Received: 19 December 2018 | Revised: 1 April 2019 | Accepted: 28 April 2019

DOI: 10.4218/etrij.2018-0688

ORIGINAL ARTICLE

ETRI Journal WILEY

Information leakage in bi-directional IFD communication system with simultaneously transmitted jamming sequence

Hyungsik Ju | Donghyuk Gwak | Tae-Joong Kim

Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea

Correspondence
Hyungsik Ju, Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea.
Email: jugun@etri.re.kr

Funding information
Korea Government, Grant/Award Number: 19ZH1600

In this paper, we describe a simultaneously transmitted jamming (ST-jamming) for bi-directional in-band full-duplex (IFD) system to improve information security at the physical layer. By exploiting ST-jamming, each legitimate user transmits data samples and jamming samples together in one orthogonal frequency division multiplexing symbol according to given traffic asymmetry. Regardless of the traffic difference in both directions in IFD communication, eavesdropping of confidential information is prevented in both directions simultaneously without the loss of data rate. We first propose an encoding scheme and the corresponding decoding scheme for ST-jamming to be used by the legitimate users. In addition, we study a transceiver structure of the legitimate users including a baseband modem uniquely designed for the use of ST-jamming. The leakage of confidential information at an eavesdropper is then quantified by studying the mutual information between the confidential transmit signals and the received signals of the eavesdropper. Simulation results show that the proposed ST-jamming significantly reduces the leakage of legitimate information at the eavesdropper.

KEYWORDS
in-band full-duplex, jamming, mutual information, physical layer security, traffic asymmetry

1 | INTRODUCTION

In-band full duplex (IFD) enables *simultaneous transmission and reception (STR) of radio frequency signals at the same frequency band* (referred to as *in-band STR* hereafter) by cancelling self-interference (SI). Recent advances in SI cancellation (SIC) technologies have made it possible to reduce the residual SI after SIC to the level of background noise [1–4]. Owing to state-of-the-art SIC technologies, the spectral efficiency of IFD communication is shown to improve up to twice as much as that in conventional half-duplex (HD) communications.

In-band STR enabled by IFD has motivated studies applying IFD to the area of physical layer security (PHYSEC). In a multiuser environment, the in-band STR of an IFD is generally known to degrade network performance, despite the benefit of doubling the spectral efficiency of a transmission link. This is because the in-band STR in a multiuser environment causes co-channel interference (CCI) between communicating users [5], or between a backhaul link and an access link [6]. However, from a PHYSEC perspective, the CCI yielded by the in-band STR of IFD can be used to protect the information of legitimate users from eavesdropping [7–19]. As studied in [7–9], a legitimate receiver operating in IFD can transmit a jamming signal while receiving the information transmitted from a legitimate transmitter. When the information of the legitimate transmitter is received by an eavesdropper, this jamming signal causes CCI on the receive (Rx) signal of the eavesdropper, preventing the legitimate information from being eavesdropped. In [10–13], IFD is applied in a bi-directional IFD (BD-IFD) communication environment where two legitimate users operating in IFD exchange their data. In this case, the transmit (Tx) signals of the two IFD legitimate users are received by an eavesdropper simultaneously. Therefore, the Tx signal of a legitimate user acts as a jamming signal that prevents the information transmitted by another legitimate user from being eavesdropped, and vice versa. Furthermore, the system level performance with the IFD-aided PHYSEC was analyzed using stochastic geometry with various system setups [14–17]. In the presence of an adversary exploiting IFD for both eavesdropping and jamming attack simultaneously, [18] and [19] studied strategies to maximize the secrecy capacity by minimizing the effects of the jamming attack.

In the previous studies [10–17] dealing with PHYSEC in BD-IFD communications, it was assumed that the data traffic is the same in both directions of IFD communication links (ie, it is symmetric). However, for practical bi-directional data communication services, the data traffic is typically different in the two directions of data links that is it is asymmetric. As reported in [20], which analyzes the traffic of downlink (DL) and uplink (UL) in cellular environment, the DL traffic accounts for 66%–95% of the entire data traffic, whereas the UL traffic accounts for only 5%–33%. In BD-IFD communications, the problem caused by such a traffic asymmetry is even more critical. This is because, in IFD communication, time and frequency resources allocated to the two data transmission links are always the same. When traffic in the two directions of data links in BD-IFD communication is asymmetric, a part of the resources available in the link carrying less traffic cannot be used for data transmission and are thus wasted. This results in significant degradation of the gain in spectral efficiency caused by the in-band STR [21–23]. In the scenario considered in [10–17], given a traffic asymmetry resulting in a waste of resources in one of the two links, the previous studies provided no guidance as to how to use these remaining resources and how the corresponding performance changes in this case.

To tackle the problem resulting from such a traffic asymmetry, in this paper, we propose a scheme referred to as simultaneously transmitted jamming (ST-jamming). The proposed scheme is to be used for BD-IFD communication between two legitimate users that exchange different amounts of confidential information with each other through orthogonal-frequency division multiplexing (OFDM) modulation in the presence of an eavesdropper. To prevent eavesdropping, each legitimate user transmits a jamming sequence using a part of the total available resources given to it that remain unused for data transmission owing to the traffic asymmetry. To this end, we propose a method in which each legitimate user transmits data samples and jamming samples together in one OFDM symbol according to the given traffic asymmetry. In addition to the CCI occurring in the Rx signal of the eavesdropper owing to the in-band STR of the two legitimate users, the jamming samples inserted into each OFDM symbol further improve PHYSEC.

In particular, the proposed scheme is effective for protecting the information of the link transmitting more traffic in BD-IFD communication. Consider a part of the resources that are not used for data transmission on the link carrying less traffic. Information transmitted using these resources on the link that carries greater traffic cannot be protected from eavesdropping because it is received by the eavesdropper without any CCI. In contrast, in the proposed scheme, all the resources in both links are used to transmit either information or jamming signals, regardless of the amount of traffic. Therefore, the Rx signals of the eavesdropper received from both directions always undergo interference, and the information on the link carrying greater traffic can also be protected from eavesdropping.

The main contributions of this paper are summarized as follows. We first propose encoding and decoding schemes for ST-jamming to be used by the legitimate users. In addition, we study a transceiver structure of the legitimate users including a baseband modem uniquely designed for the use of ST-jamming. The operations of an eavesdropper for wiretapping the information of legitimate users are then described. Based on these operations, we analyze the amount of information of the legitimate users that is leaked to the eavesdropper. Finally, to show the effectiveness of ST-jamming, the amount of information leaked is demonstrated quantitatively through simulations.

TABLE 1 Nomenclatures

HD	Half-duplex
IFD	In-band full-duplex
CCI	Co-channel interference
SI	Self-interference
SIC	Self-interference cancellation
PHYSEC	Physical layer security
OFDM	Orthogonal-frequency division multiplexing
CP	Cyclic prefix
FFT	Fast Fourier transform
IFFT	Inverse fast Fourier transform
DL	Downlink
UL	Uplink
CSCG	Circularly symmetric complex Gaussian
i.i.d	Independent and identically distributed

Table 1 shows the nomenclatures used in this paper. Here, $\mathbf{I}_N$ and $\mathbf{0}_N$ indicate an $N \times N$ identity matrix and $N \times 1$ zero vector, respectively. A diagonal matrix whose diagonal entries consist of a vector $\mathbf{x}$ is denoted by diag($\mathbf{x}$). In addition, $\text{FFT}_N(\cdot)$ and $\text{IFFT}_N(\cdot)$ represent the N-point FFT and IFFT, respectively. Furthermore, $\mathcal{CN}(\boldsymbol{\nu}, \boldsymbol{\Sigma})$ denotes the distribution of CSCG random vector, whose mean vector and covariance matrix are given by $\boldsymbol{\nu}$ and $\boldsymbol{\Sigma}$, respectively. Finally, $\mathbb{E}[\cdot]$ and ϕ represent statistical expectation and an empty set, respectively.

2 | SYSTEM MODEL

Figure 1 shows the PHYSEC system considered in this study. This system consists of two single-antenna legitimate users and a single-antenna eavesdropper. The two legitimate users are denoted as *Alice* and *Bob*, whereas the eavesdropper is denoted by *Eve*. Alice and Bob operate in IFD for BD-IFD communication. In contrast, Eve operates in HD and only receives the signals transmitted by Alice and Bob to wiretap their confidential information.

Recent advances in SIC technologies have shown that the residual SI after SIC in an IFD transceiver can reach the level of the background noise (hereafter denoted by *perfect SIC*) [1–4]. In particular, the SIC techniques in [1] and [2] designed for IFD communication based on OFDM modulation remove the SI directly from the time-domain Rx signal between the baseband (BB) OFDM Tx modem and BB OFDM Rx modem of the IFD transceiver, as shown in Figure 2.[1] This allows the SIC functionality to be isolated from the BB Tx modem and the BB Rx modem so that the SIC function operates independently of the operations of these modems. In other words, the SIC block can be implemented between the BB Tx modem and BB Rx modem without any modification of structures or functions of these modems. Hereafter, we assume that the SIC techniques in [1] and [2] are exploited at the IFD transceivers of both Alice and Bob to remove the SI in time domain between the BB Tx modem and BB Rx modem. Furthermore, perfect SIC is assumed at both Alice and Bob, and hence, the effect of SI is neglected.

Alice and Bob are required to transmit M_a and M_b data symbols, respectively, according to their respective traffic requirements. The M_a data symbols of Alice and the M_b data symbols of Bob are transmitted through time-domain Tx signals denoted by vectors $\mathbf{x}_\text{a}$ and $\mathbf{x}_\text{b}$, respectively. Both $\mathbf{x}_\text{a}$ and $\mathbf{x}_\text{b}$ consist of N time samples, where $N \geq M_\text{a}$ and $N \geq M_\text{b}$. For both $\mathbf{x}_\text{a}$ and $\mathbf{x}_\text{b}$, some of the N time samples correspond to data samples, whereas the rest correspond to jamming samples.

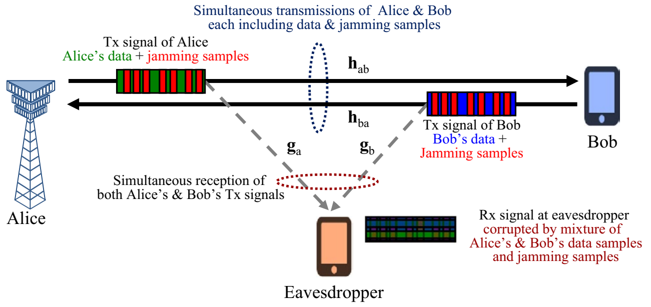
Simultaneous transmissions of Alice & Bob
each including data & jamming samples
Tx signal of Alice
Alice's data + jamming samples
$\mathbf{h}_\text{ab}$
$\mathbf{h}_\text{ba}$
$\mathbf{g}_\text{a}$
$\mathbf{g}_\text{b}$
Tx signal of Bob
Bob's data +
Jamming samples
Bob
Alice
Simultaneous reception of
both Alice's & Bob's Tx signals
Rx signal at eavesdropper
corrupted by mixture of
Alice's & Bob's data samples
and jamming samples
Eavesdropper

FIGURE 1 System model

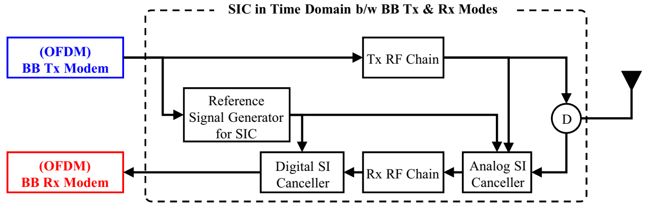

FIGURE 2 IFD transceiver for in-band STR utilizing time-domain SIC

The data samples of $\mathbf{x}_\text{a}$ are used to transmit M_a data symbols of Alice, whereas those of $\mathbf{x}_\text{b}$ are used to transmit M_b data symbols of Bob.

In Figure 1, impulse responses of the wireless channels from/to Alice to/from Bob are denoted by $\mathbf{h}_\text{ab}$ and $\mathbf{h}_\text{ba}$, respectively. Furthermore, the impulse responses of the wireless channels from Alice and Bob to Eve are denoted as $\mathbf{g}_\text{a}$ and $\mathbf{g}_\text{b}$, respectively. It is assumed that Alice and Bob have perfect information of $\mathbf{h}_\text{ba}$ and $\mathbf{h}_\text{ab}$, respectively, whereas they both have no information of either $\mathbf{g}_\text{a}$ or $\mathbf{g}_\text{b}$. In contrast, Eve has perfect information of both $\mathbf{g}_\text{a}$ and $\mathbf{g}_\text{b}$, whereas it has no information of either $\mathbf{h}_\text{ba}$ or $\mathbf{h}_\text{ab}$.

Assuming perfect SIC at both Alice and Bob, the BB equivalent expressions of the Rx signals at Alice and Bob are given, respectively, by

$$\begin{aligned}\mathbf{y}_\text{a} &= \mathbf{h}_\text{ba} \times \mathbf{x}_\text{b} + \mathbf{z}_\text{a},\\ \mathbf{y}_\text{b} &= \mathbf{h}_\text{ab} \times \mathbf{x}_\text{a} + \mathbf{z}_\text{b},\end{aligned} \tag{1}$$

with $\mathbf{z}_\text{a}$ and $\mathbf{z}_\text{b}$ denoting the received noise vectors at Alice and Bob, respectively, where $\mathbf{z}_\text{a} \sim \mathcal{CN}(\mathbf{0}_N, \sigma_\text{a}\mathbf{I}_N)$ and $\mathbf{z}_\text{b} \sim \mathcal{CN}(\mathbf{0}_N, \sigma_\text{b}\mathbf{I}_N)$. Furthermore, the BB equivalent expression of the Rx signal at Eve is given by

$$\mathbf{y}_\text{e} = \mathbf{g}_\text{a} \times \mathbf{x}_\text{a} + \mathbf{g}_\text{b} \times \mathbf{x}_\text{b} + \mathbf{z}_\text{e}, \tag{2}$$

with $\mathbf{z}_\text{e}$ denoting the received noise vector at Eve, where $\mathbf{z}_\text{e} \sim \mathcal{CN}(\mathbf{0}_N, \sigma_\text{e}\mathbf{I}_N)$. Owing to the in-band STR of both Alice and Bob, as shown in (2), transmission of $\mathbf{x}_\text{a}$ by Alice acts as a CCI when Eve receives $\mathbf{x}_\text{b}$ transmitted by Bob, and vice versa. This helps to protect the confidential information of both Alice and Bob in the physical layer. In addition, the

[1] These SIC techniques remove the SI between the OFDM BB Tx and Rx modems of an IFD transceiver by using a preamble inserted in front of the data symbols to be transmitted. Please refer to [1] and [2] for details of these SIC techniques.

jamming samples included in $\mathbf{x}_{\mathrm{a}}$ and $\mathbf{x}_{\mathrm{b}}$ help further improving PHYSEC.

3 | ENCODING AND DECODING AT LEGITIMATE USERS

In this section, we study an encoding scheme and the corresponding decoding scheme for ST-jamming at the legitimate users for given values of N, M_{a}, and M_{b}. As assumed in Section 2, SIC is performed independently of the operations of the BB Tx and BB Rx modems by exploiting the SIC technology in [1] and [2]. Therefore, we focus only on the encoding in the BB Tx modem and the decoding in the BB Rx modem for ST-jamming without detailed description of SIC.

Alice and Bob share a common lookup table $\mathcal{T}$ in which each row consists of different permutations of time sample indices (ie, $0 \sim N-1$). The set of time sample indices in the i-th row of $\mathcal{T}$ is denoted by $\boldsymbol{\tau}_i = \{\tau_i(0), \ldots, \tau_i(N-1)\}$.

Before Alice and Bob transmit their respective Tx signals, they exchange $(M_{\mathrm{a}}, i_{\mathrm{a}})$ and $(M_{\mathrm{b}}, i_{\mathrm{b}})$, which are sets of two nonnegative numbers, respectively. Based on the knowledge of M_{a}, M_{b}, i_{a}, and i_{b}, both Alice and Bob generate four sets

$$\begin{aligned}\mathcal{D}_l &= \{d_l(0), \ldots, d_l(M_l-1)\}, \quad l \in \{\mathrm{a}, \mathrm{b}\},\\ \mathcal{J}_l &= \{j_l(0), \ldots, j_l(N-M_l-1)\}, \quad l \in \{\mathrm{a}, \mathrm{b}\},\end{aligned} \tag{3}$$

subject to $(\mathcal{D}_{\mathrm{a}} \cap \mathcal{J}_{\mathrm{a}}) = (\mathcal{D}_{\mathrm{b}} \cap \mathcal{J}_{\mathrm{b}}) = \phi$ and $(\mathcal{D}_{\mathrm{a}} \cup \mathcal{J}_{\mathrm{a}}) = (\mathcal{D}_{\mathrm{b}} \cup \mathcal{J}_{\mathrm{b}}) = \{0, \ldots, N-1\}$. For this purpose, each element of $\mathcal{D}_{\mathrm{a}}$, $\mathcal{D}_{\mathrm{b}}$, $\mathcal{J}_{\mathrm{a}}$, and $\mathcal{J}_{\mathrm{b}}$ is given, respectively, by

$$\begin{aligned}d_l(n) &= \tau_{i_l}(n), \quad 0 \le n \le M_l - 1, \quad l \in \{\mathrm{a}, \mathrm{b}\},\\ j_l(n) &= \tau_{i_l}(n+M_l), \quad 0 \le n \le N - M_l - 1, \quad l \in \{\mathrm{a}, \mathrm{b}\}.\end{aligned} \tag{4}$$

Note that the encoding and decoding processes at Alice and Bob are equivalent. Therefore, in this section, we only address the encoding and decoding processes at Alice for the simplicity of presentation.

3.1 | Encoding legitimate transmit signal

Figure 3 shows the operations in the BB Tx modem at Alice to generate the time-domain Tx signal $\mathbf{x}_{\mathrm{a}}$ including both data and jamming samples. First, M_{a} data symbols are generated in frequency domain as $\mathbf{W}_{\mathrm{a}} = [W_{\mathrm{a}}(0), \ldots, W_{\mathrm{a}}(M_{\mathrm{a}}-1)]^T$, where $\mathbb{E}[|W_{\mathrm{a}}(i)|^2] = P_{\mathrm{a}}$, $\forall i = 0, \ldots, M_{\mathrm{a}}-1$. From $\mathbf{W}_{\mathrm{a}}$, we have $\mathbf{w}_{\mathrm{a}} = [w_{\mathrm{a}}(0), \ldots, w_{\mathrm{a}}(M_{\mathrm{a}}-1)]^T$, obtained as

$$\mathbf{w}_{\mathrm{a}} = \mathrm{IFFT}_{M_{\mathrm{a}}}(\mathbf{W}_{\mathrm{a}}) = \mathbf{A}_{M_{\mathrm{a}}}\mathbf{W}_{\mathrm{a}}, \tag{5}$$

with $\mathbf{A}_M$ denoting an M-point IFFT matrix whose element at the i-th row and k-th column, $A_M(i,k)$, is given by

$$A_M(i,k) = \frac{1}{\sqrt{M}} e^{j\frac{2\pi}{M}ik}, \quad \forall i, k = 0, \ldots, M-1. \tag{6}$$

Then, $\mathbf{x}_{\mathrm{a}}$ is generated with a mixture of $\mathbf{w}_{\mathrm{a}}$ given in (5) and the jamming sequence given by $\mathbf{q}_{\mathrm{a}} = [q_{\mathrm{a}}(0), \ldots, q_{\mathrm{a}}(N-M_{\mathrm{a}}-1)]^T$. Using $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{J}_{\mathrm{a}}$ given in (3) and (4), $\mathbf{x}_{\mathrm{a}} = [x_{\mathrm{a}}(0), \ldots, x_{\mathrm{a}}(N-1)]^T$ is obtained from $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{q}_{\mathrm{a}}$ as

$$x_{\mathrm{a}}(k) = \begin{cases} w_{\mathrm{a}}(i), & \text{if } k \in \mathcal{D}_{\mathrm{a}} \text{ and } k = d_{\mathrm{a}}(i),\\ q_{\mathrm{a}}(i), & \text{if } k \in \mathcal{J}_{\mathrm{a}} \text{ and } k = j_{\mathrm{a}}(i).\end{cases} \tag{7}$$

As shown in (7), $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{J}_{\mathrm{a}}$ represent sets of indices through which $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{q}_{\mathrm{a}}$ are inserted into $\mathbf{x}_{\mathrm{a}}$, respectively.

Lemma 1 (Distribution of time-domain OFDM signal)With $N \to \infty$, the statistical distribution of $\mathbf{w}_{\mathrm{a}}$ is given by $\mathbf{w}_{\mathrm{a}} \sim \mathcal{CN}(\mathbf{0}_{M_{\mathrm{a}}}, P_{\mathrm{a}}\mathbf{I}_{M_{\mathrm{a}}})$.

Proof. Please refer to [24]. ■

Proposition 1 (Distribution of jamming sequence)With $\mathbf{q}_{\mathrm{a}} \sim \mathcal{CN}(\mathbf{0}_{N-M_{\mathrm{a}}}, P_{\mathrm{a}}\mathbf{I}_{N-M_{\mathrm{a}}})$, $\mathbf{x}_{\mathrm{a}}$ obtained using (7) is observed to be a single CSCG sequence.

Proof. From Lemma 1, $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{q}_{\mathrm{a}}$ are statistically identical when $\mathbf{q}_{\mathrm{a}}$ is set to be $\mathbf{q}_{\mathrm{a}} \sim \mathcal{CN}(\mathbf{0}, P_{\mathrm{a}}\mathbf{I}_{N-M_{\mathrm{a}}})$. As $\mathbf{x}_{\mathrm{a}}$ is a mixture of two statistically identical sequences $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{q}_{\mathrm{a}}$, the distributions of $\mathbf{w}_{\mathrm{a}}$, $\mathbf{q}_{\mathrm{a}}$, and $\mathbf{x}_{\mathrm{a}}$ are statistically identical. ■

The generation of $\mathbf{x}_{\mathrm{a}}$ according to Proposition 1 makes it difficult to distinguish the data part in $\mathbf{x}_{\mathrm{a}}$ from the jamming part in $\mathbf{x}_{\mathrm{a}}$. After $\mathbf{x}_{\mathrm{a}}$ is generated, CP is added as in conventional OFDM systems, and then transmitted to Bob.[2] At Bob, $\mathbf{x}_{\mathrm{b}}$ is generated through the same procedures in (5)–(7), with M_{a}, $\mathbf{W}_{\mathrm{a}}$, $\mathcal{D}_{\mathrm{a}}$, and $\mathcal{J}_{\mathrm{a}}$ replaced by M_{b}, $\mathbf{W}_{\mathrm{b}}$, $\mathcal{D}_{\mathrm{b}}$, and $\mathcal{J}_{\mathrm{b}}$, respectively.

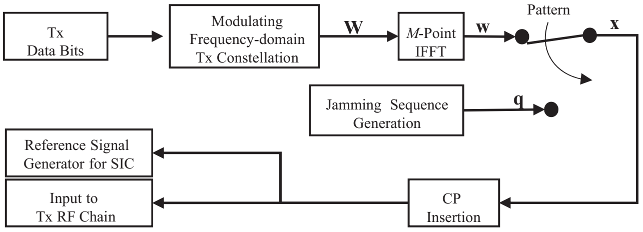

FIGURE 3 Operations in baseband Tx modem at Alice and Bob

3.2 | Decoding legitimate receive signal

Figure 4 shows the operations in the BB Rx modem at Alice to obtain the data symbols transmitted by Bob by removing

[2] Strictly speaking, the number of time samples in $\mathbf{x}_{\mathrm{a}}$ is $N + N_{\mathrm{CP}}$, where N_{CP} denotes the number of time samples included in CP. However, for notational brevity, N_{CP} is ignored later hereafter as in Equation and .

the jamming samples from $\mathbf{y}_\mathrm{a}$.[3] By applying N-point FFT, the frequency-domain representation of $\mathbf{y}_\mathrm{a}$ in (1) is attained as

$$\mathbf{Y}_\mathrm{a} = \mathbf{H}_\mathrm{ba}\mathbf{X}_\mathrm{b} + \mathbf{Z}_\mathrm{b}, \tag{8}$$

where $\mathbf{H}_\mathrm{ba} = \mathrm{diag}([H_\mathrm{ab}(0), \ldots, H_\mathrm{ab}(N-1)]^T)$ is a diagonal matrix whose diagonal entries consist of

$$\left[H_\mathrm{ab}(0), \ldots, H_\mathrm{ab})(N-1)\right]^T = \mathrm{FFT}_N(\mathbf{h}_\mathrm{ba}). \tag{9}$$

Furthermore, $\mathbf{X}_\mathrm{b}$ and $\mathbf{Z}_\mathrm{a}$ are given, respectively, by

$$\begin{aligned} \mathbf{X}_\mathrm{b} &= \mathbf{B}_N\mathbf{x}_\mathrm{b}, \\ \mathbf{Z}_\mathrm{a} &= \mathbf{B}_N\mathbf{z}_\mathrm{a}, \end{aligned} \tag{10}$$

where $\mathbf{B}_N$ denotes the N-point FFT matrix whose element at the i-th row and k-th column, $B_N(i,k)$, is given by

$$B_N(i,k) = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{N}ik}, \quad \forall i,k = 0, \ldots, N-1. \tag{11}$$

We have $\mathbf{Z}_\mathrm{a} \sim \mathcal{CN}(\mathbf{0}_N, \sigma_\mathrm{a}\mathbf{I}_N)$ because FFT of a CSCG random sequence is still a CSCG random sequence with the same statistical properties. Based on the knowledge of $\mathbf{H}_\mathrm{ba}$, the effect of the wireless channel is equalized in frequency domain as

$$\tilde{\mathbf{Y}}_\mathrm{a} = \mathbf{H}_\mathrm{ba}^{-1}\mathbf{Y}_\mathrm{a} = \mathbf{X}_\mathrm{b} + \tilde{\mathbf{Z}}_\mathrm{a}, \tag{12}$$

where $\tilde{\mathbf{Z}}_\mathrm{a} = \mathbf{H}_\mathrm{ba}^{-1}\mathbf{Z}_\mathrm{a}$. For the channel-equalized Rx signal $\tilde{\mathbf{Y}}_\mathrm{a}$ in (12), we can obtain the time-domain expression as

$$\tilde{\mathbf{y}}_\mathrm{a} = \mathbf{A}_N\tilde{\mathbf{Y}}_\mathrm{a} = \mathbf{x}_\mathrm{b} + \tilde{\mathbf{z}}_\mathrm{a}, \tag{13}$$

with $\tilde{\mathbf{z}}_\mathrm{a} = \mathbf{A}_N\tilde{\mathbf{Z}}_\mathrm{a}$. By removing the jamming samples from $\tilde{\mathbf{y}}_\mathrm{a}$ in (13) based on the knowledge of $\mathcal{D}_\mathrm{b}$, we have $\bar{\mathbf{y}}_\mathrm{a} = [\bar{y}_\mathrm{a}(0), \ldots, \bar{y}_\mathrm{a}(M_\mathrm{b}-1)]^T$, where

$$\begin{aligned} \bar{y}_\mathrm{a}(k) &= \tilde{y}_\mathrm{a}(i), && \text{if } i = d_\mathrm{b}(k) \in \mathcal{D}_\mathrm{b}, \\ &= x_\mathrm{b}(i) + \tilde{z}_\mathrm{a}(i), && \text{if } i = d_\mathrm{b}(k) \in \mathcal{D}_\mathrm{b}, \\ &= w_\mathrm{b}(k) + \bar{z}_\mathrm{a}(k). \end{aligned} \tag{14}$$

We denote $\bar{\mathbf{z}}_\mathrm{a} = [\bar{z}_\mathrm{a}(0), \ldots, \bar{z}_\mathrm{a}(M_\mathrm{b}-1)]^T$ with $\bar{z}_\mathrm{a}(k)$'s given in (14). Then, we can obtain the frequency-domain data symbols transmitted by Bob, $\mathbf{W}_\mathrm{b} = [W_\mathrm{b}(0), \ldots, W_\mathrm{b}(M_\mathrm{b}-1)]^T$, as

$$\bar{\mathbf{Y}}_\mathrm{a} = \mathbf{B}_{M_\mathrm{b}}\bar{\mathbf{y}}_\mathrm{a} = \mathbf{W}_\mathrm{b} + \bar{\mathbf{Z}}_\mathrm{a}, \tag{15}$$

where $\bar{\mathbf{Z}}_\mathrm{a} = \mathbf{B}_{M_\mathrm{b}}\bar{\mathbf{z}}_\mathrm{a}$. Note that $\mathbf{W}_\mathrm{b}$ can only be recovered properly from $\mathbf{y}_\mathrm{a}$ if M_b and $\mathcal{D}_\mathrm{b}$ are perfectly known. Although $\mathbf{x}_\mathrm{b}$ is also received by Eve as in (2), the jamming sequences included in $\mathbf{x}_\mathrm{b}$ prevent the recovery of $\mathbf{W}_\mathrm{b}$ at Eve, unless Eve does not have perfect knowledge of both M_b and $\mathcal{D}_\mathrm{b}$. The frequency-domain data symbols transmitted by Alice, $\mathbf{W}_\mathrm{a}$, can be obtained equivalently from (8)–(15) at Bob, with $\mathbf{y}_\mathrm{b}$, M_b, and $\mathcal{D}_\mathrm{b}$ replaced by $\mathbf{y}_\mathrm{a}$, M_a, and $\mathcal{D}_\mathrm{a}$, respectively.

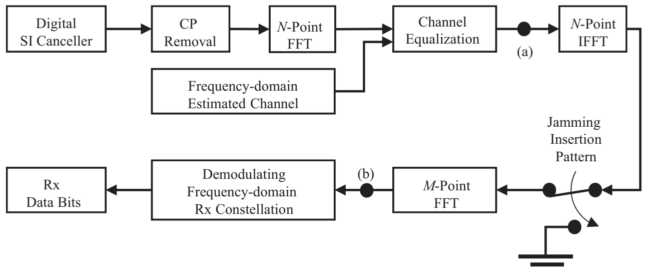
Digital SI Canceller
CP Removal
N-Point FFT
Channel Equalization
(a)
N-Point IFFT
Frequency-domain Estimated Channel
Jamming Insertion Pattern
Rx Data Bits
Demodulating Frequency-domain Rx Constellation
(b)
M-Point FFT

FIGURE 4 Operations in baseband Rx modem at Alice and Bob

Remark In this section, for the purpose of generalization, the proposed ST-jamming scheme is described for the general values M_a and M_b. However, the proposed scheme is particularly valid for a special case where the asymmetry between the traffic of Alice and the traffic of Bob is given such that $M_\mathrm{a} = N$ and $M_\mathrm{b} < N$. In this case, $N - M_\mathrm{b}$ jamming samples are inserted only in $\mathbf{x}_\mathrm{b}$ but no jamming sample is inserted in $\mathbf{x}_\mathrm{a}$. Therefore, both Alice and Bob can transmit all of their required data traffic without loss of data rate.

4 | EAVESDROPPING AND LEAKAGE OF INFORMATION AT EAVESDROPPER

In this section, we first describe the operations at Eve undertaken to wiretap the confidential information of Alice and Bob. We then quantify the leakage of the confidential information of the legitimate users at Eve. Note that the Rx operations of Eve undertaken to eavesdrop on the confidential information transmitted by Alice are equivalent to those undertaken to eavesdrop on the confidential information transmitted by Bob. Therefore, in this section, we study the Rx operations of Eve and the corresponding information leakage only for the case where Eve attempts to eavesdrop on Alice's confidential information.

4.1 | Receiver structure and operations of eve

The receiver structure of Eve is similar to that shown in Figure 4, but there are several differences. First, "Digital SI Canceller" in Figure 4 is not implemented because Eve only receives the signals transmitted from Alice and Bob without transmitting its own signal. Therefore, the output of the analog-to-digital converter (which is the input of the "Digital SI Canceller" block in Figure 4) is thus directly fed into the "CP Removal" block. In addition, Eve can have different receiver structures depending on its knowledge of the jamming insertion behavior at Alice and/or Bob. If Eve does not know the jamming insertion behavior of (7), the receiver structure of Eve is equivalent to that of a typical OFDM receiver where

[3] In Figure 3, (a) and (b) are used later to describe the Rx operations of Eve.

(a) and (b) in Figure 4 are directly connected. If Eve knows that Alice and Bob insert jamming samples into their own Tx signals as given in (7), the receiver structure of Eve is equivalent to that in Figure 4 except for not exploiting the "Digital SI Canceller" block. Hereafter, we focus only on the latter case where Eve has the knowledge of the jamming insertion behavior of the legitimate users whose a special case with $M_{\mathrm{a}} = N$ is equivalent to the former case in terms of performance analysis.

When Eve eavesdrops on the data transmitted by Alice, the Tx signal of Bob received at Eve is treated as background noise. Accordingly, the Rx signal at Eve in (2) can be modified as

$$\mathbf{y}_{\mathrm{e}} = \mathbf{g}_{\mathrm{a}} \times \mathbf{x}_{\mathrm{a}} + \mathbf{z}_{\mathrm{e}}', \tag{16}$$

where the effective noise $\mathbf{z}_{\mathrm{e}}'$ is given by $\mathbf{z}_{\mathrm{e}}' = \mathbf{g}_{\mathrm{b}} \times \mathbf{x}_{\mathrm{b}} + \mathbf{z}_{\mathrm{e}}$. From (16), we have the frequency-domain description of the Rx signal at Eve after the CP removal and N-point FFT as

$$\mathbf{Y}_{\mathrm{e}} = \mathbf{G}_{\mathrm{a}} \times \mathbf{X}_{\mathrm{a}} + \mathbf{Z}_{\mathrm{e}}', \tag{17}$$

where $\mathbf{X}_{\mathrm{a}} = \mathbf{B}_N \mathbf{x}_{\mathrm{a}}$, $\mathbf{G}_{\mathrm{a}} = \mathrm{diag}(\mathrm{FFT}_N(\mathbf{g}_{\mathrm{a}}))$, and $\mathbf{Z}_{\mathrm{e}}' = \mathbf{B}_N \mathbf{Z}_{\mathrm{e}}'$. We then have the time-domain expression of the channel-equalized Rx signal at Eve, given by

$$\tilde{\mathbf{y}}_{\mathrm{e}} = \mathbf{A}_N \mathbf{G}_{\mathrm{a}}^{-1} \mathbf{Y}_{\mathrm{e}} = \mathbf{x}_{\mathrm{a}} + \tilde{\mathbf{z}}_{\mathrm{e}}, \tag{18}$$

with $\tilde{\mathbf{z}}_{\mathrm{e}} = [\tilde{z}_{\mathrm{e}}(0), \ldots, \tilde{z}_e(N-1)]^T = \mathbf{A}_N \mathbf{G}_{\mathrm{a}}^{-1} \mathbf{Z}_{\mathrm{e}}'$.

Eve may not have perfect information of M_{a}, $\mathcal{D}_{\mathrm{a}}$, and $\mathcal{J}_{\mathrm{a}}$. Instead, Eve has a value $0 \le L_{\mathrm{a}} \le N-1$ corresponding to M_{a}. Furthermore, Eve has two sets $\mathcal{D}_{\mathrm{e,a}}$ and $\mathcal{J}_{\mathrm{e,a}}$ corresponding to $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{J}_{\mathrm{a}}$, respectively, where $\mathcal{D}_{\mathrm{e,a}}$ and $\mathcal{J}_{\mathrm{e,a}}$ are given by

$$\begin{aligned} \mathcal{D}_{\mathrm{e,a}} &= \{d_{e,a}(0), \ldots, d_{\mathrm{e,a}}(L_{\mathrm{a}}-1)\}, \\ \mathcal{J}_{\mathrm{e,a}} &= \{j_{\mathrm{e,a}}(0), \ldots, j_{\mathrm{e,a}}(N-L_{\mathrm{a}}-1)\}, \end{aligned} \tag{19}$$

subject to $\mathcal{D}_{\mathrm{e,a}} \cap \mathcal{J}_{\mathrm{e,a}} = \phi$ and $\mathcal{D}_{\mathrm{e,a}} \cup \mathcal{J}_{\mathrm{e,a}} = \{0, \ldots, N-1\}$. In this case, Eve assumes that Alice uses the set of time samples defined in $\mathcal{D}_{\mathrm{e,a}}$ to transmit L_{a} data symbols while transmitting the jamming samples using the set of time samples defined in $\mathcal{J}_{\mathrm{e,a}}$. Note that L_{a}, $\mathcal{D}_{\mathrm{e,a}}$, and $\mathcal{J}_{\mathrm{e,a}}$ are not necessarily the same as M_{a}, $\mathcal{D}_{\mathrm{a}}$, and $\mathcal{J}_{\mathrm{a}}$, respectively, because Eve may not have perfect information of M_{a}, $\mathcal{D}_{\mathrm{a}}$, and $\mathcal{J}_{a}$. From (18) and (19), we obtain $\bar{\mathbf{y}}_{\mathrm{e}} = [\bar{y}_{\mathrm{e}}(0), \ldots, \bar{y}_{\mathrm{e}}(L_{\mathrm{a}}-1)]^T$, where

$$\bar{y}_{\mathrm{e}}(k) = \tilde{y}_{\mathrm{e}}(i), \quad \text{if } i = d_{\mathrm{b}}(k) \in \mathcal{D}_{\mathrm{e,a}}, \tag{20}$$

from which we have

$$\bar{\mathbf{Y}}_{\mathrm{e}} = \mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{y}}_{\mathrm{e}} = \mathbf{B}_{L_{\mathrm{a}}} \mathbf{x}_{\mathrm{a}} + \mathbf{B}_{L_{\mathrm{a}}} \tilde{\mathbf{z}}_{\mathrm{e}.} \tag{21}$$

The processes undertaken by Eve to wiretap the confidential information of Bob are equivalent to those in (16)–(21), except that $\mathbf{y}_{\mathrm{e}}$ in (16) is modified by $\mathbf{y}_{\mathrm{e}} = \mathbf{g}_{\mathrm{b}} \times \mathbf{x}_{\mathrm{b}} + \mathbf{z}_{\mathrm{e}}'$, where $\mathbf{z}_{\mathrm{e}}' = \mathbf{g}_{\mathrm{a}} \times \mathbf{x}_{\mathrm{a}} + \mathbf{z}_{\mathrm{e}}$. Furthermore, $\mathbf{X}_{\mathrm{a}}$ and $\mathbf{G}_{\mathrm{a}}$ in (17) are replaced by $\mathbf{X}_{\mathrm{b}} = \mathbf{B}_N \mathbf{x}_{\mathrm{b}}$ and $\mathbf{G}_{\mathrm{b}} = \mathrm{diag}(\mathrm{FFT}_N(\mathbf{g}_{\mathrm{b}}))$, respectively. Finally, a new value L_{b} and new sets $\mathcal{D}_{\mathrm{e,b}}$ and $\mathcal{J}_{\mathrm{e,b}}$ may be employed instead of L_{a}, $\mathcal{D}_{\mathrm{e,b}}$, and $\mathcal{J}_{\mathrm{e,b}}$, respectively.

4.2 | Leakage of legitimate information at eve

The confidential information transmitted from Alice that is leaked to Eve can be quantified by analyzing the mutual information (MI) between the Tx signal of Alice and the Rx signal of Eve. However, it is difficult to analyze the MI directly from (21). This is because $\mathbf{x}_{\mathrm{a}}$ in (21) includes both data samples and jamming samples corresponding to $\mathbf{x}_{\mathrm{a}}$ and $\mathbf{q}_{\mathrm{a}}$, respectively. Therefore, we alternatively express $\mathbf{x}_{\mathrm{a}}$ as

$$\mathbf{x}_{\mathrm{a}} = \tilde{\mathbf{x}}_{\mathrm{a},w} + \tilde{\mathbf{x}}_{\mathrm{a},q}, \tag{22}$$

where $\tilde{\mathbf{x}}_{\mathrm{a},w} = [\tilde{x}_{\mathrm{a},w}(0), \ldots, \tilde{x}_{\mathrm{a},w}(N-1)]^T$ with

$$\tilde{x}_{\mathrm{a},w}(k) = \begin{cases} w_a(i), & \text{if } k \in \mathcal{D}_{\mathrm{a}}, \text{ and } k = d_{\mathrm{a}}(i), \\ 0, & \text{if } k \in \mathcal{J}_{\mathrm{a}}, \text{ and } k = j_{\mathrm{a}}(i), \end{cases} \tag{23}$$

and $\tilde{\mathbf{x}}_{\mathrm{a},q} = [\tilde{x}_{\mathrm{a},q}(0), \ldots, \tilde{x}_{\mathrm{a},q}(N-1)]^T$ with

$$\tilde{x}_{\mathrm{a},q}(k) = \begin{cases} 0, & \text{if } k \in \mathcal{D}_{\mathrm{a}}, \text{ and } k = d_{\mathrm{a}}(i), \\ q_{\mathrm{a}}(i), & \text{if } k \in \mathcal{J}_{\mathrm{a}}, \text{ and } k = j_{\mathrm{a}}(i). \end{cases} \tag{24}$$

Accordingly, $\tilde{\mathbf{y}}_{\mathrm{e}}$ in (18) can be modified as

$$\tilde{\mathbf{y}}_{\mathrm{e}} = \tilde{\mathbf{x}}_{\mathrm{a},w} + \tilde{\mathbf{x}}_{\mathrm{a},q} + \tilde{\mathbf{z}}_{\mathrm{e}}, \tag{25}$$

from which we have $\bar{\mathbf{y}}_{\mathrm{e}}$ after (20) as

$$\bar{\mathbf{y}}_{\mathrm{e}} = \bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}} + \bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}} + \bar{\mathbf{z}}^{L_{\mathrm{a}}}, \tag{26}$$

where $\bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}} = [\bar{x}_{\mathrm{a},w}^{L_{\mathrm{a}}}(0), \ldots, \bar{x}_{\mathrm{a},w}^{L_{\mathrm{a}}}(L_{\mathrm{a}}-1)]^T$ and $\bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}} = [\bar{x}_{\mathrm{a},q}^{L_{\mathrm{a}}}(0), \ldots, \bar{x}_{\mathrm{a},q}^{L_{\mathrm{a}}}(L_{\mathrm{a}}-1)]^T$ are given, respectively, by

$$\begin{aligned} \bar{x}_{\mathrm{a},w}^{L_{\mathrm{a}}}(k) &= \tilde{x}_{\mathrm{a},w}(i), \quad \text{if } i = d_{\mathrm{b}}(k) \in \mathcal{D}_{\mathrm{e,a}}, \\ \bar{x}_{\mathrm{a},q}^{L_{\mathrm{a}}}(k) &= \tilde{x}_{\mathrm{a},q}(i), \quad \text{if } i = d_{\mathrm{b}}(k) \in \mathcal{D}_{\mathrm{e,a}}. \end{aligned} \tag{27}$$

Furthermore, $\bar{\mathbf{z}}^{L_{\mathrm{a}}} = [\bar{z}^{L_{\mathrm{a}}}(0), \ldots, \bar{z}^{L_{\mathrm{a}}}(L_{\mathrm{a}}-1)]^T$ with

$$\bar{z}^{L_{\mathrm{a}}}(k) = \tilde{z}_{\mathrm{e}}(i), \quad \text{if } i = d_{\mathrm{b}}(k) \in \mathcal{D}_{\mathrm{e,a}}. \tag{28}$$

Therefore, from (25)–(28), $\bar{\mathbf{Y}}_{\mathrm{e}}$ in (21) can be modified as

$$\bar{\mathbf{Y}}_{\mathrm{e}} = \mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}} + \mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}} + \mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{z}}^{L_{\mathrm{a}}}, \tag{29}$$

where $\mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}}$, $\mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}}$, and $\mathbf{B}_{L_{\mathrm{a}}} \bar{\mathbf{z}}^{L_{\mathrm{a}}}$ represent the information transmitted by Alice, interference caused by inserting jamming sequences, and the sum of background noise and the CCI caused by in-band STR with Bob, respectively.

4.2.1 | Legitimate information

We first define a set $\mathcal{L}_{\mathrm{a},w} = \{l_{\mathrm{a},w}(0), \ldots, l_{\mathrm{a},w}(L_w-1)\} = \mathcal{D}_{\mathrm{a}} \cap \mathcal{D}_{\mathrm{e,a}}$, having L_w elements. Here, L_w represents the number of time samples that Eve recognizes as data samples among the time samples in $\mathbf{x}_{\mathrm{a}}$ corresponding to $\mathbf{w}_{\mathrm{a}}$. In addition, $\mathcal{L}_{\mathrm{a},w}$ denotes the set of indices where the time samples that Eve recognizes as data samples are located within $\mathbf{x}_{\mathrm{a}}$. Therefore, $\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}}$ in (29) can be expressed as

$$\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}} = \hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_w}\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w}, \tag{30}$$

where $\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w}$ and $\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_w}$ are given, respectively, by

$$\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w} = \left[w_{\mathrm{a}}(l_{\mathrm{a},w}(0)), \ldots, w_{\mathrm{a}}\left(l_{\mathrm{a},w}(L_w-1)\right)\right]^T. \tag{31}$$

$$\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_w} = [\mathbf{b}_{L_{\mathrm{a}}}(l_{\mathrm{a},w}(0)), \ldots, \mathbf{b}_{L_{\mathrm{a}}}(l_{\mathrm{a},w}(L_w-1))], \tag{32}$$

with $\mathbf{b}_{L_{\mathrm{a}}}(i)$ denoting the i-the column vector of $\mathbf{B}_{L_{\mathrm{a}}}$.

Note that $\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w}$ is a part of $\mathbf{w}_{\mathrm{a}}$ selected by the set of indices $\mathcal{L}_{\mathrm{a},w}$. Therefore, $\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w}$ can also be expressed as

$$\hat{\mathbf{x}}_{\mathrm{a},w}^{L_w} = \hat{\mathbf{A}}_{M_{\mathrm{a}}}^{L_w}\mathbf{W}, \tag{33}$$

where $\hat{\mathbf{A}}_{M_{\mathrm{a}}}^{L_w} = [(\mathbf{a}_{M_{\mathrm{a}}}(l_{\mathrm{a},w}(0)))^T, \ldots, (\mathbf{a}_{M_{\mathrm{a}}}(l_{\mathrm{a},w}(L_w-1)))^T]^T$, with $\mathbf{a}_{M_{\mathrm{a}}}(i)$ denoting the i-th row vector of $\mathbf{A}_{M_{\mathrm{a}}}$. From (30) and (33), $\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}}$ in (29) can be equivalently expressed as

$$\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},w}^{L_{\mathrm{a}}} = \hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_w}\hat{\mathbf{A}}_{M_{\mathrm{a}}}^{L_w}\mathbf{W}. \tag{34}$$

4.2.2 | Effect of jamming sequence inserted in Tx signal

We also define a set $\mathcal{L}_{\mathrm{a},q} = \{l_{\mathrm{a},q}(0), \ldots, l_{\mathrm{a},q}(L_q-1)\} = \mathcal{D}_{\mathrm{a}} \cap \mathcal{J}_{\mathrm{e,a}}$, having L_q elements. Here, L_q represents the number of time samples that Eve recognizes as jamming samples among the time samples in $\mathbf{x}_{\mathrm{a}}$ corresponding to $\mathbf{w}_{\mathrm{a}}$. In addition, $\mathcal{L}_{\mathrm{a},q}$ denotes the set of indices where these samples are located within $\mathbf{x}_{\mathrm{a}}$. Therefore, $\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}}$ in (29) can be expressed as

$$\mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{x}}_{\mathrm{a},q}^{L_{\mathrm{a}}} = \hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q} = \mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}}, \tag{35}$$

where $\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q}$ and $\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}$ are given, respectively, by

$$\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q} = [q_{\mathrm{a}}(l_{\mathrm{a},q}(0)), \ldots, q_{\mathrm{a}}(l_{\mathrm{a},q}(L_q-1))]^T, \tag{36}$$

$$\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q} = [\mathbf{b}_{L_{\mathrm{a}}}(l_{\mathrm{a},q}(0)), \ldots, \mathbf{b}_{L_{\mathrm{a}}}(l_{\mathrm{a},q}(L_q-1))]. \tag{37}$$

Note that $\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q} \sim \mathcal{CN}(\mathbf{0}_{L_q}, P_{\mathrm{a}}\mathbf{I}_{L_q})$ because it is obtained by picking L_q samples of $\mathbf{q}_{\mathrm{a}} \sim \mathcal{CN}(\mathbf{0}_N, P_{\mathrm{a}}\mathbf{I}_N)$. As $\mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}}$ is a linear transform of $\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q}$ with $\mathbb{E}[\mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}}] = \hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}(\mathbb{E}[\hat{\mathbf{x}}_{\mathrm{a},q}^{L_q}]) = \mathbf{0}_{L_{\mathrm{a}}}$, we have $\mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}} \sim \mathcal{CN}(\mathbf{0}_{L_{\mathrm{a}}}, \boldsymbol{\Sigma}_{\mathrm{a}}^{L_{\mathrm{a}}})$, where

$$\boldsymbol{\Sigma}_{\mathrm{a}}^{L_{\mathrm{a}}} = \mathrm{cov}(\mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}}) = P_{\mathrm{a}}\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}(\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q})^H. \tag{38}$$

4.2.3 | Effect of CCI and background noise

From Lemma 1 and Proposition 1, $\mathbf{x}_{\mathrm{b}}$ can be regarded as $\mathbf{x}_{\mathrm{b}} \sim \mathcal{CN}(\mathbf{0}, P_{\mathrm{b}}\mathbf{I}_N)$. Therefore, we have

$$\mathbf{z}'_{\mathrm{e}} \sim \mathcal{CN}(\mathbf{0}_N, (P_{\mathrm{b}}|\mathbf{g}_{\mathrm{a}}|_2^2 + \sigma_{\mathrm{e}}^2)\mathbf{I}_N), \tag{39}$$

where $\mathbf{z}'_{\mathrm{e}} = \mathbf{g}_{\mathrm{b}} \times \mathbf{x}_{\mathrm{b}} + \mathbf{z}_{\mathrm{e}}$ as given in (16). As $\mathbf{Z}'_e = \mathbf{B}_N\mathbf{z}'_e$ in (17), $\tilde{\mathbf{z}}_e$ in (18) and (25) can also be expressed as

$$\tilde{\mathbf{z}}_{\mathrm{e}} = \mathbf{A}_N\mathbf{G}_{\mathrm{a}}^{-1}\mathbf{B}_N\mathbf{z}'_{\mathrm{e}}. \tag{40}$$

We define a set of indices $\mathcal{L}_z$ such that

$$\mathcal{L}_{\mathrm{a},z} = \mathcal{L}_{\mathrm{a},w} \cup \mathcal{L}_{\mathrm{a},q} = \{l_{\mathrm{a},z}(0), \ldots, l_{\mathrm{a},z}(L_{\mathrm{a}}-1)\}. \tag{41}$$

After selecting L_{a} samples from $\tilde{\mathbf{y}}_{\mathrm{e}}$ according to (20), $\bar{\mathbf{z}}^{L_{\mathrm{a}}}$ given in (26) and (28) can then be equivalently expressed as

$$\bar{\mathbf{z}}^{L_{\mathrm{a}}} = \bar{\mathbf{A}}_N^{L_{\mathrm{a}}}\mathbf{G}_{\mathrm{a}}^{-1}\mathbf{B}_N\mathbf{z}'_{\mathrm{e}}, \tag{42}$$

where $\bar{\mathbf{A}}_N^{L_{\mathrm{a}}} = [(\mathbf{a}_N(l_{\mathrm{a},w}(0)))^T, \ldots, (\mathbf{a}_N(l_{\mathrm{a},w}(L_{\mathrm{a}}-1)))^T]^T$, with $\mathbf{a}_N(i)$ denoting the i-th row vector of $\mathbf{A}_N$. The frequency-domain representation of $\bar{\mathbf{z}}^{L_{\mathrm{a}}}$ is then given by

$$\bar{\mathbf{Z}}_{\mathrm{e}} = \mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{z}}^{L_{\mathrm{a}}} = \mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{A}}_N^{L_{\mathrm{a}}}\mathbf{G}_{\mathrm{a}}^{-1}\mathbf{B}_N\mathbf{z}'_{\mathrm{e}}, \tag{43}$$

where $\bar{\mathbf{Z}}_{\mathrm{e}} \sim \mathcal{CN}(\mathbf{0}_{L_{\mathrm{a}}}, \mathbf{D}_{\mathrm{e,a}}\mathbf{S}_{\mathrm{e,a}}\mathbf{D}_{\mathrm{e,a}}^H)$ with

$$\mathbf{D}_{\mathrm{e,a}} = \mathbf{B}_{L_{\mathrm{a}}}\bar{\mathbf{A}}_N^{L_{\mathrm{a}}}, \tag{44}$$

$$\mathbf{S}_{\mathrm{e,a}} = \left(P_{\mathrm{b}}\,|\mathbf{g}_{\mathrm{a}}|_2^2 + \sigma_{\mathrm{e}}^2\right)\left(\mathbf{G}_{\mathrm{a}}\mathbf{G}_{\mathrm{a}}^H\right)^{-2}. \tag{45}$$

4.2.4 | MI between legitimate Tx signal and Rx signal at eve

From (34), (35), and (43), $\bar{\mathbf{Y}}_{\mathrm{e}}$ in (29) can be equivalently expressed as

$$\bar{\mathbf{Y}}_{\mathrm{e}} = \bar{\mathbf{C}}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}\mathbf{W}_{\mathrm{a}} + \mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}} + \bar{\mathbf{Z}}_{\mathrm{e}}, \tag{46}$$

where $\bar{\mathbf{C}}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}} = \hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_w}\hat{\mathbf{A}}_{M_{\mathrm{a}}}^{L_w}$. Note that the system described with 46 is equivalent to a Gaussian multiple-input multiple-output channel where $\mathbf{W}_{\mathrm{a}}$, $\bar{\mathbf{Y}}_{\mathrm{e}}$, $\bar{\mathbf{C}}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}$, and $(\mathbf{Q}_{\mathrm{a}}^{L_{\mathrm{a}}} + \bar{\mathbf{Z}}_{\mathrm{e}})$ correspond to the input, output, channel, and noise, respectively. Therefore, given $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{D}_{\mathrm{e,a}}$ (thus $\mathcal{L}_{\mathrm{a},w}$) with $\mathbf{G}_{\mathrm{a}}$, the MI between the Tx signal of Alice and the Rx signal at Eve is given by

$$C_{\mathrm{a}}\left(\mathcal{D}_{\mathrm{a}},\mathcal{D}_{\mathrm{e,a}},\mathbf{G}_{\mathrm{a}}\right)=\log_2\left(\left|\mathbf{I}_{L_{\mathrm{a}}}+P_{\mathrm{a}}\mathbf{C}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}\left(\mathbf{U}_{\mathrm{a}}^{L_{\mathrm{a}}}\right)^{-1}\right|\right), \tag{47}$$

where $\mathbf{C}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}$ and $\mathbf{U}_{\mathrm{a}}^{L_{\mathrm{a}}}$ are given, respectively, as

$$\mathbf{C}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}=\bar{\mathbf{C}}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}\left(\bar{\mathbf{C}}_{M_{\mathrm{a}}}^{L_{\mathrm{a}}}\right)^{H}, \tag{48}$$

$$\mathbf{U}_{\mathrm{a}}^{L_{\mathrm{a}}}=P_{\mathrm{a}}\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}\left(\hat{\mathbf{B}}_{L_{\mathrm{a}}}^{L_q}\right)^{H}+\mathbf{D}_{\mathrm{e,a}}\mathbf{S}_{\mathrm{e,a}}\mathbf{D}_{\mathrm{e,a}}^{H}. \tag{49}$$

Notably, $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ represents the minimum transmission rate of $\mathbf{w}_{\mathrm{a}}$ required at Alice for preventing Eve from recovering $\mathbf{w}_{\mathrm{a}}$. In other words, Eve cannot decode the confidential information carried by $\mathbf{w}_{\mathrm{a}}$ even if it receives $\mathbf{x}_{\mathrm{a}}$, as long as Alice transmits $\mathbf{w}_{\mathrm{a}}$ at a rate larger than $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$. This indicates that the smaller the value of $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$, the easier it is to prevent eavesdropping on the confidential information transmitted by Alice.

Figure 5 shows $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ with respect to various values of L_{a} and L_w. To obtain these example results, it is assumed that $N = 256$, $M_{\mathrm{a}} = 128$, and $\mathbf{G}_{\mathrm{a}} = \mathbf{I}_N$. To focus on the discrepancy between $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{D}_{\mathrm{e,a}}$ reflected by L_w, it is also assumed that $\mathbf{g}_{\mathrm{b}} = \mathbf{0}$, that is, no CCI owing to the in-band STR of Bob.[4] Furthermore, P_{a} and σ_{e}^2 are set such that $P_{\mathrm{a}}/\sigma_{\mathrm{e}}^2 = 30\,\mathrm{dB}$.

It is observed that $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ is maximized when $L_{\mathrm{a}} = L_w = M_{\mathrm{a}}$, that is, Eve perfectly knows where $\mathbf{w}_{\mathrm{a}}$ is located within $\mathbf{x}_{\mathrm{a}}$ and all data information of Alice is thus tapped by Eve. When the discrepancy between $\mathcal{D}_{\mathrm{a}}$ and $\mathcal{D}_{\mathrm{e,a}}$ occurs, that is, $L_{\mathrm{a}} \neq M_{\mathrm{a}}$ or $L_w \neq M_{\mathrm{a}}$, it is shown that $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ decreases with a decrease in L_w and/or an increase in L_{a}. In particular, the increase in L_{a} is observed to have a greater effect on the decrease in $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ than the decrease in L_w. Furthermore, $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ becomes sufficiently close to zero with a sufficiently small L_{a} and/or L_w.

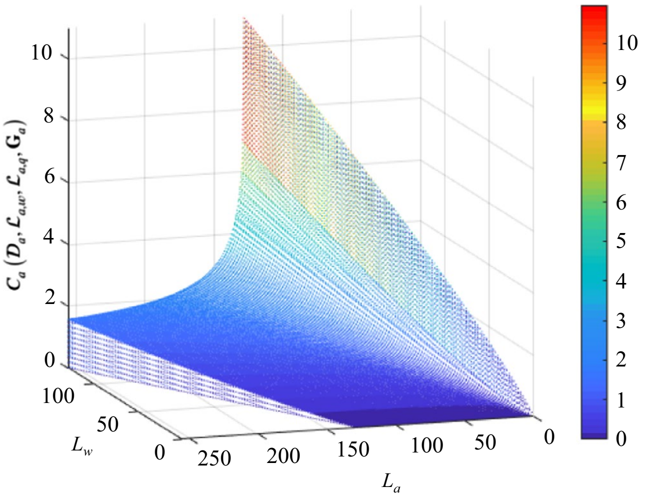

FIGURE 5 $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ with respect to various values of L_{a} and L_w for $N = 256$, $M_{\mathrm{a}} = 128$, and $\mathbf{G}_{\mathrm{a}} = \mathbf{I}_N$

5 | SIMULATION RESULTS

In this section, we simulate the information leakage from the transmissions of Alice and Bob to Eve with respect to the location of Eve. On a two-dimensional plane, Alice and Bob are assumed to be located at (−50, 0) and (50, 0), respectively, where the distance between the two locations (x_1, y_1) and (x_2, y_2) is given by $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ in meters. For each position of Eve on the network, the information leakage is measured by $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ and $C_{\mathrm{b}}(\mathcal{D}_{\mathrm{b}}, \mathcal{D}_{\mathrm{e,b}}, \mathbf{G}_{\mathrm{b}})$ given in (47).[5]

The simulation parameters are summarized in Table 2. The wireless channels in the network are all assumed to be time-invariant frequency-flat channels in which the received power of a signal is affected only by the distance-dependent signal power attenuation. Using the parameters given in Table 2, $\mathbf{h}_{\mathrm{ab}}$ and $\mathbf{h}_{\mathrm{ba}}$ are modeled as $\mathbf{h}_{\mathrm{ab}} = \mathbf{h}_{\mathrm{ba}} = \theta d_{\mathrm{ab}}^{-\alpha}\delta(n)$, where $\delta(n)$ represents the unit sample function, given by

$$\delta(n)=\begin{cases}1, \text{ if } n=0,\\ 0, \text{ otherwise.}\end{cases} \tag{50}$$

Accordingly, we have $\mathbf{H}_{\mathrm{ab}} = \mathbf{H}_{\mathrm{ba}} = \theta d_{\mathrm{ab}}^{-\alpha}\mathbf{I}_N$. Furthermore, $\mathbf{g}_{\mathrm{a}}$ and $\mathbf{g}_{\mathrm{b}}$ are given by $\mathbf{g}_{\mathrm{a}} = \theta d_{\mathrm{ae}}^{-\alpha}\delta(n)$ and $\mathbf{g}_{\mathrm{b}} = \theta d_{\mathrm{be}}^{-\alpha}\delta(n)$, respectively, where d_{ae} and d_{be} represent the distances from Alice and Bob to Eve in meters, respectively. Accordingly, we also have $\mathbf{G}_{\mathrm{a}} = \theta d_{\mathrm{ae}}^{-\alpha}\mathbf{I}_N$ and $\mathbf{G}_{\mathrm{b}} = \theta d_{\mathrm{be}}^{-\alpha}\mathbf{I}_N$.

For each position of Eve on the two-dimensional plane, Figures 6–8 show $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ (left) and $C_{\mathrm{b}}(\mathcal{D}_{\mathrm{b}}, \mathcal{D}_{\mathrm{e,b}}, \mathbf{G}_{\mathrm{b}})$ (right) in bps/Hz. In these figures, the red square and the blue circle represent Alice and Bob, respectively. As shown in Table 2, we consider three values of M_{b}, that is, $M_{\mathrm{b}} = 128$ (Figure 6), 256 (Figure 7), and 384 (Figure 8), whereas M_{a} is fixed at 512. By setting $L_{\mathrm{a}} = L_{\mathrm{b}} = N$ with $\mathcal{D}_{\mathrm{e,a}} = \mathcal{D}_{\mathrm{e,b}} = \{0, \ldots, N-1\}$, Eve is assumed to receive all the data samples transmitted by both Alice and Bob.

Note that $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ and $C_{\mathrm{b}}(\mathcal{D}_{\mathrm{b}}, \mathcal{D}_{\mathrm{e,b}}, \mathbf{G}_{\mathrm{b}})$ represent the minimum transmission rates of $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{w}_{\mathrm{b}}$ required to prevent Eve from restoring the confidential information contained in $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{w}_{\mathrm{b}}$, respectively. For example, in Figure 6, when located at (50, 40), Eve cannot recover the confidential information in $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{w}_{\mathrm{b}}$, unless the transmission rates of $\mathbf{w}_{\mathrm{a}}$ and $\mathbf{w}_{\mathrm{b}}$ are smaller than 0.05 bps/Hz and 0.3 bps/Hz, respectively.

The Tx signal of Alice is protected only by the CCI that occurs at Eve owing to the in-band STR of Bob, because the jamming samples are not inserted in $\mathbf{x}_{\mathrm{a}}$. As shown in the left sides of Figures 6–8, $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ is very small when Eve is located close to Bob because the CCI at Eve

[4] The case where $\mathbf{g}_{\mathrm{b}}$ is not a zero vector and thus interference from the transmission of Bob is received at Eve is considered in the next section.

[5] Although only $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ is shown in (47), $C_{\mathrm{b}}(\mathcal{D}_{\mathrm{b}}, \mathcal{D}_{\mathrm{e,b}}, \mathbf{G}_{\mathrm{b}})$ can also be obtained in exactly the same way as $C_{\mathrm{a}}(\mathcal{D}_{\mathrm{a}}, \mathcal{D}_{\mathrm{e,a}}, \mathbf{G}_{\mathrm{a}})$ is obtained.

TABLE 2 Simulation parameters

Tx powers of Alice (P_a)	24 dBm
Tx powers of Bob (P_b)	23 dBm
Powers of Rx noise (σ_a, σ_b, and σ_e)	−101 dBm[a]
Distance between Alice and Bob (d_{ab})	100 meter
Signal power attenuation at reference distance 1 m (θ)	−30 dB
Pathloss exponent (α)	4
Sample length of a time-domain symbol (N)	512
Number of data constellations/Tx at Alice (M_a)	512
Number of data constellations/Tx at Bob(M_b)	128, 256, 384

[a] The channel bandwidth and the noise spectral density are assumed to be 20 MHz and −174 dBm/Hz, respectively.

is sufficiently strong. However, when Eve is located close to Alice, $C_a(\mathcal{D}_a, \mathcal{D}_{e,a}, \mathbf{G}_a)$ has a very large value because the CCI at Eve becomes negligible. In this case, Alice should encode $\mathbf{w}_a$ at an impractically high information rate to prevent eavesdropping by Eve.

In contrast, the Tx signal of Bob is protected not only by the CCI that occurs at Eve owing to the in-band STR of Alice, but also by the jamming samples inserted in $\mathbf{x}_b$. When Eve is close to Alice, the CCI occurring at Eve is very strong and thus substantially decreases $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$, as shown in the right sides of Figures 6–8. However, when Eve is close to Bob, $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$ remains small owing to the jamming samples inserted in $\mathbf{x}_b$ despite the negligible effect of the CCI, unlike the $C_a(\mathcal{D}_a, \mathcal{D}_{e,a}, \mathbf{G}_a)$ obtained when Eve is close to Alice. Furthermore, at a given location of Eve near Bob, $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$ decreases with an increase in M_b. This is because the smaller the value of M_b, the more jamming samples are inserted into $\mathbf{x}_b$, making it more difficult for Eve to decode and eavesdrop on the confidential information transmitted by Bob.

Note that both $C_a(\mathcal{D}_a, \mathcal{D}_{e,a}, \mathbf{G}_a)$ and $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$ are small when Eve is close to Bob, even though the jamming samples are not inserted in $\mathbf{x}_a$. This indicates that, when Eve is close to Bob and the traffic required at Alice and Bob is given such that $M_a = N$ and $M_b < N$, the confidential information transmitted by Alice and Bob is simultaneously protected from eavesdropping, without loss of their respective data rates.

Remark Note that the setup used in these simulations describes a simplified representation of typical small-cell environments, in which Alice and Bob correspond to a small-cell base station (BS) and user equipment (UE), respectively. In a typical cellular environment (including that with small-cells), not only is the DL traffic much greater than the UL traffic, but the security for UL data is also more emphasized. This is because UL data often contain private information for, for example, authentication. Furthermore, eavesdroppers are more likely to be located closer to the UE than to the BS. In a small-cell environment where an eavesdropper is located near the UE, the simulation results show the effectiveness of ST-jamming in protecting the confidential information in the UL and DL, without loss of data rate in the DL.

6 | CONCLUSIONS

In this paper, we proposed a scheme referred to as ST-jamming, which enhances PHYSEC given the asymmetry of traffic in BD-IFD communication. We first studied the generation of a transmit signal including both the data samples and jamming samples. We then described a scheme to decode

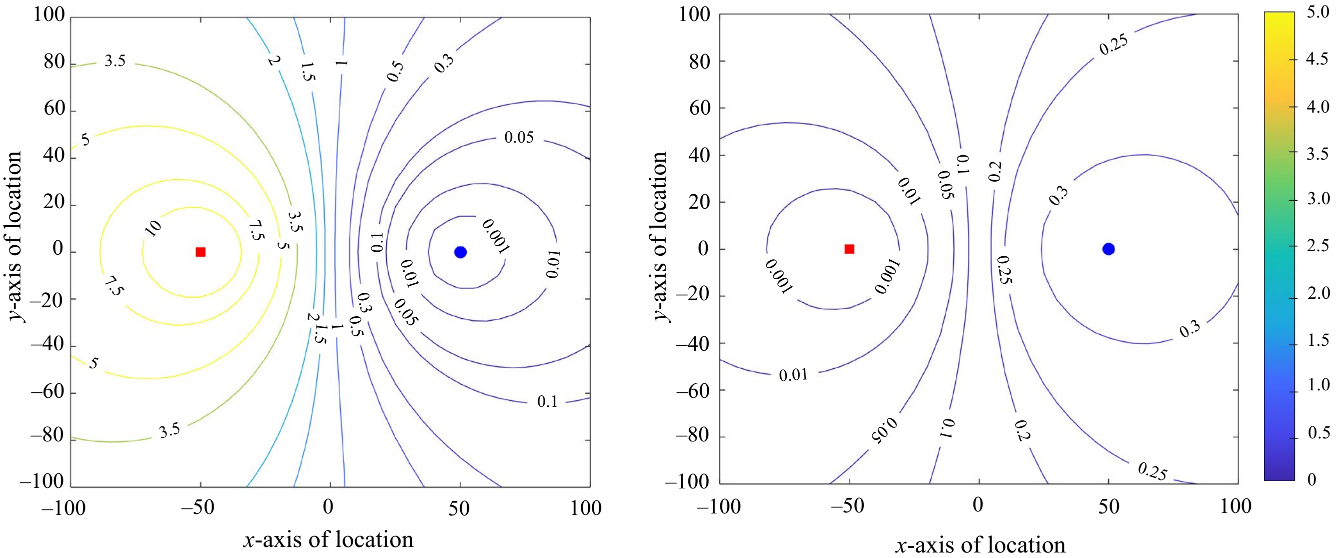

FIGURE 6 $C_a(\mathcal{D}_a, \mathcal{D}_{e,a}, \mathbf{G}_a)$ (left) and $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$ (right) with respect to the location of Eve, when $M_b = 128$

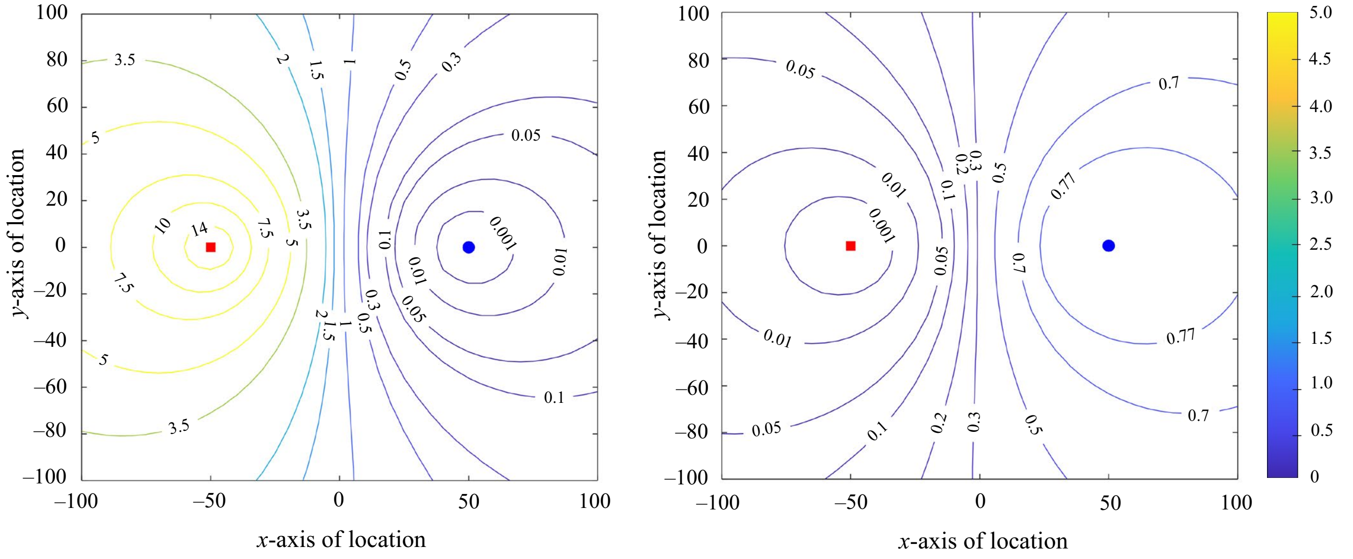

FIGURE 7 $C_a(\mathcal{D}_a, \mathcal{D}_{e,a}, \mathbf{G}_a)$ (left) and $C_b(\mathcal{D}_b, \mathcal{D}_{e,b}, \mathbf{G}_b)$ (right) with respect to the location of Eve, when $M_b = 256$

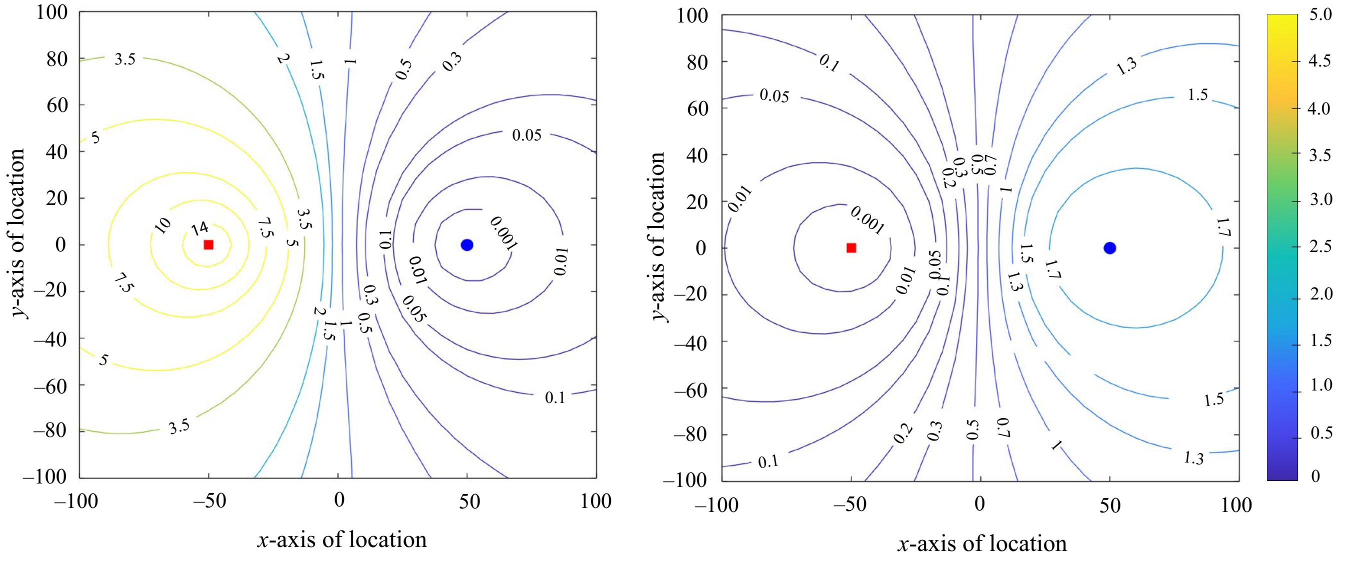

FIGURE 8 $C_\mathrm{a}(\mathcal{D}_\mathrm{a}, \mathcal{D}_\mathrm{e,a}, \mathbf{G}_\mathrm{a})$ (left) and $C_\mathrm{b}(\mathcal{D}_\mathrm{b}, \mathcal{D}_\mathrm{e,b}, \mathbf{G}_\mathrm{b})$ (right) with respect to the location of Eve, when $M_\mathrm{b} = 384$

the legitimate information by removing the jamming samples. The information leakage at the eavesdropper was analyzed by investigating the MI between the Tx signals of the legitimate users and the Rx signal at the eavesdropper. The simulation results showed that the proposed ST-jamming is effective to prevent eavesdropping on the confidential information of legitimate users without loss of their respective data rate, when practical traffic asymmetry is given.

Based on the works presented in this paper, we can visualized the following future research directions: First, we can consider a scenario with multiple pairs of legitimate users all or a part of which operate with IFD. In this case, the management of CCI between legitimate users will be one of the most important technical issues because it can severely degrade the data transmission performance of the legitimate users. In addition, we can also consider a case in which the legitimate users and/or eavesdropper(s) are equipped with multiple antennas. For the legitimate users, interference alignment for CCI management between the legitimate users and multiantenna signal processing for secrecy enhancement will be interesting research topics. Furthermore, it is necessary to study multi-antenna transmission techniques for the legitimate users to improve secrecy performance because the multi-antenna signal processing at the eavesdropper may mitigate the effect of jamming. Finally, the secrecy performance of the proposed scheme and its extension in the presence of multiple eavesdroppers with/without colluding in the network may be studied.

ACKNOWLEDGMENTS

This work was supported by an Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korea Government (19ZH1600, ST-Jamming for Overhead-Free PHY Layer-Secured Communication).

ORCID

Hyungsik Ju https://orcid.org/0000-0002-7787-8466

REFERENCES

1. H. Ju et al., *Novel digital cancelation method in presence of harmonic self-interference*, ETRI J. **39** (2017), no. 2, 245–254.
2. D. Bharadia et al., *Full duplex radios*, in Proc. ACM SIGCOMM, Hong Kong, China, Aug. 2013. pp. 375–386.
3. K.E. Kolodziej, J.G. McMichael, and B.T. Perry, *Multitap RF canceller for in-band full-duplex wireless communications*, IEEE Trans. Wireless Commun. **15** (2016), no. 6, 4321–4334.
4. M. Sakai et al., *Self-interference cancellation in full-duplex wireless with IQ imbalance*, Phy. Commun. **18** (2016), no. 1, 2–14.
5. H. Ju et al., *Capacity enhancement of uni-directional in-band full-duplex cellular networks through co-channel interference cancellation*, ETRI J. **40** (2018), no. 2, 207–217.
6. L. Zhang et al., *3-D drone-base-station placement with in-band full-duplex communications*, IEEE Commun. Lett. **22** (2018), no. 9, 1902–1905.
7. L. Chen et al., *Fast power allocation for secure communication with full-duplex radio*, IEEE Trans. Signal Process. **65** (2015), no. 14, 3846–3861.
8. C. Liu et al., *Secure spatial modulation with a full-duplex receiver*, IEEE Wireless Commun. Lett. **6** (2017), no. 6, 838–841.
9. T. Guo et al., *Secrecy-oriented antenna assignment optimization at full-duplex receiver with self-interference*, IEEE Wireless Commun. Lett. **7** (2018), no. 4, 562–565.
10. X. Tang, P. Ren, and Z. Han, *Iterative power optimization towards secure multi-channel full-duplex communication*, in Proc. IEEE Global Commun. Conf. (GLOBECOM), Washington, DC, USA, Dec. 2016, pp. 1–6.
11. Q. Li et al., *Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI*, IEEE Trans. Signal Process. **65** (2017), no. 17, 4684–4697.
12. N. Mahmood and P. Mogensen, *On the secrecy degrees of freedom with full-duplex communication*, in Proc. IEEE Int. Commun. Conf. (ICC) Workshops, Paris, France, May 2017, pp. 1310–1315.
13. L. Li et al., *Linear precoder design for an MIMO Gaussian wiretap channel with full-duplex source and destination nodes*, IEEE Trans. Inform. Forensics and Security **13** (2018), no. 2, 421–436.
14. W. Tang et al., *Physical layer security in heterogeneous networks with jammer selection and full-duplex users*, IEEE Trans. Wireless Commun. **16** (2017), no. 12, 7982–7995.
15. T.-X. Zheng et al., *Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy*, IEEE Trans. Wireless Commun. **16** (2017), no. 6, 3827–3839.
16. T.-X. Zheng et al., *Safeguarding decentralized wireless networks using full-duplex jamming receivers*, IEEE Trans. Wireless Commun. **16** (2017), no. 1, 278–292.
17. A. Babaei et al., *Full-duplex small-cell networks: a physical-layer security perspective*, IEEE Trans. Commun. **66** (2018), no. 7, 3006–3021.
18. M. R. Abedi et al., *Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: active adversary*, IEEE Trans. Wireless Commun. **16** (2017), no. 2, 885–899.
19. M.K. Hanawal, D.N. Nguyen, and M. Krunz, *Jamming attack on in-band full-duplex communications: Detection and countermeasures*, in Proc. IEEE INFOCOM, San Francisco, CA, USA, Apr. 2016, pp. 1–9.
20. Report ITU-R, IMT Traffic Estimates for the Years of 2020 to 2030, Radiocommunication Sector of ITU (2015), M.2370, 1–49.
21. J. Liu et al., *Performance gain of full duplex over half duplex under bidirectional traffic asymmetry*, in Proc. IEEE Int. Commun. Conf. (ICC) Workshop, Kuala Lumpur, Malaysia, May 2016, pp. 90–103.
22. H. Malik et al., *Cross-layer approach for asymmetric traffic accommodation in full-duplex wireless networks*, in Proc. IEEE Eur. Conf. Netw. Commun. (EuCNC), Oulu, Finland, June 2015, pp. 265–269.
23. Y. Sun et al., *Optimal joint power and subcarrier allocation for full-duplex multicarrier non-orthogonal multiple access systems*, IEEE Trans. Commun. **65** (2017), no. 3, 1077–1091.
24. D. Wulich et al., *Level clipped high-order OFDM*, IEEE Trans. Commun. **48** (2000), no. 6, 928–930.

AUTHOR BIOGRAPHIES

Hyungsik Ju received his BS and PhD degrees in Electrical Engineering from Yonsei University, Seoul, Rep. of Korea, in 2005 and 2011, respectively. From September 2011 to March 2012, he worked as a researcher at Yonsei University. From March 2012 to August 2014, he was with the Department of Electrical and Computer Engineering of the National University of Singapore, Singapore, as a research fellow. Since September 2014, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Korea, as a senior researcher. His current research interests include full-duplex wireless communication, wireless information and power transfer and wireless powered networks, relay-based multi-hop communication and full-duplex relay systems.

Donghyuk Gwak received his BS and MS in electrical engineering from Seoul National University, Seoul, Rep. of Korea, in 2010 and 2013, respectively. Since 2013, he has been a researcher with the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea. His research interests include beamforming, interference management, compressive sensing, and massive MIMO.

Tae-Joong Kim received his BS, MS, and PhD degrees from Yonsei University in 1991, 1993, and 1998, respectively. He joined Eonex Ltd. in 2001, where he had worked first on chipset system-design and later on software protocol stack and field test until 2006. He has been working for the Electronics and Telecommunications Research Institute (ETRI) Daejeon, Korea since 2006, and has developed 4G-LTE and 5G mobile communication systems. He is currently an Assistant Vice President and in charge of the Future Mobile Communication Research Division in ETRI.