IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 13, 2018, accepted May 30, 2018, date of publication June 6, 2018, date of current version July 6, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2844558

Physical-Layer Security Against Smart Eavesdroppers: Exploiting Full-Duplex Receivers

JONGYEOP KIM, (Student Member, IEEE), JINWOONG KIM, JEMIN LEE, (Member, IEEE), AND JIHWAN P. CHOI, (Senior Member, IEEE)

Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu 42998, South Korea

Corresponding author: Jihwan P. Choi (jhchoi@dgist.ac.kr)

This work was supported in part by the Korean Government (Ministry of Science and ICT) under the National Research Foundation of Korea under Grants 2017R1C1B2009280 and 2015R1C1A1A01051503, and in part by the DGIST Research and Development Program of the Ministry of Science and ICT under Grant 18-ST-02.

ABSTRACT As many security solutions integrated with various technologies have been proposed against eavesdropping attacks, technical advances for adversaries can also pose a serious security threat. This paper considers a problem of smart eavesdropping attacks on multiple-input-multiple-output wiretap channels for a legitimate transceiver. We present a smart eavesdropper model and a cooperative jamming solution between transceivers that can control the jamming signal power to achieve the optimal secrecy performance. In particular, for practical applications, our proposed solution considers the residual self-interference from the full-duplex receiver and the limited cancellation capability of the smart eavesdropper. We derive the secrecy outage probability in general and smart eavesdropper cases, and show numerical results and secrecy regions for evaluation. As a result, our proposed solutions can improve the secrecy performance significantly by exploiting the full-duplex receiver and the cooperative jamming strategies with the sophisticated power control according to power expenditure.

INDEX TERMS Physical layer security, full-duplex systems, optimal power allocation, jamming, eavesdropping, residual self-interference, secrecy outage probability.

I. INTRODUCTION

Recently, the physical-layer security with the information theoretic approach has attracted considerable attention for secure wireless communications due to the broadcast property of the wireless medium. In the pioneering work on the information theoretic security, Wyner [1] introduced the wiretap channel and Csisźar and Köorner [2] extended it to broadcast channels, showing that a positive secrecy capacity can be achieved when eavesdroppers have worse channel conditions than the legitimate channel. Since then, from various perspectives, the study of physical-layer security has inspired merging of various technologies in antennas, channel coding, relay, full-duplex, and artificial noise.

One of the important concepts in physical-layer security is to exploit the characteristics of dynamically changing channels, such as fading, noise, interference, and diversity, for confidential communication [3]–[10]. However, it is difficult to achieve the secrecy of legitimate channels because legitimate nodes cannot precisely obtain the channel state information of eavesdroppers hiding in the channel. To solve this, Goel and Negi [11] proposed an innovative idea of using artificial noise (AN), which can confuse eavesdroppers without performance degradation of legitimate nodes. Moreover, the AN-assisted strategy, which does not require the channel state information (CSI) of eavesdroppers, can be a very reasonable solution for eavesdropping attacks in practice. The AN scheme has been considered in the literature with various models such as multiple-input-multiple-output (MIMO) wiretap scenarios [12], multiple user (MU) systems [13], cooperative jamming strategies [14], [15], and full-duplex systems [16]–[18].

A. PREVIOUS WORK

Many of previous work has assumed that eavesdroppers merely overhear on communications. These limited eavesdroppers neither actively intercept the CSI of the legitimate links nor inject additional interferences on the channel. However, recently, in the active eavesdropper model [19] eavesdroppers are no longer considered being resource-limited (e.g., antenna resource, power, and signal processing capability) or passive in the wiretap channel. For instance, smart adversaries using the full-duplex scheme perform eavesdropping and pilot contamination attacks simultaneously to disturb the CSI exchange between transmitters and receivers [20]. Spoofing relay attacks [21], which operate the full-duplex scheme with simultaneous signal reception and relaying, can significantly improve the information leakage rate over previous eavesdropping models. Moreover, surprisingly, the enhanced eavesdroppers exploiting the aid of multiple antennas can eliminate the jamming signals of the transmitter efficiently [22]. A MUSIC-like algorithm [23] and a Hyperplane Clustering algorithm [24] were proposed to separate jamming interferences from signals by using orthogonality between them.

With the advancement of the eavesdropping techniques, we now encounter a new problem: if a smart eavesdropper with advanced RF circuit technologies and abundant resource-based computing can be realized, it will cause severe security problems through eavesdropping attacks of high performance. For example, the channel estimation process [25] of the legitimate nodes through training symbol exchange and feedback channels may help to achieve close to channel capacity, but on the contrary, may be very vulnerable to smart eavesdroppers who can overhear the channel. In particular, if a smart eavesdropper can obtain the full CSI of the legitimate wireless channel, it may nullify the existing security solutions such as secure beamforming, transmission/reception diversity, and friendly jamming. Hence, for more challenging security problems we need to consider enhanced eavesdropper models, which have sufficient resources such as multiple antennas, fast signal processing capability, and enhanced computing power.

B. CONTRIBUTIONS

The contributions of this paper can be summarized as follows:

- We investigate security problems and solutions, depending on the capability of eavesdroppers that are either passive or smart. We propose a cooperative jamming scheme to countermeasure attacks from smart eavesdroppers that can cancel the jamming signal and listen to the confidential data signal.
- Due to the self-interference by the additional jamming transmission at the receiver, we consider establishing proper power allocation between a transmitter and a receiver with the limited power budget.
- Our secrecy performance is evaluated regarding a trade-off between the cancellation capability of smart eavesdroppers and the self-interference of jamming receivers. Finally, we analyze the performance of the cooperative jamming strategy on the secrecy region.

The remaining of this paper is organized as follows: Section II presents the eavesdropper models of passive and smart cases and the full-duplex receiver. Section III shows the derivation of the secrecy outage probability (SOP) in both eavesdropper cases. Section IV presents cooperative jamming strategies. Section V analyzes numerical results and presents a secrecy region according to riskiness of each eavesdropper. Finally, Section VI concludes the paper.

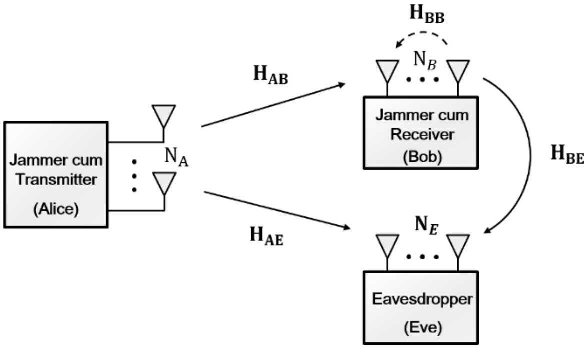


FIGURE 1. System model for secure communication with a full-duplex receiver in presence of an eavesdropper.

II. SYSTEM AND EAVESDROPPER MODEL

A. SYSTEM MODEL

We consider a MIMO wiretap channel where the transmitter Alice communicates with a legitimate receiver Bob while an eavesdropper Eve hears the confidential data signal transmitted by Alice as shown in Fig. 1. The channels are assumed to be quasi-static Rayleigh fading with zero-mean complex Gaussian noise. All the channels experience slow fading with the same fading block length, implying that fading coefficients remain constant during the transmission of the entire signals. We also assume that the full channel state information between Alice and Bob, independent of the eavesdropper channel, is exchanged by training/feedback and transmission protocols. Matrices $\boldsymbol{H}_{AB} \in \mathbb{C}^{N_A \times N_B}$, $\boldsymbol{H}_{AE} \in \mathbb{C}^{N_A \times N_E}$ and $\boldsymbol{H}_{BE} \in \mathbb{C}^{(N_B-1) \times N_E}$ represent channels from Alice to Bob, Alice to Eve, and Bob to Eve, respectively. In practice, neither Alice nor Bob can know Eve's CSI. To increase the received signal strength, Bob uses a selection combining (SC) scheme [26], while Eve uses a maximal ratio combining (MRC) scheme with multiple ($N_E \geq 2$) antennas [27]. Alice is equipped with $N_A(\geq 2)$ antennas. Bob has $N_B(\geq 2)$ antennas, of which the selected single antenna is for receiving the best-quality signal and the remaining $N_B - 1$ antennas are for transmitting additional jamming signals to Eve. The selected antenna i by the SC scheme that maximizes the received instantaneous SNR can be written as

$$i = \underset{k \in 1,\ldots,N_B}{\arg\max} \left| \boldsymbol{h}_{AB,k} \right|, \tag{1}$$

where $\boldsymbol{h}_{AB,k} \in \mathbb{C}^{N_A \times 1}$ represents the kth column of $\boldsymbol{H}_{AB}$.

B. EAVESDROPPER MODEL

1) PASSIVE EAVESDROPPER

In a practical scenario, eavesdroppers are usually passive and silent to hide their espionage behaviors. Against eavesdropping attacks, we can use the friendly jamming strategy [11], [28], in which artificial noise is transmitted in addition to the confidential data signal to degrade the channel quality of the potential eavesdroppers. The transmit signal from Alice $\boldsymbol{x}(n) \in \mathbb{C}^{N_A \times 1}$ takes a structure of

$$\boldsymbol{x}\left(n\right) = \left[\boldsymbol{\omega}_S \quad \boldsymbol{\omega}_1 \cdots \boldsymbol{\omega}_{N_A-1}\right] \begin{bmatrix} s\left(n\right) \\ J_1\left(n\right) \\ \vdots \\ J_{N_A-1}\left(n\right) \end{bmatrix}$$
$$= \boldsymbol{\omega}_S s\left(n\right) + \boldsymbol{w}(n), \tag{2}$$

where $s\left(n\right)$ is the confidential data signal with the power of $P_S = E\left\{|s(n)|^2\right\} = \sigma_s^2$ at time n; $\boldsymbol{\omega}_S = \frac{\boldsymbol{h}_{AB,i}}{\|\boldsymbol{h}_{AB,i}\|}$ represents the normalized beamforming coefficients. Here, $\boldsymbol{w}(n)$ is the artificial noise (AN), given by

$$\boldsymbol{w}\left(n\right) = \sum\nolimits_{\boldsymbol{k=1}}^{N_A-1} \boldsymbol{\omega}_k J_k(\mathrm{n}), \tag{3}$$

where $\boldsymbol{\omega}_k$ is an orthonormal beamforming coefficient toward the null space of $\boldsymbol{h}_{AB,i}^H$ i.e., $\boldsymbol{h}_{AB,i}^H \boldsymbol{w}\left(n\right) = 0$, with $(\cdot)^{\boldsymbol{H}}$ denoting a transpose-conjugate operation, and $J_k(n)$ represents a noise generated according to an independent and identical Gaussian distribution $\mathcal{N}\left(0,\sigma_{JA}^2/(N_A-1)\right)$. Hence, the artificial noise with the power of $P_{JA} = E\left\{\|\boldsymbol{w}(n)\|^2\right\} = \sigma_{JA}^2$ lies in the null space of the legitimate channel. We consider the instantaneous power constraints at the transmitter as follows:

$$P_S + P_{JA} = \sigma_s^2 + \sigma_{JA}^2 \leq P_{T,A}, \tag{4}$$

where $P_{T,A}$ is the transmission power budget at Alice. Since $\boldsymbol{h}_{AB,i}^H \boldsymbol{w}\left(n\right) = 0$, the artificial noise can be cancelled at Bob, and its received signal becomes

$$y_B = \boldsymbol{h}_{AB,i}^H \boldsymbol{\omega}_S s\left(n\right) d_{AB}^{-a/2} + n_B\left(n\right), \tag{5}$$

where d is the distance between Alice and Bob, a is the path-loss exponent, and $n_B\left(n\right) \sim \mathcal{CN}\left(0, \sigma_n^2\right)$ is the complex additive white Gaussian noise (AWGN). The received signal by passive Eve, on the other hand, can be expressed as

$$\boldsymbol{y}_{(\boldsymbol{P})\boldsymbol{E}} = \boldsymbol{H}_{AE}^H \boldsymbol{\omega}_S s(n) d_{AE}^{-a/2} + \boldsymbol{H}_{AE}^H \boldsymbol{w}\left(n\right) d_{AE}^{-a/2} + \boldsymbol{n}_{\boldsymbol{E}}(n), \tag{6}$$

where $\boldsymbol{n}_{\boldsymbol{E}}\left(n\right) \sim \mathcal{CN}\left(0,\sigma_n^2\right)$ and Eve performs the MRC scheme to combine the receiver signals. Note that the friendly jamming noise does not affect Bob's received signal but degrades Eve's [11], Therefore, Eve cannot successfully decode the confidential data signal $s(n)$ when the effect of artificial noise from (3) is large.

2) SMART EAVESDROPPER

So far, previous work has assumed that most eavesdroppers are resource-limited and there is no correlation between the main channel ($\boldsymbol{H}_{AB}$) and the eavesdropping channel ($\boldsymbol{H}_{AE}$). Moreover, passive eavesdroppers could not avoid or defend the friendly jamming. This modeling of the limited malicious nodes motivates to consider enhanced eavesdropping attacks on the feedback of CSI between transmitters and receivers. Here, we introduce a smart eavesdropper, which can mitigate the friendly jamming impact by using antenna techniques or signal processing.

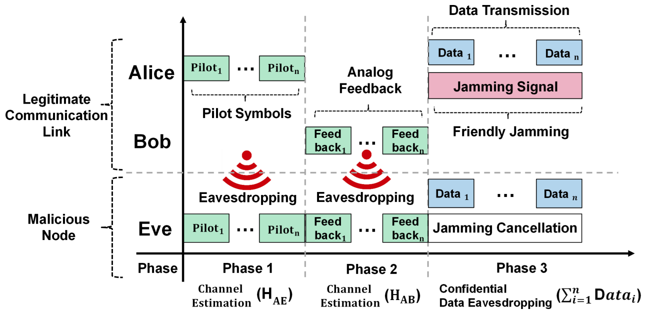


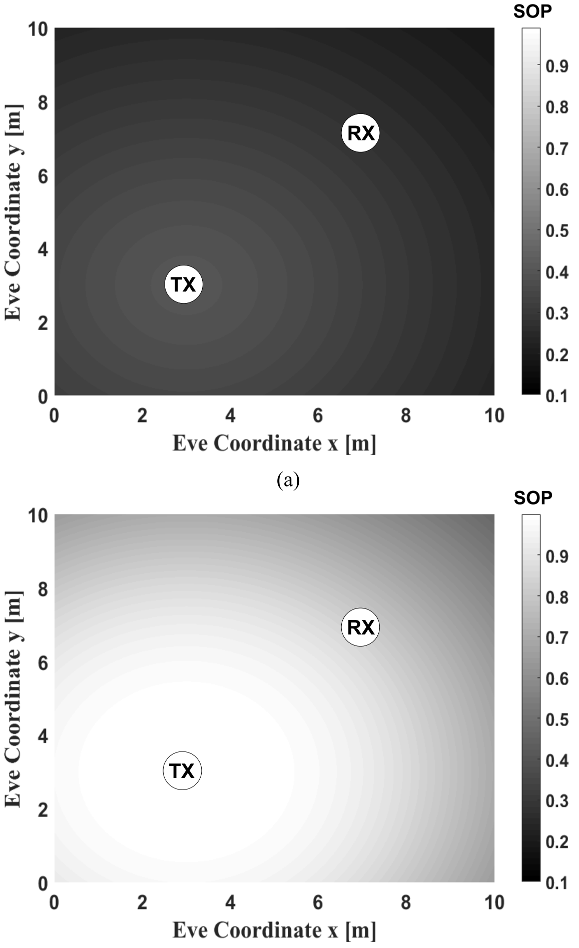
FIGURE 2. **Eavesdropping process of smart eavesdropper in secure communication.**

In our model, Alice transmits the friendly jamming signal lying in the null space of the Bob's channel. This strategy is valid only when Eve cannot intercept the CSI of main and eavesdropper channels. Hence, if Eve can obtain the main channel information ($\boldsymbol{H}_{AB}$) as well as that of the eavesdropper channel ($\boldsymbol{H}_{AE}$), she can easily decode confidential data without much interference. We assume that the smart eavesdropper has a capability to extract all the channel information because pilots and training symbols of the standardized commercial equipment can be exploited [25]. The three-phase eavesdropping attack protocol in Fig. 2 can be described as follows:

- In phase 1: Eve estimates the channel information of $\boldsymbol{H}_{AE}$ by eavesdropping pilot symbols broadcast from Alice.
- In phase 2: Eve can also estimate the main channel information ($\boldsymbol{H}_{AB}$) by eavesdropping feedback information from Bob (e.g., CSI or modulation coding scheme feedback). Hence, Eve can estimate the null space matrix of the main channel, used for friendly jamming from Alice.
- In phase 3: Although Alice transmits the friendly jamming signal and the confidential data signal at the same time for secure communication, Eve can decode the confidential data signal through jamming cancellation by utilizing CSI of both $\boldsymbol{H}_{AB}$ and $\boldsymbol{H}_{AE}$.

The impacts of passive and smart eavesdropping on the secrecy performance are contrasted in Fig. 3. The capability of general eavesdroppers is mostly compromised by artificial noise jamming, while an advanced eavesdropper can easily obtain confidential information without jamming interference. Light shading with high values of secrecy outage probability (SOP), which will be mathematically defined in subsection III-B, represents bad secrecy performances in most areas of Fig 3(b). Hence, for this critical threat of the smart eavesdropper, the previous friendly jamming scheme cannot guarantee communication secrecy, which motivates a new countermeasure.

First, we consider an ideal smart Eve case which can know full CSI of all nodes. The received signal by the ideal smart



(a)

(b)

FIGURE 3. Examples of security threats with (a) a passive and (b) a smart eavesdropper in terms of the normalized secrecy outage probability. The friendly jamming scheme can achieve high secrecy performance against the passive eavesdropper, while the smart eavesdropper can cause a security problem.

Eve can be expressed as

$$y^{Ideal}_{(S)E} = \boldsymbol{H}^H_{AE}\boldsymbol{\omega}_S s(n) d_{AE}^{-a/2} + \boldsymbol{n_E}(n), \tag{7}$$

where $\boldsymbol{H}^H_{AE}\boldsymbol{w}(n)$ of (6) is canceled by utilizing both CSI of $\boldsymbol{H}_{AB}$ and $\boldsymbol{H}_{AE}$. The artificial noise can no longer compromise the eavesdropper that can perfectly intercept both full CSI. However, contrary to eavesdropping on pilot signals or training symbols, it may be very difficult to listen to the feedback channel ($\boldsymbol{H}^H_{AB}$) perfectly from a practical standpoint.

Eve may not perfectly cancel the friendly jamming interference due to the limited eavesdropping capabilities such as channel estimation errors, subtle frequency offsets, different characteristics of RF components, etc. Then, after the jamming signal cancellation, there can be residual jamming interference as

$$\mathrm{E}\left\{\left\|\tilde{\boldsymbol{h}}^H_{AB}\boldsymbol{w}(n)\right\|^2\right\} = \epsilon P_{JA}, \tag{8}$$

where $\tilde{\boldsymbol{h}}_{AB}$ is the estimated channel of h_{AB} and ϵ is the residual jamming interference ratio ($0 \leq \epsilon \leq 1$).

The received signal by the practical smart Eve with $\epsilon > 0$ can be expressed as

$$y^{Practical}_{(S)E} = \boldsymbol{H}^H_{AE}\boldsymbol{\omega}_S s(n) d_{AE}^{-a/2} + \boldsymbol{H}^H_{AE}(\tilde{\boldsymbol{h}}^H_{AB}\boldsymbol{w}(n))^{1/2} d_{AE}^{-a/2} + \boldsymbol{n_E}(n), \tag{9}$$

which is reduced to the ideal case of (7) with $\epsilon = 0$. Since both ideal and practical models of the proposed eavesdropper are assumed to be sufficient to mitigate friendly jamming, we need a new physical layer security solution to counteract severe security threats. We will explain this in the following subsection.

C. ADDITIONAL JAMMING STRATEGY USING FULL-DUPLEX RECEIVER

The friendly jamming strategies have been designed for communication secrecy with less degradation of performance at a legitimate receiver such as the friendly jamming beamforming [11], [29] and the precoding design of multi-antenna transmission [30]. However, these solutions need CSI between Alice and Bob for successful friendly jamming. Hence, this channel dependency has rather made the system vulnerable to smart eavesdropping attacks. Consequently, existing friendly jamming techniques can no longer be a valid solution for enhanced malicious nodes with all channel information such as smart eavesdroppers.

We thus consider additional cooperative jamming transmission at Bob to degrade the Eve performance over the Bob-Eve channel $\boldsymbol{H}_{BE}$. The eavesdropper is generally unable to cancel this jamming since it is not easy for the eavesdropper to acquire the information on $\boldsymbol{H}_{BE}$. Specifically, the full-duplex jamming receiver transmits jamming signals while receiving the confidential data signal using the full-duplex technique at the same time [17], [18]. We consider the average jamming power constraint at the receiver as

$$P_{JB} = \mathrm{E}\left\{\|\boldsymbol{J}_B(n)\|^2\right\} = \sigma^2_{JB} \leq P_{T,B}, \tag{10}$$

where the jamming noise $\boldsymbol{J}_B(n) \sim \mathcal{N}\left(0, \sigma^2_{JB}\right)$ and $P_{T,B}$ is the power budget for additional jamming. However, the additional jamming transmission via full-duplex techniques causes an undesired feedback loop from the receiver output to the receiver input through self-interference channel h_{BB}. Theoretically, self-interference can be canceled perfectly down to the level of the noise floor [31], [32]. However, in practice, the cancellation cannot be perfect and a certain level of the self-interference remains due to the estimation error of the self-interference channel, non-ideal operation of digital-to-analog converter (DAC), and amplifier nonlinearity [33]. The average residual loop interference after self-interference cancellation is expressed as [34], [35].

$$E\left\{\left\|\boldsymbol{J}_B(n)\,\tilde{\boldsymbol{h}}_{BB}\right\|^2\right\} = \beta P_{JB}, \tag{11}$$

where $\tilde{\boldsymbol{h}}_{BB}$ represents the channel estimation error of h_{BB} and β is the average residual self-interference ratio

$(0 \leq \beta \leq 1)$ after cancellation [36]–[38]. By substituting (11) for average residual self-interference, the power of the received signal at Bob in (5), P_B, can be expressed as

$$P_B = P_S d_{AB}^{-a} + \beta P_{JB} + \sigma_n^2. \tag{12}$$

We note that the value of β is determined based on the hardware and self-interference cancellation techniques after the jamming strategy is established. Then, the jamming power is allocated according to the value of β. We emphasize that the transmitted jamming power is related to the value of β, not to channel change, showing how we should perform jamming power allocation at the receiver. Moreover, the self-interference from excessive jamming power at the receiver can lead to performance degradation of the secrecy communication link. Therefore, to establish optimal friendly jamming strategies, we should consider the impacts of the jamming power and the self-interference jointly at the receiver. We will discuss the impact of self-interference and the corresponding secrecy performance in Section IV.

III. ACHIEVABLE SECRECY PERFORMANCE

In this section, we evaluate the secrecy performance under two scenarios of general and intelligent eavesdropping, assuming that smart eavesdroppers can nullify friendly jamming signals from the transmitter. We model the signal to interference plus noise ratios (SINR) of the main channel and the wiretap channel in our model, derive the probability density function (PDF) and the cumulative distribution function (CDF) to define secrecy capacity, and make an analysis of the secrecy performance.

A. PRELIMINARIES

Let $P_{K,ij}$ denote the transmission power. Here, K represents a type of the transmit signal among confidential data signal (S), jamming from Alice (J_A), and jamming from Bob (J_B), and ij stands for a link between Alice to Bob, Alice to Eve, Bob to Bob, and Bob to Eve, respectively (i.e., *AB, AE, BB, BE*). For notational simplicity, we define the normalized power values as

$$P_{S,AB} = \frac{P_S}{d_{AB}^a \sigma_n^2}, \quad P_{S,AE} = \frac{P_S}{d_{AE}^a \sigma_n^2}, \quad P_{JA,AE} = \frac{P_{JA}}{d_{AE}^a \sigma_n^2},$$
$$P_{JB,BB} = \frac{P_{JB}}{\sigma_n^2}, \quad P_{JB,BE} = \frac{P_{JB}}{d_{BE}^a \sigma_n^2}, \tag{13}$$

where the normalizing factors are the path loss and the AWGN component with variance σ_n^2. Then, the instantaneous SINR at Bob can be written as

$$\Gamma_B = \frac{P_S d_{AB}^{-a} \zeta_{AB}}{\beta P_{JB} + \sigma_n^2} = \frac{P_{S,AB} \zeta_{AB}}{\beta P_{JB,BB} + 1}, \tag{14}$$

where ζ_{ij} represents the channel gain $|h_{ij}|^2$ between node i and j. The instantaneous SINR of the passive (P) Eve is

$$\Gamma_{(P)E} = \frac{P_{S,AE} \zeta_{AE}}{P_{JA,AE} \zeta_{AE} + 1}, \tag{15}$$

where the passive eavesdropper is fully affected by the transmitted friendly jamming. On the other hand, the smart eavesdropper can eliminate the friendly jamming from Alice, so that the instantaneous SINR at the smart Eve can be written as

$$\Gamma_{(S)E} = \frac{P_{S,AE} \zeta_{AE}}{\epsilon P_{JA,AE} \zeta_{AE} + P_{J2,BE} \zeta_{BE} + 1}. \tag{16}$$

Note that if $\epsilon = 1$, we can also see the additional jamming effect of Bob in the passive Eve case. We will compare effects of additional jamming with conventional jamming from Alice in Section V.

The secrecy capacity can be used to assess the security of the legitimate user from Eve, defined as the difference between the main channel capacity $C_B = \log_2 (1 + \Gamma_B)$ and the wiretap channel capacity $C_E = \log_2 \left(1 + \Gamma_{(i)E}\right)$ of passive Eve ($i = P$) and smart Eve ($i = S$). Therefore, the secrecy capacity is expressed as [3]

$$C_S = \begin{cases} (C_B - C_{(i)E})^+ & \text{if } \Gamma_B > \Gamma_{(i)E} \\ 0 & \text{if } \Gamma_B < \Gamma_{(i)E}, \end{cases} \tag{17}$$

where $(x)^+ = \max(x, 0)$. In the presence of fading, these capacities can be modeled as random variables that vary with the instantaneous SINRs.

B. SECRECY OUTAGE PROBABILITY

The SOP, introduced to measure the secrecy performance of wireless communication [3], [4], is defined as the probability that the secrecy capacity is less than a target secrecy rate η, expressed as

$$\begin{aligned} P_{out}(\eta) &= P\left[C_S < \eta | \Gamma_B > \Gamma_{(i)E}\right] P\left[\Gamma_B > \Gamma_{(i)E}\right] \\ &\quad + P\left[C_S < \eta | \Gamma_B \leq \Gamma_{(i)E}\right] P\left[\Gamma_B \leq \Gamma_{(i)E}\right]. \end{aligned} \tag{18}$$

Since $P[C_S < \eta | \Gamma_B \leq \Gamma_{(i)E}] = 1$, the SOP can be expressed as (similar to [4])

$$P_{out}(\eta) = \int_0^{\infty} F_B\left(2^\eta (1 + \gamma_E) - 1\right) f_{(i)E}(\gamma_E)\, d\gamma_E, \tag{19}$$

where $F_B(\cdot)$ is the CDF of Γ_B and $f_{(i)E}(\cdot)$ is the PDF of $\Gamma_{(i)E}$.

In this section, we assume that the smart Eve uses the MRC scheme [27] with the eavesdropping channel gain (ζ_{AE}) between Alice and Eve, and ζ_{BE} follows the chi-square distribution. Note that Eve cannot estimate the channel state between Bob and Eve as there is no transmission of pilots and feedback messages. We then derive the SOP in the presence of smart eavesdropper as follows.

Lemma 1: In the presence of smart eavesdropper, the SOP is obtained by

$$\begin{aligned} &P_{out}(\eta) \\ &= \int_0^{\frac{P_{S,AE}}{\epsilon P_{JA,AE}}} F_B\left(2^\eta (1 + \gamma_E) - 1\right) f_{(S)E}(\gamma_E)\, d\gamma_E \\ &= \int_0^{\underline{P_{S,AE}}} \quad \epsilon P_{JA,AE} \\ &\quad \times \left[1 - \exp\left(\frac{-(2^\eta (1+\gamma_E) - 1)\left(\beta P_{JB,BB}\overline{\zeta_{BB}} + 1\right)}{P_{S,AB}\overline{\zeta_{AB}}}\right)\right]^{N_B} \end{aligned}$$

$$\times\left(-\frac{1}{\overline{\zeta_{BE}}}\sum_{k=0}^{N_E-1}\sum_{n=0}^{k}\frac{\binom{k}{n}}{k!}\Gamma\left(n+1\right)\left(\psi_1'\psi_2\psi_3\right.\right.$$

$$\left.\left.+\psi_1\psi_2'\psi_3+\psi_1\psi_2\psi_3'\right)\right)d\gamma_E, \quad (20)$$

where ψ_i, $i = 1, 2, 3$, are given by

$$\psi_1 = \exp\left(\frac{-\gamma_E}{\overline{\zeta_{AE}}\left(P_{S,AE}-\gamma_E\epsilon P_{JA,AE}\right)}\right), \quad (21)$$

$$\psi_2 = \left[\frac{\gamma_E P_{JB,BE}^{\frac{n}{k}}}{\overline{\zeta_{AE}}(P_{S,AE}-\gamma_E\epsilon P_{JA,AE})}\right]^k, \quad (22)$$

$$\psi_3 = \left[\frac{\gamma_E P_{JB,BE}}{\overline{\zeta_{AE}}\left(P_{S,AE}-\gamma_E\epsilon P_{JA,AE}\right)}+\frac{1}{\overline{\zeta_{BE}}}\right]^{-n-1}. \quad (23)$$

and ψ_i' is the derivative of ψ_i, given by

$$\psi_1' = -\psi_1\frac{P_{S,AE}}{\overline{\zeta_{AE}}\left(P_{S,AE}-\gamma_E\epsilon P_{JA,AE}\right)^2}, \quad (24)$$

$$\psi_2' = k\left[\psi_2\right]^{\frac{k-1}{k}}\frac{P_{JB,BE}^{\frac{n}{k}}P_{S,AE}}{\overline{\zeta_{AE}}\left(P_{S,AE}-\gamma_E\epsilon P_{JA,AE}\right)^2}, \quad (25)$$

$$\psi_3' = \left(-n-1\right)\left[\psi_3\right]^{\frac{-n-2}{-n-1}}\frac{P_{S,AE}P_{JB,BE}}{\overline{\zeta_{AE}}\left(P_{S,AE}-\gamma_E\epsilon P_{JA,AE}\right)^2}. \quad (26)$$

Proof: See Appendix for the complete proof. ■

In the passive eavesdropper case without additional jamming at Bob, the SINR of Bob in (14) can be expressed as $\Gamma_B = P_{S,AB}\zeta_{AB}$ and the SOP can be derived with $\beta = 0$ in (20). Note that the SOP in (20) does not have a closed form expression, but it can be numerically obtained by computing softwares such as Matlab or Maple.

IV. COOPERATIVE JAMMING STRATEGIES

In order to improve the secrecy performance through cooperative jamming with the transmitter, we now discuss a power allocation strategy between Alice and Bob and the achievable secrecy performance according to the type of eavesdroppers. For successful collaborative jamming with Alice, Bob should simultaneously perform friendly jamming transmission and successful decoding of the received signals. As the jamming power increases at Bob, the successful decoding probability can decrease due to the self-interference while the eavesdropping probability is degraded as well. Therefore, in this section, we determine the transmission power for the confidential data and the jamming signal at Alice and Bob, so as to minimize the SOP with the limited power budgets in (4) and (10). We also consider different eavesdropper models. Our power allocation problem can be formulated as

$$\begin{aligned}&\min P_{out}\left(P_S, P_{JA}, P_{JB}\right)\\ &\text{s.t. } P_S + P_{JA} \leq P_{T,A}\\ &\qquad P_{JB} \leq P_{T,B},\end{aligned} \quad (27)$$

where $P_{T,A}$ and $P_{T,B}$ are the power budgets at Alice and Bob, respectively. The non-convexity of the power optimization problem in (27) makes it difficult to obtain a solution for power allocation. We can find the optimal points of (27) through brute-force search for different types of Eve by adjusting the discretized level of variables.

We define the two jamming strategies: Alice's jamming only (AJ) and cooperative jamming (CJ) of Alice and Bob. To guarantee high secrecy performance, we establish power allocation strategies with the constraints of the average residual self-interference ratio (β) and the remaining jamming interference ratio (ϵ).

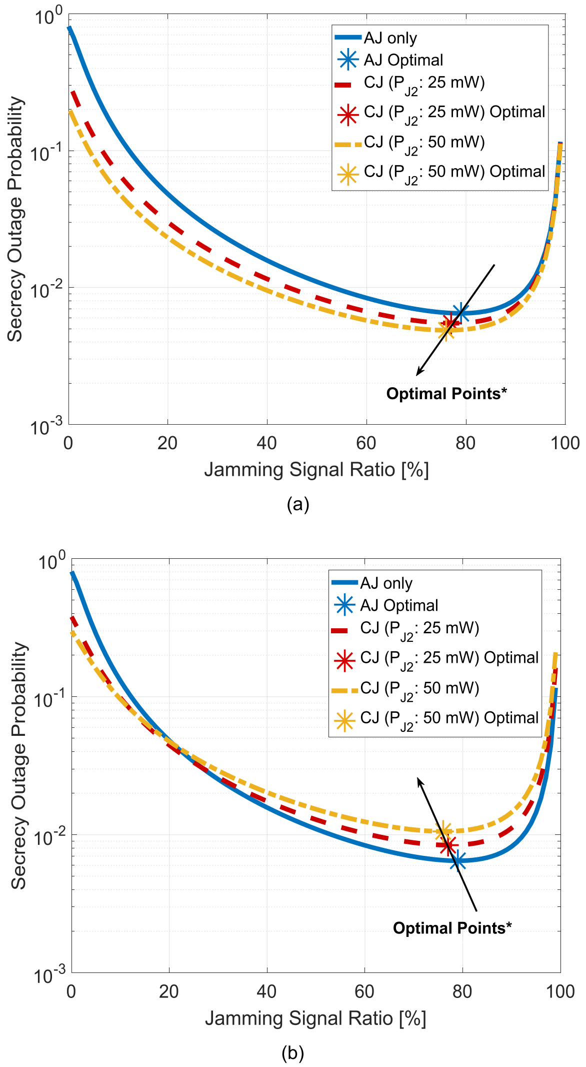
As aforementioned, since the passive eavesdropper cannot cancel the jamming signal, we can easily achieve communication secrecy by using only AJ without the help of Bob's jamming transmission. Moreover, the CJ transmission of the receiver in case of $\beta = 0$ can help to enhance the secrecy performance while self-interference at the receiver may not be perfectly canceled for $\beta > 0$ due to unstable spatial suppression and imperfect time domain cancellation. Hence, we should consider a proper power allocation strategy of CJ for passive eavesdroppers.

The smart eavesdropper can cancel the null-space jamming of the transmitter by eavesdropping the CSI of the main channel. Since the jamming strategy of the TX jammer can no longer improve the secrecy performance, we should achieve secrecy with the help of our proposed CJ scheme (i.e., a receiver-assisted scheme). However, the receiver that performs data signal receptions and jamming transmissions can experience poor reception performances because it cannot completely cancel self-interference, described in subsection II-C. Therefore, the receiver needs to adjust the jamming power (P_{JB}) appropriately based on the amount of transmission power (P_S, P_{JA}) of the transmitter and the self-interference effect in (11) from receiver jamming. In order to establish a cooperative power allocation strategy for smart eavesdroppers, we compare the influences of the average residual self-interference (β) of Bob and the cancellation capability (ϵ) of the eavesdropper in subsection V-A.

To build the same jamming strategy with a half-duplex receiver, one needs an external jammer (Charlie) that should be precisely synchronized with the transmitter. The friendly jamming of the external jammer requires secret key pre-distribution between Bob and Charlie, causing additional security vulnerability and cost increase. On the other hand, the full-duplex cooperative jammer in our model can be cost-effective since it there is no need of an external jammer.

V. NUMERICAL RESULTS

In this section, we assume that the three nodes (Alice, Bob, and Eve) are located at the same distance between each other (i.e., $D_{AB} = D_{AE} = D_{BE}$), and verify the friendly jamming efficiency with the target secrecy rate $\eta = 0.1$[4]. In the numerical analysis, the numbers of node antennas are assumed to be $N_A = 2$, $N_B = 2$, and $N_E = 3$, respectively, and the power budget of the receiver is set to $P_{T,B} = 50$ mW, which is 50 % of the transmitter power $P_{T,A} = 100$ mW.



(a)

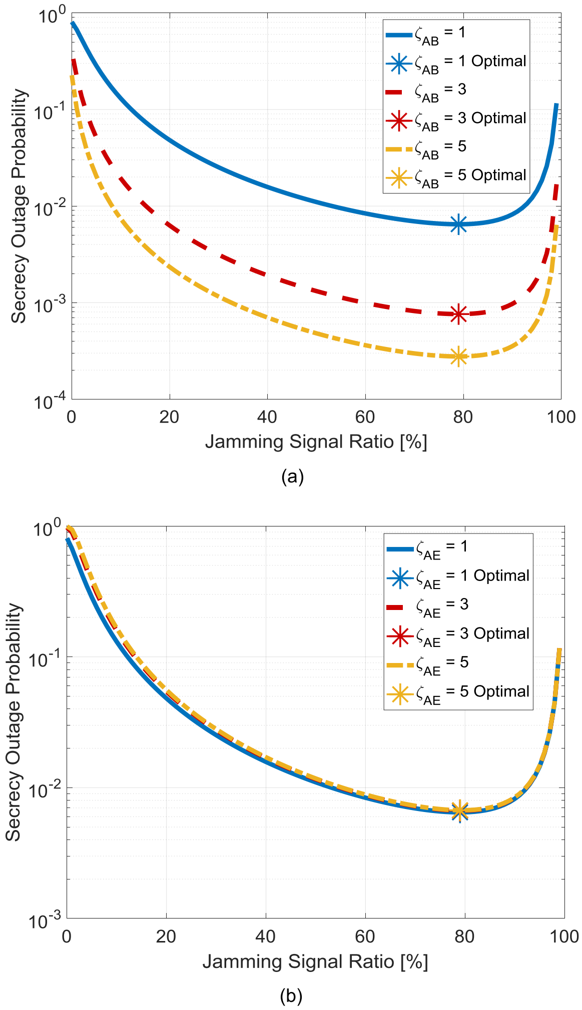
(b)

FIGURE 4. Secrecy performance under different self-interference levels ((a) $\beta = 0$ % or (b) $\beta = 1$ %). The power budgets of Alice and Bob are assumed to be $P_S + P_{JA} \leq 100$ mW and $P_{JB} \leq 50$ mW, respectively.

A. SECRECY PERFORMANCE

1) PASSIVE EAVESDROPPERS

In the passive eavesdropper case, Fig. 4 shows secrecy performances under different self-interference effects by the transmitted jamming power level (P_{JB}) at the receiver. The optimal results of the AJ scheme with $P_{JB} = 0$ have been numerically obtained. One intuitive solution of giving an additional secrecy margin to the legitimate receiver can lead to different results depending on the amount of the residual self-interference. Fig. 4(a) shows that additional jamming (P_{JB}) by the receiver is always helpful due to no residual self-interference on the receiver. Hence, the secrecy performance improves and Alice can save the power consumption of P_{JA} at the expense of P_{JB}. The optimal points of jamming to signal ratio (JSR), which is defined to be $P_{JA}/(P_S + P_{JA})$, head to the bottom left with the increase of the JSR. We see that the objective in (27) is a decreasing function with respect to P_S. Therefore, it is optimal to allocate all the remaining power of $P_{T,A} - P_{JA}$ to P_S, always making the power constraint of the transmitter active at $P_S + P_{JA} = P_{T,A}$. On the contrary, Fig. 4(b) presents that even a small amount of the residual self-interference by receiver jamming can cause considerable degradation of the secrecy performance. For JSR > 20 %, the secrecy performance of the CJ is worse than that of the AJ because the residual self-interference is stronger than the received signal power from Alice to Bob. The optimal points move differently from those of Fig. 4(a). Therefore, in order to use the CJ scheme effectively, a countermeasure must be taken to eliminate the self-interference in advance and a CJ strategy between Alice and Bob should be established.



(a)

(b)

FIGURE 5. Secrecy outage probabilities under different instantaneous channel gains of (a) the legitimate receiver and (b) the eavesdropper.

Fig. 5 shows one of the advantages of friendly jamming: the secrecy performance does not depend on the eavesdropper channel gains. Fig. 5(a) illustrates that the secrecy performance improves according to the increasing channel gain

$\overline{\zeta_{AB}}$ at the receiver. On the other hand, in Fig. 5(b), even if $\overline{\zeta_{AE}}$ increases up to 5 dB compared with $\overline{\zeta_{AB}}$, the outage probability seldom changes. This is because the receiver power levels of both the data signal and the jamming signal go up according to the increase of the eavesdropper channel gain. Therefore, the passive Eve, which is not a compelling threat, can be easily mitigated through a jamming transmission at the transmitter as in most previous work. On the other hand, it will be challenging to protect from powerful eavesdroppers, which will be a more practical scenario in the future [40], [41].

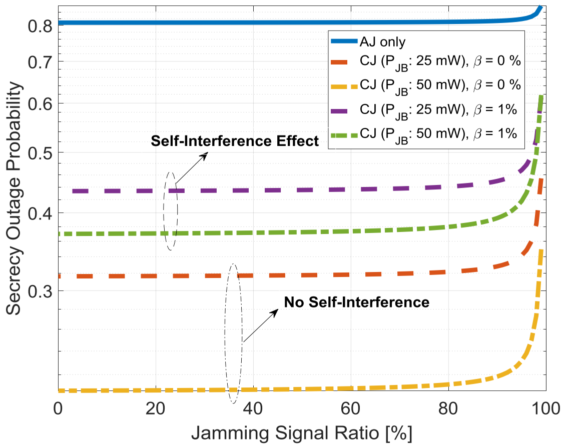
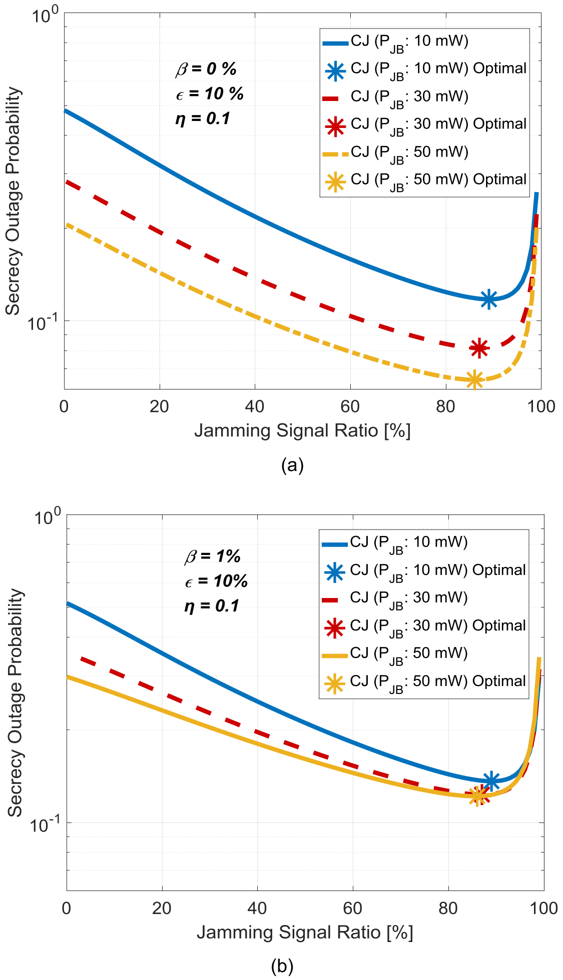


FIGURE 6. **Comparison of secrecy performances for different power allocation strategies with the smart Eve. The self-interference impact is verified under the different RX-Jamming power of 25 mW and 50 mW.**

2) SMART EAVESDROPPERS

In the ideal smart eavesdropper case of $\epsilon = 0$, Fig. 6 shows the difference of outage probabilities due to the self-interference effect between AJ and CJ schemes. When the jamming power increases over most ranges of JSR, the outage probability of the AJ scheme stays at higher than 0.8 due to the perfect cancellation capability of the ideal smart eavesdropper, which concludes that the AJ scheme shows worse secrecy performances than the CJ scheme in general. Nevertheless, the CJ scheme may suffer from self-interference even after cancellation at the receiver. For example, the average residual self-interference of $\beta = 1$ % with $P_{JB} = 50$ mW increases the secrecy outrage probability by more than 1.5 times compared with the case of no self-interference of $\beta = 0$. In both cases of $\beta = 0$ and 1 %, stronger jamming signals should be transmitted at the receiver, and then lower outage probabilities can be achieved. The best power allocation strategy is to set as $P_S = P_{T,A}^{Max}$, $P_{JA} = 0$, and $P_{JB} = P_{T,B}^{Max}$, but usually infeasible due to the limited power budget of transceivers.



(a)

(b)

FIGURE 7. **Comparison of secrecy outage probabilities according to the amount of average residual self-interference (a) $\beta = 0$ and (b) 1 % in the practical eavesdropper case ($\epsilon = 10$ %).**

In the practical smart eavesdropper case of $\epsilon = 10$ %, Fig. 7 compares secrecy performances based on the optimal power allocation of (27) without and with self-interference: $\beta = 0$ in (a) and 1 % in (b). Each star (*) marker represents the minimal outage point with a different amount of P_{JB}. Fig. 7(a) shows lower outage probability values than Fig. 7(b) due to the ideal receiver jamming performance with no residual self-interference. On the contrary, Fig. 7(b) shows that the outage probability is affected by self-interference significantly, even with a small amount of the average residual self-interference, $\beta = 1$ %. In this case, the best power allocation strategy is $P_S = 14$ mW, $P_{JA} = 86$ mW, $P_{JB} = 50$ mW, obtained by (27). In both cases (a) and (b), the optimal points move to right down gradually, implying that the transmitter can achieve the same secrecy performance with the help of P_{JB} to make up for the decreasing amount of P_{JA}.

The improvement of secrecy performances is much less significant in Fig. 7(b) than (a) because the increase of P_{J2} can do harm in the form of self-interference. Therefore, in the practical smart eavesdropper case, it is essential to consider self-interference for efficient power allocation between Alice and Bob in the cooperative jamming strategy. Next, we will discuss the power expenditure, considering the self-interference effect at the receiver, the jamming cancellation capability of the eavesdropper, and the path loss in the secrecy region.

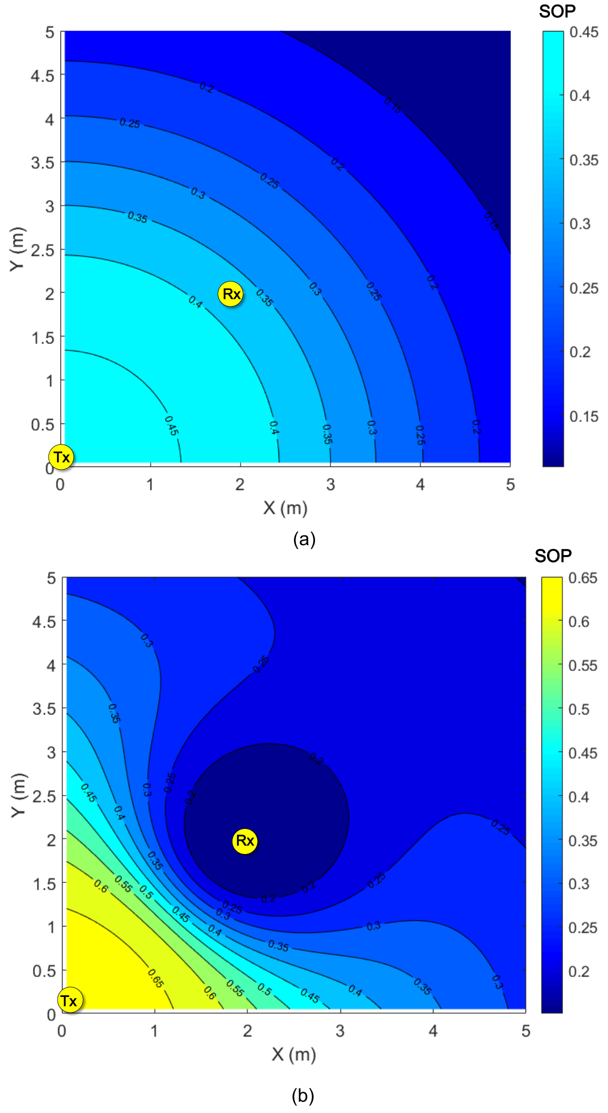
B. SECRECY REGION

In the previous subsection, we observed achievable secrecy performances according to the eavesdropping capability and the self-interference residuals under the fixed deployment of nodes (i.e., $D_{AB} = D_{AE} = D_{BE}$). Here we evaluate the secrecy region as the eavesdropping attack point changes with the path-loss exponent $a = 4$. We assume a two-dimensional plane, where Alice is located at $(0, 0)$ and Bob at $(2, 2)$. We set the average residual self-interference at $\beta = 1$ % and the residual jamming interference at $\epsilon = 10$ %. The best power allocation strategy of $P_S = 14$ mW, $P_{JA} = 86$ mW, and $P_{JB} = 50$ mW is used. Average channel gains are assumed to be $\overline{\zeta_{AB}} = \overline{\zeta_{AE}} = \overline{\zeta_{BE}} = 1$, to focus more on the impact of Eve location changes.

Note that in the practical condition we do not know exactly where the eavesdropper is located and what the channel state is. However, from results of this section, we can obtain the information of which areas are more vulnerable to security, helping to establish an effective friendly jamming strategy. If we can estimate a suspicious location of a malicious node, we can enhance the secrecy performance through an advanced jamming scheme which can adapt jamming signals based on the instantaneous channel gains [42].

Fig. 8 shows the secrecy regions of the AJ and CJ schemes in the presence of the passive eavesdropper. Fig. 8(a) illustrates better security performances as the Eve location moves away from Alice. With the AJ scheme, Alice transmits jamming signals and confidential messages together, so that the closer the Eve is to Alice, the more degradation the security suffers from. To countermeasure this, it is necessary to increase jamming power or to use the cooperative jamming technique. Fig. 8(b) shows the secrecy region using the CJ technique, which can cover a wider area with the improved security, compared with AJ. It is interesting to observe the outage probabilities near to the source (Alice) higher than those of the AJ scheme in Fig. 8(a). Nevertheless, the degradation of the security performance due to self-interference does not mean an increase of the eavesdropping rate because the self-interference effect due to receiver jamming decreases the SINR of Bob only. In order to increase the channel capacity of Bob, we should consider a more advanced self-interference cancellation technique.

Nevertheless, the degradation of the secrecy performance due to self-interference does not mean an increase of the eavesdropping rate because the self-interference effect due to receiver jamming decreases the SINR of Bob only. In order to increase the channel capacity of Bob, we should consider a more advanced self-interference cancellation technique.



(a)

(b)

FIGURE 8. In case of passive eavesdropper, comparison of secrecy regions of (a) AJ and (b) CJ scheme.

Fig. 9 shows secrecy regions with security differences of AJ and CJ schemes in the smart eavesdropper case. In Fig. 9(a), most areas are threatened seriously, unless the eavesdropper is far enough away from Alice. We can see that it is very difficult to achieve security from the enhanced eavesdropping attack and an additional jamming scheme should be considered to reinforce the AJ scheme. Fig. 9(b) shows the improved secrecy region by using the AJ scheme together with additional jamming. In this case, the secrecy performance around Bob is similar to the passive eavesdropper case of Fig. 8(b). We can see that the CJ scheme can enhance secrecy performances near Bob. It is difficult to improve outage probabilities near Alice, but realistic places for eavesdroppers to conceal may be near Bob. Hence, the proposed solution is reasonable for providing security, and a more sophisticated power control will be required to support the self-interference cancellation capability.

C. POWER EXPENDITURE

From the results of the previous subsection, we realize that the better cancellation capability of the eavesdropper requires

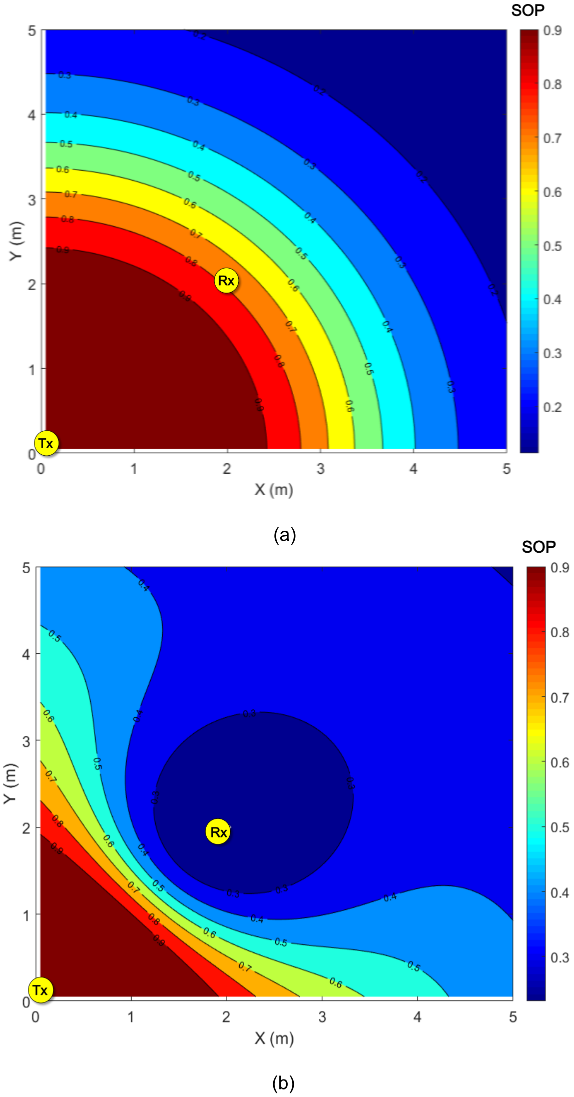


FIGURE 9. In case of smart eavesdropper, comparison of secrecy regions of (a) AJ and (b) CJ scheme ($\beta = 1$ % and $\epsilon = 10$ %).

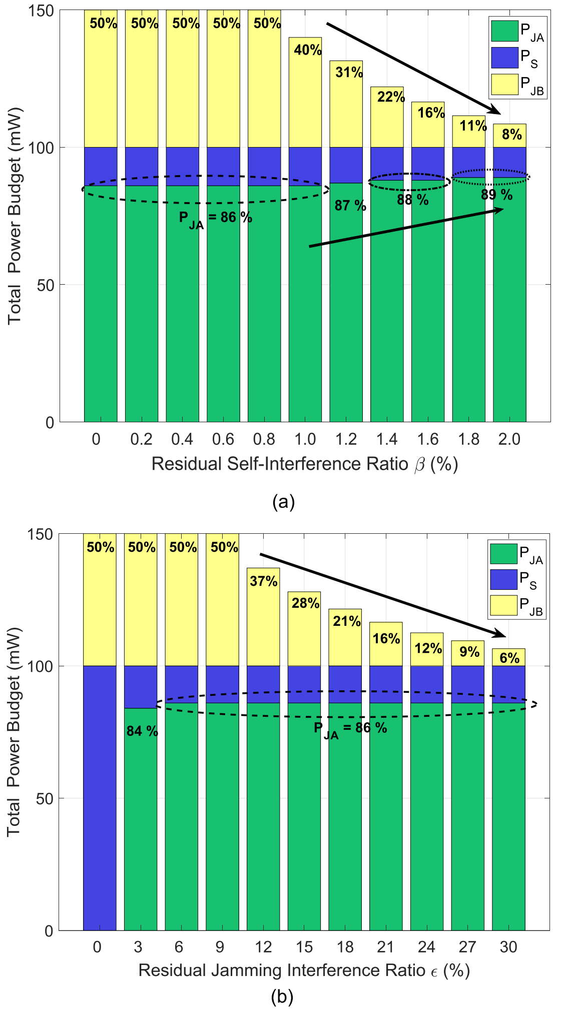


FIGURE 10. Comparison of the power expenditure to minimize secrecy outage probabilities under (a) increasing β or (b) increasing ϵ. The total power budget is 150 mW (Alice: 100 mW, Bob: 50 mW).

more jamming power at the receiver. However, because stronger jamming power at the receiver causes a stronger self-interference impact, we should plan power expenditure considering both β and ϵ for optimal power allocation in the limited power budget.

Fig. 10 describes the change of the optimal power expenditure to minimize the outage probability according to the self-interference effect of Bob and the cancellation capability of Eve. Our simulations are performed in the condition of the fixed node locations with $D_{AB} = D_{AE} = D_{BE}$. We assumed $\epsilon = 10$ % and $0 \leq \beta \leq 2$ % in Fig. 10(a), and $\beta = 1$ % and $0 \leq \epsilon \leq 30$ % in Fig. 10(b).

To reduce the computational cost of the brute-force search, we discretize P_S, P_{JA} and P_{JB}, which decide the complexity in solving (27). In Fig. 10, the simulations were performed with the discretized level of 1 mW in the total power budget ($0 \leq P_S + P_{JA} \leq 100\ mW, 0 \leq P_{JB} \leq 50\ mW$). Even if the levels were further refined (e.g., 0.1 mW), only the computation time increased without improving results much. Hence, our brute-force search can find the optimal solution in reasonably low complexity.

Fig. 10(a) illustrates how the power allocation of the full-duplex jamming receiver should be performed from the point view of a system when the residual interference increases. The increase of P_{JA} reduces P_S in terms of the limited power budget in (4) and the self-interference from P_{JB} degrades secrecy performances. It is observed that with $\beta \geq 1.4$ %, the additional jamming power (P_{JB}) should be reduced to less than a half of the power budget at the receiver because the impact of the average residual self-interference is more significant than the obtained secrecy performance by using P_{JB}. Fig. 10(b) shows that the eavesdropper can be mitigated with less jamming power (P_{JB}) required. In case of $\epsilon = 0$, the best strategy of power allocation to minimize the outage probability is only using P_S and P_{JB} without P_{JA}, since the eavesdropper can perfectly cancel the jamming signal (P_{JA}).

On the other hand, in case of $\epsilon > 0$, the JSR of the transmitter maintains almost 86 % regardless of P_{JB} and ϵ. Thus, we can conclude that the additional jamming with high power does not always obtain desirable secrecy results.

The cooperative jammer in practice may require fast calculation of β and high capability of the self-interference canceller, which is costly with feedback overhead. Therefore, the system designer may have to sacrifice performance to reduce cost and complexity. The capability of self-interference cancellation is another important parameter to determine the real system performance. In an experimental level [31], it is possible to cancel up to -110 dB, indicating that our solution using full-duplex technology can be implemented in Wi-Fi networks.

VI. CONCLUSION

We have investigated the impact of passive and smart eavesdropping attacks in the MIMO wiretap scenario for physical layer security. Intelligent eavesdropping attacks can cause a severe security problem because the smart eavesdropper can cancel friendly jamming by stealing the CSI between legitimate nodes. To solve this problem, we have proposed the CJ strategies that optimize power allocation between the transmitter and the receiver. This receiver-assisted scheme significantly increases the secrecy performance of the entire system because the eavesdropper cannot obtain the CSI of Bob to Eve. We have demonstrated the efficacy of the proposed solution through the evaluation of secrecy regions even in the presence of the smart eavesdropper. However, excessive jamming power can lead to secrecy performance degradation due to residual self-interference. The analysis of power expenditure has shown the requirement of sophisticated power allocation schemes with self-interference into consideration.

One interesting future work is to evaluate our proposed method through a real test-bed based on the full-duplex system in the limited power scenarios such as sensor networks, military communications, and cellular networks. The proposed solution can be also extended to the multiple cooperative jammer scenario by taking into account the interference power increase, different self-interference cancellation levels, and performance degradation of legitimate receivers due to multiple jamming signals.

APPENDIX

Proof of Lemma 1: In (19), we first derive CDF of Γ_B in the presence of smart Eve as [26]

$$
\begin{aligned}
F_B(\gamma_B) &= P\left(\frac{P_{S,AB}\zeta_{AB,i}}{\beta P_{JB,BB}+1} < \gamma_B\right) \\
&= \prod_{k=1}^{\mathrm{N}_B} F_{\zeta_{AB,k}}\left(\zeta_{AB,k} < \frac{\gamma_B(\beta P_{JB,BB}+1)}{P_{S,AB}}\right) \\
&= \left[1-\exp(\frac{-\gamma_B\left(\beta P_{JB,BB}\overline{\zeta_{BB}}+1\right)}{P_{S,AB}\overline{\zeta_{AB}}})\right]^{\mathrm{N}_B}, \qquad (28)
\end{aligned}
$$

where i is the index selected by the SC scheme in (1). To derive the PDF of $\Gamma_{(S)E}$, we first obtain the CDF of $\Gamma_{(S)E}$ as

$$
\begin{aligned}
F_{(S)E}(\gamma_E) &= P\left[\frac{P_{S,AE}\zeta_{AE}}{\epsilon P_{JA,AE}\zeta_{AE}+P_{JB,BE}\zeta_{BE}+1} < \gamma_E\right] \\
&= P\left[\zeta_{AE} < \frac{\gamma_E P_{JB,BE}\zeta_{BE}+\gamma_E}{P_{S,AE}-\gamma_E\epsilon P_{JA,AE}}\right] \\
&= \int_0^{\infty}\int_0^{h(\zeta_{BE})} f_{Z_{AE}}(\zeta_{AE}) f_{Z_{BE}}(\zeta_{BE})\, d\zeta_{AE} d\zeta_{BE},
\end{aligned}
\qquad (29)
$$

where $h(\zeta_{BE}) = \frac{\gamma_E P_{JB,BE}\zeta_{BE}+\gamma_E}{P_{S,AE}-\gamma_E\epsilon P_{JA,AE}}$. From (29), the CDF of $\Gamma_{(S)E}$ can be derived as

$$
\begin{aligned}
F_{(S)E}(\gamma_E) &= \int_0^{\infty}\int_0^{h(\zeta_{BE})} \frac{\zeta_{AE}^{N_E-1}}{\overline{\zeta_{AB}}^{\mathrm{N}_E}\Gamma(Ne)} \\
&\quad \times \exp\left(\frac{-\zeta_{AE}}{\overline{\zeta_{AE}}}\right)\frac{1}{\overline{\zeta_{BE}}}\exp\left(\frac{-\zeta_{BE}}{\overline{\zeta_{BE}}}\right) d\zeta_{AE} d\zeta_{BE} \\
&= \int_0^{\infty}\left[1-\exp\left(\frac{-h(\zeta_{BE})}{\overline{\zeta_{AE}}}\right)\sum_{k=0}^{N_E-1}\frac{\left(\frac{h(\zeta_{BE})^k}{\overline{\zeta_{AE}}}\right)}{k!}\right] \\
&\quad \times\left[\frac{1}{\overline{\zeta_{BE}}}\exp\left(\frac{-\zeta_{BE}}{\overline{\zeta_{BE}}}\right)\right] d\zeta_{BE} \qquad (30) \\
&= 1-\frac{1}{\overline{\zeta_{BE}}}\int_0^{\infty}\exp\left(\frac{-h(\zeta_{BE})}{\overline{\zeta_{AE}}}\right)\exp\left(\frac{-\zeta_{BE}}{\overline{\zeta_{BE}}}\right) \\
&\quad \times\sum_{k=0}^{N_E-1}\frac{\left(\frac{h(\zeta_{BE})}{\overline{\zeta_{AE}}}\right)^k}{k!} d\zeta_{BE} \qquad (31)
\end{aligned}
$$

By applying the binomial expansion to (31), we can derive the CDF of $F_{(S)E}(\gamma_E)$ as (32)-(34), as shown at the top of the next page. Finally, according to the gamma distribution formula with the gamma function $\Gamma(\cdot)$, the outage probability in (29) can be written as

$$
F_{(S)E}(\gamma_E) = 1-\sum_{k=0}^{N_E-1}\sum_{n=0}^{k}\frac{\binom{k}{n}}{k!}\Gamma(n+1)(\psi_1\psi_2\psi_3), \qquad (35)
$$

where $\Gamma(\cdot)$ denotes the Gamma function [39, Eq. (8.310.1)] and ψ_i, $i = 1, 2, 3$ are in (21)-(23). Finally, we obtain the PDF of $\Gamma_{(\mathrm{S})\mathrm{E}}$ by differentiating (35) as

$$
\begin{aligned}
f_{(S)E}(\gamma_E) &= \frac{d}{d\gamma_E}F_{(S)E}(\gamma_E) \\
&= -\frac{1}{\overline{\zeta_{BE}}}\sum_{k=0}^{Ne-1}\sum_{n=0}^{k}\frac{\binom{k}{n}}{k!}\Gamma(n+1) \\
&\quad \times(\psi_1'\psi_2\psi_3+\psi_1\psi_2'\psi_3+\psi_1\psi_2\psi_3'), \qquad (36)
\end{aligned}
$$

where ψ_i', $i = 1, 2, 3$ are in (24)-(26).

From (16), γ_E cannot be greater than $\frac{P_{S,AE}}{\epsilon P_{JA,AE}}$, so the integration interval of γ_E should be up to $\frac{P_{S,AE}}{\epsilon P_{JA,AE}}$ in (20). Therefore, by plugging (28) and (36) in (19), we obtain the SOP in (20).

$$
\begin{aligned}
&F_{(S)E}\left(\gamma_E\right)\\
&= 1 - \frac{1}{\overline{\overline{\zeta_{BE}}}} \sum_{k=0}^{N_E-1} \frac{1}{k!} \int_0^\infty \exp\left(\frac{-h(\zeta_{BE})}{\overline{\zeta_{AE}}} + \frac{-\zeta_{BE}}{\overline{\zeta_{BE}}}\right)\left(\frac{h(\zeta_{BE})}{\overline{\zeta_{AE}}}\right)^k d\zeta_{BE} \qquad (32)\\
&= 1 - \frac{1}{\overline{\overline{\zeta_{BE}}}} \sum_{k=0}^{N_E-1} \frac{1}{k!} \int_0^\infty \exp\left(\frac{-\zeta_{BE}\left(\overline{\zeta_{BE}}\gamma_E P_{JB,BE} + \overline{\zeta_{AE}} P_{S,AE} - \gamma_E \beta P_{JA,AE}\overline{\zeta_{AE}}\right) - \overline{\zeta_{BE}}\gamma_E}{\overline{\zeta_{AE}\zeta_{BE}}\left(P_{S,AE} - \gamma_E\beta P_{JA,AE}\right)}\right)\left(\frac{h(\zeta_{BE})}{\overline{\zeta_{AE}}}\right)^k d\zeta_{BE} \qquad (33)\\
&= 1 - \frac{1}{\overline{\overline{\zeta_{BE}}}}\psi_1 \sum_{k=0}^{N_E-1} \frac{1}{k!} \int_0^\infty \exp\left(-\zeta_{BE}\frac{\overline{\zeta_{BE}}\gamma_E P_{JB,BE} + \overline{\zeta_{AE}} P_{S,AE} - \gamma_E \beta P_{JA,AE}\overline{\zeta_{AE}}}{\overline{\zeta_{AE}\zeta_{BE}}\left(P_{S,AE} - \gamma_E\beta P_{JA,AE}\right)}\right)\left(\frac{\gamma_E P_{JB,BE}\zeta_{BE} + \gamma_E}{\overline{\zeta_{AE}}\left(P_{S,AE} - \gamma_E\beta P_{JA,AE}\right)}\right)^k d\zeta_{BE}, \qquad (34)
\end{aligned}
$$

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2006, pp. 356–360.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[6] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[7] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.

[9] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[10] G. Chen and J. P. Coon, "Secrecy outage analysis in random wireless networks with antenna selection and user ordering," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 334–337, Jun. 2017.

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[12] Y. Fan, X. Liao, and A. V. Vasilakos, "Physical layer security based on interference alignment in K-user MIMO Y wiretap channels," *IEEE Access*, vol. 5, pp. 5747–5759, Apr. 2017.

[13] N. Li, X. Tao, and J. Xu, "Artificial noise assisted communication in the multiuser downlink: Optimal power allocation," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 295–298, Feb. 2015.

[14] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620–19630, Sep. 2017.

[15] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[16] J. Kim and J. P. Choi, "Cancellation-based friendly jamming for physical layer security," in *Proc. IEEE GLOBECOM*, Dec. 2016, pp. 1–6.

[17] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

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

[19] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[20] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[21] Y. Zeng and R. Zhang, "Active eavesdropping via spoofing relay attack," in *Proc. IEEE ICASSP*, Mar. 2016, pp. 2159–2163.

[22] F. Wu, W. Wang, B. Yao, and Q. Y. Yin, "Effective eavesdropping in the artificial noise aided security scheme," in *Proc. IEEE/CIC Int. Conf. Commun. China*, Aug. 2013, pp. 214–218.

[23] F. Wu, W. J. Wang, and H. M. Wang, "A unified mathematical model for spatial scrambling based secure wireless communication and its wiretap method," *Sci. Sin. Inform.*, vol. 42, no. 4, pp. 483–492, Apr. 2012.

[24] L. Liu, J. Liang, and K. Huang, "Eavesdropping against artificial noise: Hyperplane clustering," in *Proc. IEEE Int. Conf. Inf. Sci. Technol.*, Mar. 2013, pp. 1571–1575.

[25] J. Choi and Y.-H. Lee, "Optimum pilot pattern for channel estimation in OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 2083–2088, Sep. 2005.

[26] W. C. Jakes, *Microwave Mobile Communications*, 1st ed. New York, NY, USA: Wiley, 1974.

[27] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[28] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE ICC*, May 2010, pp. 1–6.

[29] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[30] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[31] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM*, Aug. 2013, pp. 375–386.

[32] J. Kim, W. Jeon, K.-J. Park, and J. P. Choi, "Coexistence of full-duplex based IEEE 802.15.4 and IEEE 802.11," *IEEE Trans. Ind. Informat.*, to be published.

[33] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[34] T. Snow, C. Fulton, and W. J. Chappell, "Transmit–receive duplexing using digital beamforming system to cancel self-interference," *IEEE Trans. Microw. Theory Techn.*, vol. 59, no. 12, pp. 3494–3503, Dec. 2011.

[35] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[36] J. Lee and T. Q. S. Quek, "Hybrid full-/half-duplex system analysis in heterogeneous wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2883–2895, May 2015.

[37] D. W. K. Ng, E. S. Lo, and R. Schober, "Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1291–1304, May 2012.

[38] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.

[39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2007.

[40] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[41] K. Cumanan *et al.*, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2017.

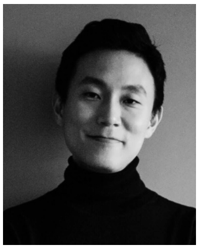
[42] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

JONGYEOP KIM (S'14) received the B.S. degree from Keimyung University, Daegu, South Korea, in 2013. He is currently pursuing the Ph.D. degree with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu. His research interests include the coexistence issues of wireless networks on the unlicensed band and physical-layer security.

JINWOONG KIM received the B.S. degree from Kyungpook National University, Daegu, South Korea, in 2017. He is currently pursuing the M.S. degree with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu. His research interests include the physical-layer security of wireless communication and information theory.

JEMIN LEE (S'06–M'11) received the B.S. (Hons.), M.S., and Ph.D. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2004, 2007, and 2010, respectively. She was a Post-Doctoral Fellow at the Massachusetts Institute of Technology, Cambridge, MA, USA, from 2010 to 2013, and a Temasek Research Fellow at iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, from 2014 to 2016. She is currently an Assistant Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. Her current research interests include physical-layer security, wireless communication security, ultra-dence networks, and machine-type communication.

Dr. Lee received the IEEE ComSoc AP Outstanding Paper Award in 2017, the IEEE ComSoc AP Outstanding Young Researcher Award in 2014, the Temasek Research Fellowship in 2013, and the Chun-Gang Outstanding Research Award in 2011. She served as a Guest Editor for the IEEE Wireless Communications, special issue on LTE in Unlicensed Spectrum, in 2016, and *Physical Communication* (Elsevier), special issues on Physical-Layer Security in 2016 and Heterogeneous and Small Cell Networks in 2014. She is currently an Editor of the IEEE Transactions on Wireless Communications and the IEEE Communications Letters.



JIHWAN P. CHOI (S'01–M'06–SM'17) received the B.S. degree from Seoul National University, Seoul, South Korea, in 1998, and the M.S. and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2000 and 2006, respectively. Until 2012, he was a Principal System Engineer with the Wireless Research and Development (R&D) Group, Marvell Semiconductor Inc., Santa Clara, CA, USA, for mobile system design and standardization of 4G wireless networks. He also served as a part-time ICT R&D Planner with the Institute for Information and Communications Promotion, South Korea, from 2016 to 2017, where he was designing government R&D projects and strategies on satellite communications. He is currently an Associate Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His research interests are in the cross-layer design of space and wireless networks, and the applications of machine learning.