = (\sqrt{p_A}\mathbf{x}_A * \sqrt{d_{AB}^{-\phi}}\mathbf{g}_{AB})[n] + (\sqrt{p_B}\mathbf{x}_B * \mathbf{h}_{BB})[n] + (\sqrt{p_E}\mathbf{x}_E * \sqrt{d_{BE}^{-\phi}}\mathbf{g}_{BE})[n] + w_B[n], \tag{3}$$

$$y_E[n] = (\sqrt{p_A}\mathbf{x}_A * \sqrt{d_{AE}^{-\phi}}\mathbf{g}_{AE})[n] + (\sqrt{p_E}\mathbf{x}_E * \mathbf{h}_{EE})[n] + (\sqrt{p_B}\mathbf{x}_B * \sqrt{d_{BE}^{-\phi}}\mathbf{g}_{BE})[n] + w_E[n], \tag{4}$$

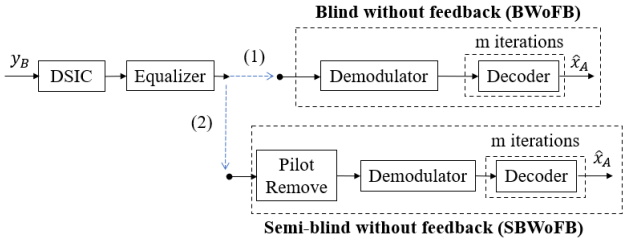


Fig. 2: Flowchart of BWoFB and SBWoFB schemes.

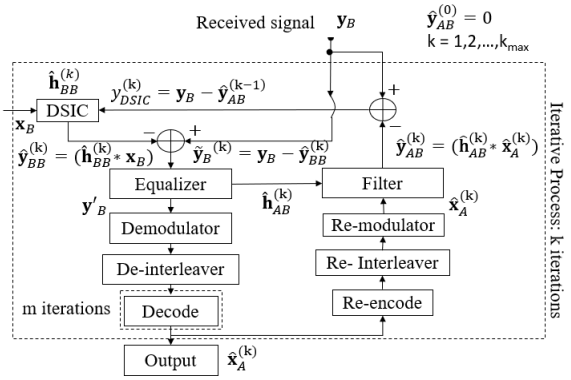


Fig. 3: Flowchart of BFB scheme.

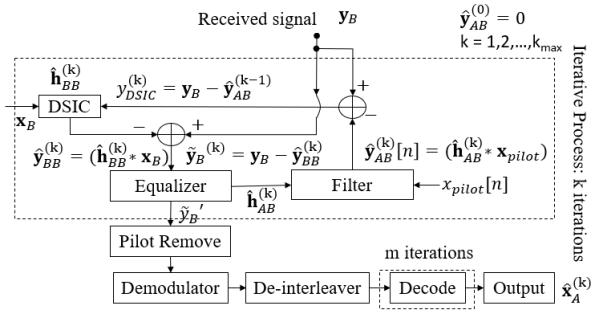


Fig. 4: Flowchart of SBFB scheme.

Additionally, due to its suitable performance in low SNR regions [15], it is recommended that the semi-blind algorithm needs to be used in active eavesdropper case, by adding pilot symbols to the information message and implementing feedback loops for the estimation and equalization processes, as shown in Fig. 4. In fact, the adding pilot symbols are used to form the estimated version of the intended signal. The algorithm is stopped when $k = k_{max}$. Then, the pilot symbols are eliminated from the equalized signal, and then the system proceeds to demodulate, de-interleave, and decode the message to get the final message. It is also worth noting that only one iteration in SPA decoding algorithm ($m_{max} = 1$).

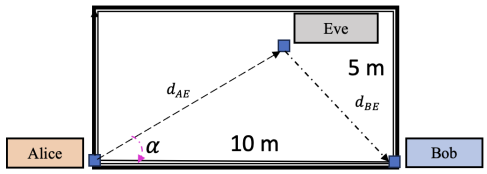


Fig. 5: System model respected to locations of eavesdropper.

C. The Model of Eavesdropper's Locations

In this paper, we consider the secrecy performance under the condition that the eavesdropper is moved to different positions inside of a fixed rectangular room as shown in Fig. 5.

In particular, the distance between Alice and Bob d_{BA} is fixed at 10 m, while only Eve is allowed to freely move. Therefore, based on Alice and Bob's location as a reference, we will consider two scenarios such as (i) changing the angle α, where $\alpha \in [15, 30, 45, 60, 75, 90]^\circ$ and (ii) changing the distance d_{AE}, where $d_{AE} \in [2, 4, 6, 8, 10]$ m. At this point, d_{AE} and α must be chosen in order to satisfy the condition that Eve does not move outside the room. Furthermore, this configurations also lead to change the distance between Bob and Eve, d_{BE}, where $d_{BE} = \sqrt{d_{AB}^2 + d_{AE}^2 - 2d_{AB}d_{AE}cos(\alpha)}$.

In this paper, let us assume following hypotheses:

- For passive scenario, Bob uses solely blind estimation due to its adequate performance in the evaluated SNR area, compared to the conventional SPA decoding at Eve, because Eve only operates in Half-Duplex mode.
- For active scenario, when the SNR at Bob is reduced by the jamming signal from Eve, semi-blind feedback technique is also used beside blind method at Bob due to its high performance in low SNR, compared to the conventional BWoFB/SBWoFB scheme at Eve;
- Both Bob and Eve have equal computational capability.

D. Security Gap

The security gap is established and illustrated in Fig. 6 to emphasize the reliability and secrecy conditions in relation to BER performance and SNR parameters [4], [8], [12]. In particular, is calculated as the smallest difference of SNRs (in dB) between the receiver and the eavesdropper:

$$S_g(dB) = SNR_{B,min} - SNR_{E,max} \tag{5}$$

where $SNR_{B,min}$ is the minimal SNR that corresponds to $BER_{B,max}$, and Bob must operate in order for the BER to be less than a reliability threshold, i.e. $BER_{B,max} = 10^{-5}$ [12]. Similarly, $SNR_{E,max}$ is the maximal SNR corresponding to $BER_{E,min}$ can approach a certain threshold, i.e. $BER_{E,min} = 0.5$, It is referred to as the security threshold

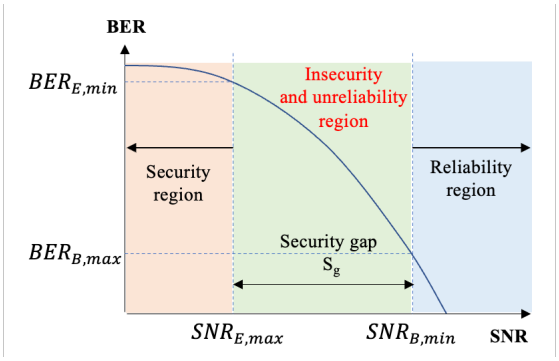


Fig. 6: Security gap.

since Eve is unable to precisely decode the information message in this region [4]. A lower S_g will result in a reduced cost as well as higher reliability and security features. As a result, the purpose of this article is to keep the value and the increase of S_g as small as possible regardless of Eve's position.

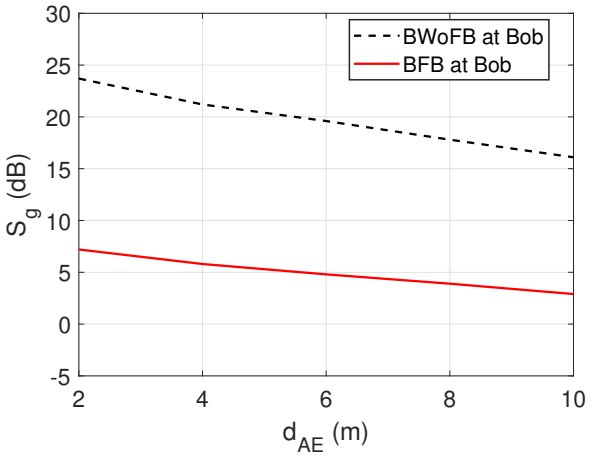
III. Results and Discussions

A. Simulation Specifications

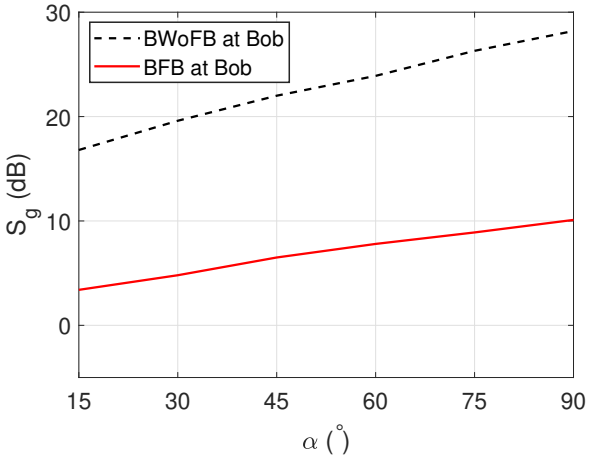
Monte Carlo simulations on MATLAB are used to evaluate the secrecy performance of our suggested schemes. (256,128) 5G QC-LDPC codes are used with the code rate $R = 1/2$ and 10^6 transmission frames. Modulation scheme is QPSK and four pilot symbols are added in semi-blind scheme. Number of iteration (k_{max}, m_{max}) of feedback schemes is (4,1) and number of iterations m_{max} of without feedback schemes is 20. Based on the Rayleigh distribution, the SI channel and self-jamming channel are set up with three taps. The intended and wiretap channels have four taps, and the fading coefficients are based on the ITU-R channel model [21]. We further assume that the measurement environment is set up inside a furnished room and the path-loss exponent coefficient is $\phi = 3$ [9].

B. In Case of Passive Eavesdropper

Fig. 7 shows the security gap S_g versus the distance between Alice and Eve (d_{AE}) and the angle α in case of passive eavesdropper. The self-interference to noise ratio at Bob (ρ_{BB}) and the self-jamming to noise ratio from Bob to Eve (ρ_{BE}) are fixed at 35 dB. On Bob's decoding side, both BFB and BWoFB schemes are used, whereas Eve just uses the traditional SPA algorithm to decode the message. First of all, the angle α is fixed at 30° and the distance d_{AE} will be changed in the interval $[2, 10]$, as shown in Figure 7a. The result indicates that when Eve will move far away from Alice (d_{AE} increases), the security gap S_g will decrease. However, the BFB scheme at Bob gives a better result than the BWoFB scheme. Indeed, the security gap S_g is always below 7dB and tends to go to 0 dB when Bob uses BFB scheme. In contrast, the security gap S_g is always larger than about 15 dB when using BWoFB scheme at Bob. In Figure 7b, we try to change the angle in the interval $[15; 90]$ and fix the distance $d_{AE} = 6$ (m). It implies that the security gap S_g increases when the angle α increases, which means the security factor will decrease. Because Eve is close to Alice and far away from Bob, she will have better channel conditions than Bob. However, we can improve Bob's security by employing a BFB algorithm. In fact, the slope of the BFB curve is smaller than that of the BWoFB curve, implying that



(a) S_g versus d_{AE} with $\alpha = 30°$.

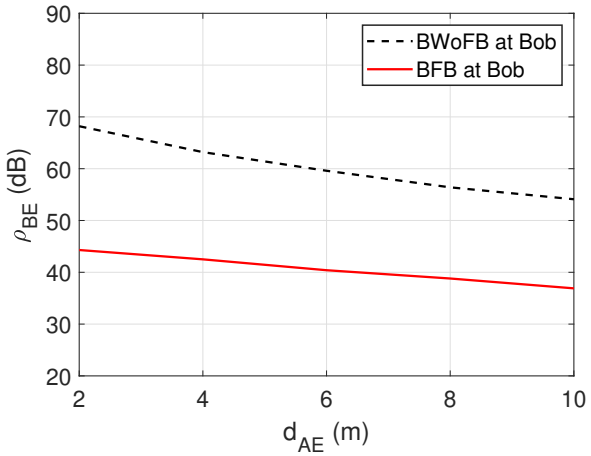


(b) S_g versus α with $d_{AE} = 6$ m.

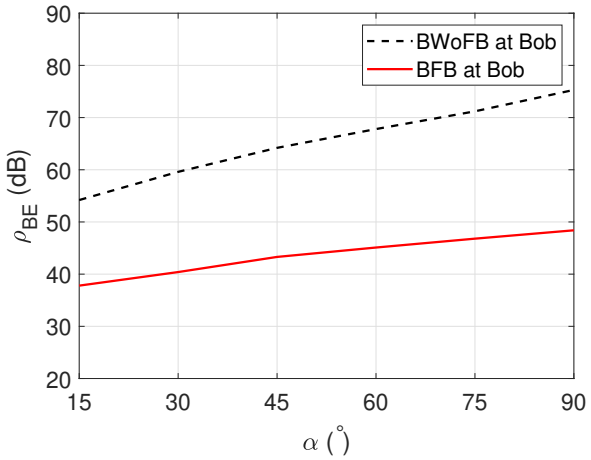
Fig. 7: S_g versus d_{AE}, α in case of passive eavesdropper, $\rho_{BB} = \rho_{BE} = 35$ dB.

the BFB scheme in Bob is less sensitive to increasing of α, i.e, S_g increases about 6 dB in feedback curve while it increases about 12 dB in BWoFB curve, when α varies from 15 to 90°.

Next, Fig. 8 shows the self-jamming to noise ratio (ρ_{BE}) versus the distance between Alice and Eve (d_{AE}) and the angle α, where the security gap S_g is fixed at 0 dB, which can be seen as a perfect security and reliability threshold. Indeed, Fig. 8a shows ρ_{BE} versus d_{AE} when we fix $\alpha = 30°$. We can see that using BFB scheme at Bob gives a better result than the conventional BWoFB scheme, it uses nearly 38 dB compared to about 54 dB when $d_{AE} = 10$ (m). Furthermore, Fig. 8b shows ρ_{BE} versus α when the distance $d_{AE} = 6$ m. We can clearly see that ρ_{BE} obviously increases as α increases, implying that Bob must use more power for the self-jamming signal to ensure the security and reliability of the transmission when Eve tries to move far away from Bob. However, the slope of the BFB curve is smaller than that of the BWoFB curve. In particular, the maximum self-jamming power that Bob needs to use is only about 48 dB when $\alpha = 90°$ compared to that of nearly 75 dB. As a result, using the BFB system at Bob can minimize the use of self-jamming power, i.e. Bob needs to increase about 10 dB if using feedback scheme compared to around 20 dB if using without feedback scheme when the angle α goes from 15 to 90°.

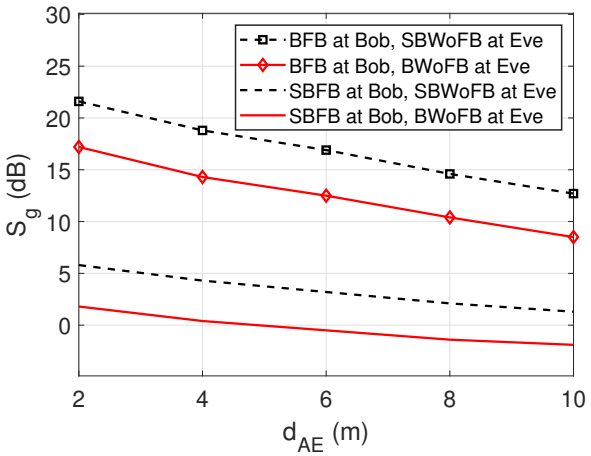


(a) ρ_{BE} versus d_{AE} with $\alpha = 30°$.

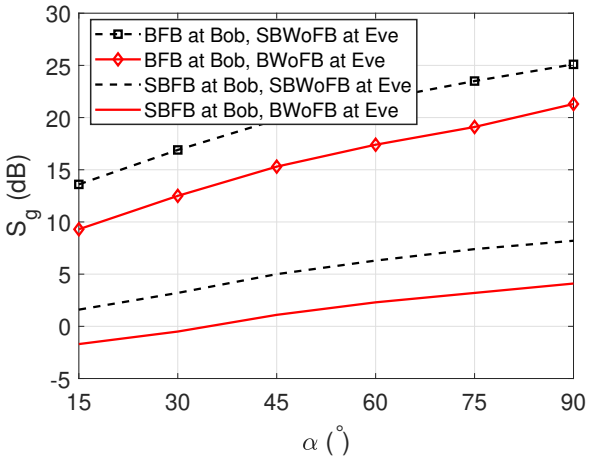


(b) ρ_{BE} versus α with $d_{AE} = 6$ m.

Fig. 8: ρ_{BE} versus d_{AE}, α in case of passive eavesdropper, $S_g = 0$ dB.



(a) S_g versus d_{AE} with $\alpha = 30°$.



(b) S_g versus α with $d_{AE} = 6$ m.

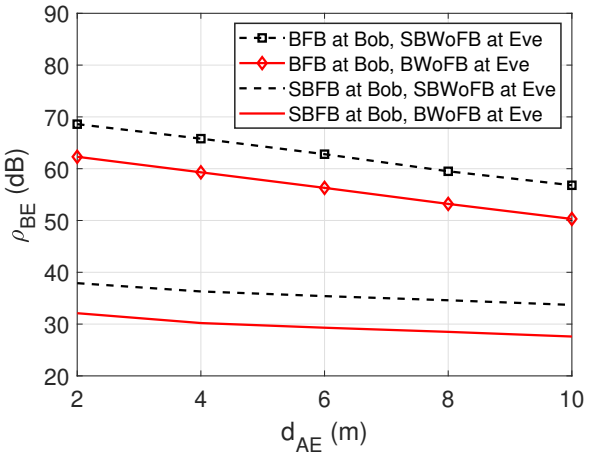
Fig. 9: S_g versus d_{AE}, α in case of active eavesdropper, $\rho_{BE} = \rho_{EB} = \rho_{BB} = \rho_{EE} = 35$ dB.

Consequently, regardless of Eve's location, using a BFB mechanism at Bob in the situation of a passive eavesdropper provides a benefit in terms of not only ensuring security and reliability factors but also maintaining power usage. This feature can be used in IoT transmissions and green communications.

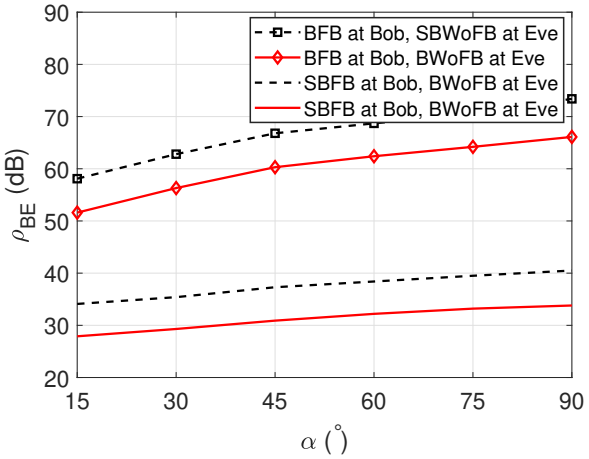
C. In Case of Active Eavesdropper

Fig. 9 shows the security gap S_g versus the distance between Alice and Eve d_{AE} and the angle α in case of active eavesdropper. The self-jamming to noise ratios from Bob to Eve ρ_{BE} and vice versa, ρ_{EB} are both set up at 35 dB. While the self-interference to noise ratio at each user, ρ_{BB} and ρ_{EE} are also set up at 35 dB. The BFB/SBFB schemes are implemented on Bob's receiver side, whereas Eve uses the conventional BWoFB/SBWoFB scheme. First, Fig. 9a shows S_g versus the distance d_{AE} when $\alpha = 30°$. It can be seen that S_g will decrease when d_{AE} increases and using SBFB scheme at Bob gives better results than BFB scheme. Indeed, S_g is small and can go nearly to 0 or below 0 dB if SBFB scheme is applied at Bob and BWoFB scheme is applied at Eve. In contrast, S_g can only achieve to 8 dB or 12 dB when using BFB scheme at Bob at $d_{AE} = 10$ m. According to the results in Figure 9b, when d_{AE} is set up at 6 m and try to vary α from 15 to 90°, the security gap S_g also increases when Eve is moved far away to Bob (d_{BE} increases). The SBFB at Bob curves, on the other hand, has a smaller slope than the BFB at Bob curves. In particular, it only increases about 5-6 dB when using SBFB at Bob compared to nearly 12 dB when using BFB at Bob, which means that changing the angle α has less of an effect on the security factor if semi-blind scheme at Bob is used, regardless of BWoFB/SBWoFB schemes at Eve.

Fig. 10 shows the self-jamming to noise ratio from Bob to Eve ρ_{BE} versus the distance between Alice and Eve d_{AE} and the angle α in case of active eavesdropper. In this scenario, the self-jamming to noise ratio from Eve to Bob ρ_{EB} is set at 35 dB, the self-interference to noise ratio at each user, ρ_{BB} and ρ_{EE} are also fixed at 35 dB and the security gap S_g is fixed at 0 dB. In Fig. 10a, when α is fixed at 30° and we try to change d_{AE}, it shows that increasing d_{AE}, which means Eve will move far away Alice, will lead to decrease ρ_{BE} and semi-blind scheme needs smaller ρ_{BE} than blind scheme at Bob, regardless the usage of BWoFB/SBWoFB schemes at Eve, i.e., around 28-34 dB compared to 50-56 dB at $d_{AE} = 10$ m. Moreover, in Figure 10b, when we try to vary α from 15 to 90° and fix d_{AE} at 6 m, the obtained results highlight the benefits of using SBFB scheme at Bob, particularly when its slope is smaller than that of the BFB curve, whether conventional BWoFB/SBWoFB are used at Eve. It means that when Bob



(a) ρ_{BE} versus d_{AE} with $\alpha = 30°$.



(b) ρ_{BE} versus α with $d_{AE} = 6$ m.

Fig. 10: ρ_{BE} versus d_{AE}, α in case of active eavesdropper, $S_g = 0$ dB.

uses the SBFB scheme, he can save the power of the self-jamming signal, i.e Bob needs maximum $\rho_{BE} = 40$ dB to ensure $S_g = 0$ dB when $\alpha = 90°$ if semi-blind scheme is applied. If blind scheme is used, it needs minimum around $\rho_{BE} = 65$ dB to ensure the reliability and security factors.

Therefore, it has become more important than ever for Bob to use SBFB scheme to ensure the security and reliability factors as well as improve the power consumption factor, regardless of location of eavesdropper Eve.

IV. Conclusion

The secrecy coding in short-packet FD wiretap transmission has been studied by evaluating the security gap S_g performance with different localizations of both passive and active eavesdroppers. This study shows how the reliability and security parameters in PLS are considerably impacted by the power of the self-jamming signal. The use of a blind and semi-blind iterative algorithms in passive scenario and in active scenario, respectively, illustrates the robustness in comparison to the conventional method, in terms of the security gap S_g and the self-jamming power from Bob (ρ_{BE}) regardless of the positions of the eavesdropper. Consequently, it is highly advisable to use joint iterative blind or semi-blind algorithms at the authorized receiver to enhance security while maintaining power consumption in the context of short-packet FD wiretap transmission (IoT applications and green communications).

Acknowledgment

This research is supported by the IBNM (Brest Institute of Computer Science and Mathematics) CyberIoT Chair of Excellence at the University of Brest.

References

[1] B. V. Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 131–137, 2018.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, pp. 1355–1387, 1975.

[3] L. H. Ozarow and A. D. Wyner, "Wire-tap channel ii," *Bell System Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[4] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "Ldpc codes for the gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

[5] Y. Liu, X. Zhu, E. G. Lim, Y. Jiang, and Y. Huang, "Fast iterative semi-blind receiver for urllc in short-frame full-duplex systems with cfo," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 839–853, 2019.

[6] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Transactions on Signal Processing*, vol. 63, no. 23, pp. 6285–6298, 2015.

[7] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[8] Z. Dryer, A. Nickerl, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Full-Duplex Jamming for Enhanced Hidden-Key Secrecy," in *IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.

[9] N. Arı, N. Thomos, and L. Musavian, "Active eavesdropping in short packet communication: Average secrecy throughput analysis," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.

[10] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679 –695, 2018.

[11] J. H. Bae, A. Abotabl, H. P. Lin, K. B. Song, and J. Lee, "An overview of channel coding for 5G NR cellular communications," *Transactions on Signal and Information Processing*, vol. 8, no. 17, 2019.

[12] B. Macro, M. Nicola, R. Giocomo, and C. Franco, "Security gap analysis of some ldpc coded transmission schemes over the flat and fast fading gaussian wire-tap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 15, no. 232, 10 2015.

[13] J. Du, "A partially coupled ldpc coded scheme for the gaussian wiretap channel," *IEEE Communications Letters*, vol. 24, no. 1, pp. 7–10, 2020.

[14] B. Q. Vuong, R. Gautier, A. Fiche, M. Marazin, H. Q. Ta, and L. L. Nguyen, "Joint iterative blind self-interference cancellation, propagation channel estimation and decoding processes in full-duplex transmissions," *IEEE Access*, vol. 10, pp. 22 795–22 807, 2022.

[15] B. Q. Vuong, R. Gautier, H. Q. Ta, L. L. Nguyen, A. Fiche, and M. Marazin, "Joint semi-blind self-interference cancellation and equal-isationprocesses in 5g qc-ldpc-encoded short-packet full-duplex trans-missions," *Sensors*, vol. 22, no. 6, 2022.

[16] B. Q. Vuong, R. Gautier, A. Fiche, M. Marazin, and D.-S. Cristina, "Secrecy coding analysis of short packet full-duplex transmis- sions with joint iterative channel estimation and decoding processes," *Sensors*, vol. 22, no. 14, 2022.

[17] G. Liu, W. Feng, Z. Han, and W. Jiang, "Performance analysis and optimization of cooperative full-duplex d2d communication underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5113–5127, 2019.

[18] T. Kim, M. Kyungsik, and S. Park, "Self-interference channel training for full-duplex massive mimo systems," *Sensors*, vol. 21, no. 9, 2021.

[19] S. Haykin, *Adaptive filter theory*. Pearson, 1993, vol. 29.

[20] E. Sharon, S. Litsyn, and J. Goldberger, "An efficient message-passing schedule for LDPC decoding," *IEEE Convention of Electrical and Electronics Engineers in Israel, Proceedings*, no. 4, pp. 223–226, 2004.

[21] *Guidelines for evaluation of radio transmission technologies for IMT-2000*, International Telecommunication Union, 1997.