Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8407297, 11 pages
https://doi.org/10.1155/2018/8407297

Research Article

Precoding-Aided Spatial Modulation for the Wiretap Channel with Relay Selection and Cooperative Jamming

Zied Bouida,[1] **Athanasios Stavridis**,[2] **Ali Ghrayeb**,[3,4] **Harald Haas**,[2] **Mazen Hasna**,[5] **and Mohamed Ibnkahla**[6]

[1]*Systems and Computer Engineering (SCE) Department, Carleton University, Ottawa, Canada*
[2]*The Institute for Digital Communications and the Joint Research Institute for Signal and Image Processing, School of Engineering, The University of Edinburgh, Edinburgh EH9 3JL, UK*
[3]*The Electrical and Computer Engineering Department, Texas A&M University at Qatar, Doha, Qatar*
[4]*Qatar Computing Research Institute (QCRI), Doha, Qatar*
[5]*The College of Engineering, Qatar University, Doha, Qatar*
[6]*Cisco Research Chair in Sensor Technology for the Internet of Things with the SCE Department, Carleton University, Ottawa, Canada*

Correspondence should be addressed to Zied Bouida; bouidazied@gmail.com

Received 17 February 2018; Revised 7 June 2018; Accepted 8 July 2018; Published 5 August 2018

Academic Editor: Yafei Hou

We propose in this paper a physical-layer security (PLS) scheme for dual-hop cooperative networks in an effort to enhance the communications secrecy. The underlying model comprises a transmitting node (Alice), a legitimate node (Bob), and an eavesdropper (Eve). It is assumed that there is no direct link between Alice and Bob, and the communication between them is done through trusted relays over two phases. In the first phase, precoding-aided spatial modulation (PSM) is employed, owing to its low interception probability, while simultaneously transmitting a jamming signal from Bob. In the second phase, the selected relay detects and transmits the intended signal, whereas the remaining relays transmit the jamming signal received from Bob. We analyze the performance of the proposed scheme in terms of the ergodic secrecy capacity (ESC), the secrecy outage probability (SOP), and the bit error rate (BER) at Bob and Eve. We obtain closed-form expressions for the ESC and SOP and we derive very tight upper-bounds for the BER. We also optimize the performance with respect to the power allocation among the participating relays in the second phase. We provide examples with numerical and simulation results through which we demonstrate the effectiveness of the proposed scheme.

1. Introduction

Due to the broadcast nature of the wireless propagation environment, information transmission security has been considered as prominent frontier in wireless communications [1]. In this context, physical-layer security (PLS) has been introduced in order to ensure confidential communication by applying communication techniques in the physical layer by exploiting the spatiotemporal characteristics of wireless channels [2]. The key idea behind PLS is to exploit different characteristics of both the main and the eavesdropper's channels [3]. The pioneering work on wiretap channel [4] has shown that perfect secrecy can be achieved if the eavesdropper's channel is a degraded version of the main channel. Later in [5], it has been shown that perfect secrecy can be achieved even if the eavesdropper's channel is on average better than the main channel, by exploiting the channel fading.

Due to the importance of physical-layer security, research work on this topic is gaining more and more interest in the context of next generation networks. In particular, information security is becoming very important in 5G systems where massive user connections and exponentially increasing wireless services are supported as investigated in [6, 7] and references therein. In this context, several techniques have been used in order to safeguard 5G systems. Focusing on precoding-aided spatial modulation and cooperative jamming, we provide in what follows the motivation behind each

of these techniques and how it contributes to 5G systems safeguarding.

In light of the above, a plethora of works has appeared in the literature, addressing different aspects of physical-layer security. Based on the concept of spatial modulation (SM) [8, 9] and owing to its spatial focusing property and its nondeterministic precoding algorithm, precoding-aided spatial modulation (PSM) has been presented as a suitable precoding technique to realize PLS [10–13]. In PSM, two types of modulations, namely, a variation of space shift keying (SSK) [14, 15] and conventional amplitude-phase modulation (APM), are jointly used to convey information. Specifically, Pre-SSK is implemented using the indices of receiver antennas rather than transmit antennas, with the aid of zero forcing precoding (ZFP) [16]. In this context, PSM employs two distinctive advantages: (i) additional information transmission in space domain and (ii) low-complexity detection [17]. Due to the several advantages of SM in terms of error performance, energy efficiency, and complexity (and PSM for all these advantages with additional security), it becomes a promising candidate for 5G systems [18, 19]. Therefore, using PSM for the security of 5G results from the combination of SM with additional security features.

While PSM has gained attention in the literature as a solution to enhance the secrecy performance of wiretap channels, this technique has not been studied in the context of cooperative communications where the secrecy performance can be further improved and fit more in 5G systems. Indeed, relays can be used to enhance the secrecy of the system by increasing the capacity of the main channel while reducing the capacity of the eavesdropper channel [20]. In this context, an appropriate relay selection is used in [21] to enhance the secrecy performance by taking eavesdroppers' links into consideration. In [22], relay selection with destination-based jamming under a total power constraint is proposed. While this technique enhances the secrecy performance, it assumes that Eve has no direct link with Alice and thus puts a limitation on the location of Eve. Moreover, it requires the channel state information (CSI) at the relays in order to select the best relay to the destination.

Considering a dual-hop cooperative scenario, we propose a PSM-based scheme aimed at enhancing the communication secrecy between Alice and Bob in the presence of a passive Eve. Assuming that Alice and Bob can only communicate through the help of a number of trusted relays, we use different techniques to enhance the secrecy communication between these nodes without putting any constraint on the location of Eve with respect to Alice and Bob. In this context, using PSM at Alice while simultaneously transmitting a jamming signal from Bob guarantees the secrecy during the first phase. In the second phase, the secrecy performance is enhanced through the use of jamming from multiple relays. Specifically, the relay selected by PSM detects and forwards the useful signal while other relays contribute to the jamming of the eavesdropper. In this paper, we analyze the performance of the proposed scheme in terms of the ergodic secrecy capacity (ESC) and secrecy outage probability (SOP) where we obtain closed-form expressions for those metrics. We also optimize the performance with respect to the power allocation among the participating relays in the second phase. We provide examples with numerical and simulations results through which we demonstrate the effectiveness of the proposed scheme.

In light of the above, the main contributions behind the work proposed in this paper can be summarized as follows:

(i) Taking advantage of its low probability of interception, PSM is extended in this paper to the cooperative communication scenario where Alice and Bob communicate through the help of N_R trusted relays.

(ii) While the secrecy performance for the first phase is enhanced using PSM, a cooperative jamming from multiple relays is considered to improve the secrecy performance during the second phase.

(iii) The ESC and SOP are derived in closed-form expressions and the results are confirmed for accuracy using Monte-Carlo simulations. Power allocation optimization is also given by simulation to further enhance the secrecy performance of the proposed scheme.

(iv) The ABEP upper-bound expressions at Bob and Eve are derived and the results are confirmed for accuracy using Monte-Carlo simulations. These results show the advantages of PSM and multirelay jamming during the first and the second phase, respectively. Indeed, the proposed techniques enhance the ABEP performance at Bob while degrading that of Eve.

The remainder of this paper is organized as follows. Section 2 defines the system and channel models and the mode of operation of the proposed PSM-based technique. Section 3 analyzes the secrecy performance in terms of the ESC and the OSC. Section 4 confirms this performance via selected numerical results. Section 5 concludes the paper.

Notation. In this paper, we use boldface uppercase and lowercase letters to, respectively, denote matrices and vectors. The Hermitian transpose, inverse, and trace of a matrix $\mathbf{A}$ are, respectively, represented by $\mathbf{A}^H$, $\mathbf{A}^{-1}$, and $tr(\mathbf{A})$. The N-dimensional identity matrix is denoted by $\mathbf{I}_N$. The Euclidean norm, Frobenius norm, absolute value, and real part are, respectively, represented by $\|\cdot\|$, $\|\cdot\|_{\mathrm{F}}$, $|\cdot|$, and $\Re\{\cdot\}$. $\mathbb{C}^{i\times j}$ stands for a set of complex matrices of $i \times j$ dimensions.

2. System and Channel Models

2.1. System Model. In Figure 1, we consider a secure dual-hop communication system between Alice and Bob through the help of N_r single-antenna trusted relays in the presence of an eavesdropper, Eve, where Alice has no direct link to Bob. The number of antennas of Alice, Bob, and Eve are denoted as N_a, N_b, and N_e, respectively. The practical number of antennas at these nodes depends on the used wireless and antenna technologies. Indeed, while current LTE devices can accommodate a maximum of four antennas, future 5G user equipment will accommodate a larger number of antennas thanks to the use of millimeter-wave and massive MIMO [23].

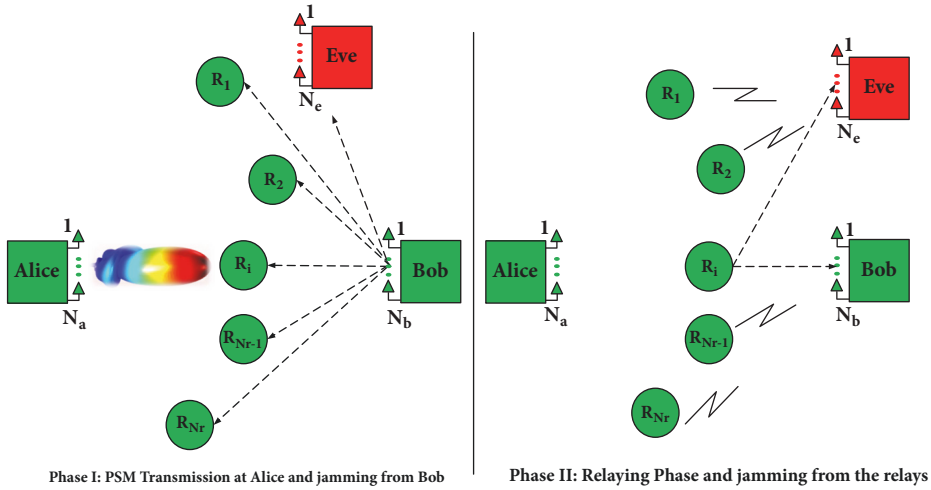

FIGURE 1: System model.

TABLE 1: Precoded SSK mapper rule example for $N_r = 4$; i.e., $k_1 = 2$.

k_1 bits	Relay activated	$\mathbf{e}_i$
$[0\ 0]$	1	$[1\ 0\ 0\ 0]^T$
$[0\ 1]$	2	$[0\ 1\ 0\ 0]^T$
$[1\ 0]$	3	$[0\ 0\ 1\ 0]^T$
$[1\ 1]$	4	$[0\ 0\ 0\ 1]^T$

In this work, we use a PSM-based relay-selection scheme in order to take advantage of the low probability of interception (LPI) of PSM. Following the principles of PSM [16, 17], we assume that $N_a > N_r$ and that $N_r = 2^{k_1}$, where k_1 is a positive integer to be able to use PSM. Hence, in PSM, relays' indices can be used by Alice to convey k_1 bits per symbol information following SSK principles. Therefore, the relay intended by reception is selected based on the k_1 incoming bits. In addition to SSK, we assume that Alice also exploits a conventional $M(= 2^{k_2})$-ary APM. Thus, each PSM symbol to be transmitted consists of $k = k_1 + k_2$ bits, which is first divided into two subsymbols, a k_1-bit SSK symbol and a k_2-bit APM symbol. The k_1-bit SSK symbol is mapped to a vector $\mathbf{e}_i$, which is the ith column of an identity matrix $\mathbf{I}_{N_r}$, and the subscript i is determined by the decimal value of the k_1-bit SSK symbol. The k_2-bit APM symbol is mapped to a unit-power symbol b_j chosen from the constellation according to the decimal value of the k_2-bit APM symbol. Then, the PSM symbol is formed as $\mathbf{s}_i^j = \mathbf{e}_i b_j$. After precoding, this signal is transmitted via the N_a transmit antennas of Alice. An example of relay selected based on the k_1 incoming bits is given in Table 1.

2.2. Channel Models. In this work, we consider Rayleigh block fading channels and we denote by h_{ij} the channel coefficient between nodes i and j. These coefficients have a complex Gaussian distribution with zero-mean and variance $d_{ij}^{-\alpha}$, i.e., $\mathcal{CN}(0, d_{ij}^{-\alpha})$, where d_{ij} is the distance between nodes i and j, and α is the path-loss exponent of wireless channels. Let $\mathbf{H}_{AR} = [\mathbf{h}_{AR_1}, \mathbf{h}_{AR_2}, \ldots, \mathbf{h}_{AR_{N_r}}]^T$ be the channel matrix between Alice and different relays, where $\mathbf{h}_{AR_i} \in \mathbb{C}^{1\times N_r}$ is the channel vector between Alice and the ith relay having $\mathcal{CN}(0, d_{AR_i}^{-\alpha})$ distributed components, where d_{AR_i} is the distance between Alice and the ith relay.

3. Performance Analysis

3.1. Received Signals. During the first phase, Alice transmits symbol $\mathbf{s}_i^j$ via its N_a antennas. Assuming that the channel state information to all relays is known to Alice, let $\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{Nr}]$ be a $N_a \times N_r$ precoding matrix used by Alice in order to send information to one of the relays. Then, the received signal from Alice at the relays is expressed as

$$\mathbf{y}_R = \mathbf{H}_{AR}\mathbf{P}\mathbf{s}_i^j + \boldsymbol{\eta}_R, \tag{1}$$

where $\boldsymbol{\eta}_R \in \mathbb{C}^{N_r\times 1}$ is the additive white Gaussian noise (AWGN) experienced by different relays, having complex Gaussian distributions of $\mathcal{CN}(0, \sigma_r^2)$. All channels are assumed to experience a block Rayleigh fading. While Alice knows the CSI of Alice-Relays channels, it is unable to acquire the CSI of Eve because this latter is assumed to be a passive eavesdropper.

Using the zero forcing precoder, the precoding matrix used by Alice can be expressed similar to [16] as

$$\mathbf{P} = \beta\mathbf{H}_{AR}^H\left(\mathbf{H}_{AR}\mathbf{H}_{AR}^H\right)^{-1}, \tag{2}$$

where

$$\beta = \sqrt{\frac{\left(\left(1-\delta_1\right)P/2\right)}{tr\left[\left(\mathbf{H}_{AR}\mathbf{H}_{AR}^H\right)^{-1}\right]}} \tag{3}$$

is a power normalization factor to achieve the power constraint of $tr(\mathbf{P}\mathbf{P}^H) = (1-\delta_1)P/2$, P denotes the total

transmitted power during the two phases, and δ_1 is a power allocation factor, $\delta_1 \in (0, 1]$. In the proposed scheme, the total power P is divided equally between the two transmission phases. Thus, $P/2$ is used in the first phase while being divided between the useful signal from Alice and the jamming signal from Bob. This division happens through the use of the power allocation factor δ_1; i.e., $(1-\delta_1)P/2$ is used by Alice and $\delta_1 P/2$ is used by Bob. During the second phase, the remaining $P/2$ is shared among all relays using the power allocation factor $\delta_2 \in (0, 1]$ as follows: (i) $P_s = \delta_2 P/2$ is used by the selected relay to transmit the useful signal and (ii) $P_J = (1-\delta_2)P/(2(N_r-1))$ is used by each of the remaining $N_r - 1$ relays to send the jamming signal received from Bob.

Thanks to the use of ZFP, the signal is only received by the ith relay and this can be seen by substituting (2) in (1). Thus, the received signal from Alice at different relays is given by

$$\begin{aligned} y_{Ri} &= \beta b_j + \eta_{Ri}, \\ y_{Rk} &= \eta_{Rk}, \quad \forall k \neq i. \end{aligned} \tag{4}$$

In this first phase, Bob also cooperates by broadcasting a jamming signal J_B. Thus, the received signals from Alice and Bob during this phase at all relays is given by

$$\begin{aligned} y_{Ri} &= \beta b_j + \sqrt{\frac{\delta_1 P}{2}}\mathbf{h}_{BR_i} J_B + \eta_{Ri}, \\ y_{Rk} &= \sqrt{\frac{\delta_1 P}{2}}\mathbf{h}_{BR_k} J_B + \eta_{Rk}, \quad \forall k \neq i, \end{aligned} \tag{5}$$

where $\mathbf{h}_{BR_k} \in \mathbb{C}^{N_b \times 1}$ is the channel vector between Bob and the kth relay R_k. To simplify the detection of Alice's signal at the relays, the jamming signal is assumed to have a complex Gaussian distribution with zero-mean and variance σ_J^2; i.e., $J_B \sim \mathcal{CN}(0, \sigma_J^2)$. Thus, the received signal at different relays can be reformulated as

$$\begin{aligned} y_{R_i} &= \beta b_j + \widetilde{\eta}_{Ri}, \\ y_{Rk} &= \widetilde{\eta}_{Rk}, \quad \forall k \neq i, \end{aligned} \tag{6}$$

where $\widetilde{\eta}_{Rk}$ has a complex Gaussian distribution with zero-mean and variance $\widetilde{\sigma}^2 = \delta_1 P/2 \|\mathbf{h}_{BR_k}\|_{\mathrm{F}}^2 \sigma_J^2 + {\sigma_r}^2$.

Similar to [24], we assume that the relays communicate via a backhaul-link (this link can be established through control channels and does not necessary imply that the used channels are dedicated). Thus, taking into consideration the received CSI at the relays from Bob, we can employ the following centralized low-complexity Maximum Likelihood (ML) detector:

$$\begin{aligned} \left[\widehat{i}, \widehat{j}\right] &= \arg\min_{i,j} \left\| \mathbf{y}_R - \beta \mathbf{s}_i^j \right\| \\ &= \arg\min_{i,j} \beta \left| b_j \right|^2 - 2\Re\left\{ y_{R_i}^* b_j \right\}. \end{aligned} \tag{7}$$

The use of the ML detector in (7) ensures that a single relay is activated during the second transmission phase. In this context, the relay intended by the PSM selection is used at the second phase to transmit the decoded APM signal b_j using power P_s and the remaining $N_r - 1$ relays send the perfectly estimated jamming signal received from Bob during the first phase each using a power $P_J = (P/2 - P_s)/(N_r - 1)$. When the relayed signals are received by Bob, this latter can employ self-interference subtraction as it knows the jamming signal J_B and it has received channel estimations with all relays. Thus, the received signal at Bob is given by

$$\mathbf{y}_B = \sqrt{P_s} b_j \mathbf{h}_{R_i B} + \boldsymbol{\eta}_B, \tag{8}$$

where η_B is the $\mathcal{CN}(0, \sigma_b^2)$ AWGN at Bob and $\mathbf{h}_{R_i B}$ is the channel coefficient between the ith relay R_i and Bob.

During the first phase, the received signal from Alice and Bob at Eve is expressed as

$$\mathbf{y}_{E,1} = \mathbf{H}_{AE} \mathbf{P} \mathbf{s}_i^j + \sqrt{\frac{\delta_1 P}{2}} \mathbf{H}_{BE} J_B + \boldsymbol{\eta}_{E,1}, \tag{9}$$

where $\boldsymbol{\eta}_{E,1} \in \mathbb{C}^{N_e \times 1}$ is the AWGN experienced by Eve during the first phase, having complex Gaussian distribution of $\mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$. $\mathbf{H}_{AE} \in \mathbb{C}^{N_e \times N_a}$ is the channel matrix between Alice and Eve having $\mathcal{CN}(0, d_{AE}^{-\alpha})$ distributed components. $\mathbf{H}_{BE} \in \mathbb{C}^{N_e \times N_b}$ is the channel matrix between Bob and Eve having $\mathcal{CN}(0, d_{BE}^{-\alpha})$ distributed components.

The received signal at Eve for the second phase is given by

$$\mathbf{y}_{E,2} = \sqrt{P_s} b_j \mathbf{h}_{R_i E} + \sqrt{P_J} \sum_{k \neq i} \mathbf{h}_{R_k E} J_B + \boldsymbol{\eta}_{E,2}, \tag{10}$$

where $\boldsymbol{\eta}_{E,2} \in \mathbb{C}^{N_e \times 1}$ is the $\mathcal{CN}(0, \sigma_e^2)$ AWGN experienced by Eve during the second phase.

3.2. Ergodic Secrecy Capacity. Using the received signal expression in (8), the signal-to-noise ratio (SNR) at Bob can be expressed as

$$\Gamma_B = \frac{P_s}{\sigma_b^2} \left\| \mathbf{h}_{R_i B} \right\|_{\mathrm{F}}^2. \tag{11}$$

The SNRs at Eve for both the first and second phases are derived using (9) and (10), respectively, as follows:

$$\gamma_{E,1} = \frac{\left\| \mathbf{H}_{AE} \mathbf{P} \right\|_{\mathrm{F}}^2}{\delta_1 (P/2) \left\| \mathbf{H}_{BE} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2} \tag{12}$$

and

$$\gamma_{E,2} = \frac{P_s \left\| \mathbf{h}_{R_i E} \right\|_{\mathrm{F}}^2}{P_J \sum_{k \neq i} \left\| \mathbf{h}_{R_k E} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2}. \tag{13}$$

Similar to [22], the ergodic secrecy capacity for the considered dual-hop scheme can be given as

$$C_s = \mathbb{E}\left\{ \left[\frac{1}{2} \log_2 \left(\frac{1 + \Gamma_B}{1 + \Gamma_E} \right) \right]^+ \right\}, \tag{14}$$

where $\Gamma_E = \max(\gamma_{E,1}, \gamma_{E,2})$ in order to account for the worst-case scenario.

In this paper, we take advantage of the low probability of interception of PSM to guarantee the secrecy of the transmission during the first phase and thus assume that $\Gamma_E = \gamma_{E,2}$. Indeed, as discussed in [11], if the Alice-Relays channels vary fast enough, the transmission from Alice to each relay is more or less a "one-time pad" cryptographic scheme, which is rendered absolutely secure. In this scenario, Eve cannot detect any information sent from Alice to Bob due to the one-time pad effect. When the Alice-Bob channels vary sufficiently slow, Eve is still incapable of detecting the SSK symbol i, as Eve is unable to estimate the precoding matrix $\mathbf{P}$ separately. Consequently, Eve needs to have both its CSI of $\mathbf{H}_{A,E}$ and the perfect knowledge of $\mathbf{P}$ to successfully eavesdrop $\mathbf{s}_i^j$. Thus, we assume that Eve is not able to get any useful information during the first phase. In order to confirm this assumption, we show in Figure 2 that $\gamma_{E,2}$ exceeds $\gamma_{E,1}$ almost surely for different simulation scenarios and parameters.

Due to intractability of (14), we can derive a lower bound on the ESC as follows:

$$\begin{aligned} C_s \geq C_{s_{lb}} &= \left[\mathbb{E}\left\{\frac{1}{2}\log_2\left(\frac{1+\Gamma_B}{1+\Gamma_E}\right)\right\}\right]^+ \\ &= \frac{1}{2\ln 2}\left[\mathbb{E}\left\{\ln\left(1+\Gamma_B\right)\right\} - \mathbb{E}\left\{\ln\left(1+\Gamma_E\right)\right\}\right]^+. \end{aligned} \tag{15}$$

Assuming that all noise variances are equal to σ^2, we define the average SNRs $\rho = P/(2\sigma^2)$ and $\rho_s = P_s/\sigma^2$. Thus, the received SNR at Bob can be written as

$$\Gamma_B = \rho_s \sum_{k=1}^{N_b} \left|h_{R_i B_k}\right|^2, \tag{16}$$

and the cumulative distribution function (CDF) of Γ_B is given by

$$F_{\Gamma_B}(\gamma_b) = 1 - \sum_{k=0}^{N_b-1} \frac{1}{k!}\left(\frac{\gamma_b}{\overline{\gamma}_b \rho_s}\right)^k e^{-\gamma_b/\rho_s\overline{\gamma}_b}, \tag{17}$$

where $\overline{\gamma}_b = d_{R_i B}^{-\alpha}$.

Using the CDF approach, the first part of the ergodic secrecy capacity lower bound is given in closed-form by

$$\begin{aligned} \mathbb{E}\left\{\ln\left(1+\Gamma_B\right)\right\} &= \int_0^\infty \frac{1-F_{\Gamma_B}(\gamma_b)}{1+\gamma_b} d\gamma_b \\ &= \sum_{k=0}^{N_b-1} \frac{1}{k!\overline{\gamma}_b{}^k \rho_s{}^k} \int_0^\infty \frac{\gamma_b^k}{1+\gamma_b} e^{-\gamma_b/\rho_s\overline{\gamma}_b} d\gamma_b \\ &= \sum_{k=0}^{N_b-1} \frac{1}{\overline{\gamma}_b{}^k \rho_s{}^k} \Psi\left(k+1, k+1; \frac{1}{\rho_s\overline{\gamma}_b}\right), \end{aligned} \tag{18}$$

where $\Psi(\cdot,\cdot;\cdot)$ is the Confluent Hypergeometric function of the second kind [25, equation (9.211.4)]. Similarly, using (13), the CDF of Eve's SNR is given by

$$F_{\gamma_{E,2}}(\gamma_e) = \int_0^\infty F_X\left(\frac{1}{\rho_s}\left(P_J y + 1\right)\gamma_e\right) f_Y(y)\, dy, \tag{19}$$

where $F_X(\cdot)$ is the CDF of the random variable $X = \|\mathbf{h}_{R_i E}\|_{\mathrm{F}}^2$ and $f_Y(\cdot)$ is the probability density function (PDF) of the RV $Y = \sum_{k\neq i} \|\mathbf{h}_{R_k E}\|_{\mathrm{F}}^2$ representing in this case the summation of $N = N_e(N_r - 1)$ exponential random variables.

Using the CDF approach, similar to (18), the second part of the ergodic secrecy capacity lower bound can be obtained:

$$\begin{aligned} \mathbb{E}\left\{\ln\left(1+\Gamma_E\right)\right\} &= \int_0^\infty \frac{1-F_{\Gamma_E}(\gamma_e)}{1+\gamma_e} d\gamma_e \\ &= \sum_{k=0}^{N_e-1} \sum_{j=0}^{k} \frac{(N+j-1)! P_J^j \rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\quad \times \int_0^\infty \frac{\gamma_e^k}{\left(\gamma_e+1\right)\left(P_J\gamma_e+\rho_s\right)^{N+j}} e^{-\gamma_e/\overline{\gamma}_e\rho_s} d\gamma_e, \end{aligned} \tag{20}$$

where $\overline{\gamma}_e = d_{R_i,E}^{-\alpha}$.

3.3. Secrecy Outage Probability. The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than a predetermined secrecy rate $\mathscr{R}_s$ [5] and it is given by

$$\begin{aligned} P_{\text{out}}(\mathscr{R}_s) &= \Pr\left[C_s \leq \mathscr{R}_s\right] \\ &= \Pr\left[\Gamma_B \leq 2^{\mathscr{R}_s}\left(1+\Gamma_E\right) - 1\right] \\ &= \int_0^\infty F_{\Gamma_B}\left(2^{\mathscr{R}_s}\left(1+\gamma_e\right) - 1\right) f_{\Gamma_E}(\gamma_e)\, d\gamma_e \\ &= 1 - \sum_{l=0}^{N_b-1} \frac{P_J^N}{l!\overline{\gamma}_b{}^l \rho_s{}^l} \sum_{k=0}^{N_e-1} \sum_{j=0}^{k} \frac{(N+j-1)!\rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\quad \times \sum_{m=0}^{l} \sum_{n=0}^{m} \binom{l}{m}\binom{m}{n} (-1)^{l-m} 2^{m\mathscr{R}_s} e^{-2^{\mathscr{R}_s}-1/\rho_s\overline{\gamma}_e} \\ &\quad \times \int_0^\infty \left(\frac{1}{\rho_s\overline{\gamma}_e}\gamma_e^2 + \left(N+j-k+\frac{1}{P_J\overline{\gamma}_e}\right)\gamma_e - k\frac{\rho_s}{P_J}\right) \\ &\quad \times \frac{\gamma_e^{n+k-1}}{\left(\gamma_e+\rho_s/P_J\right)^{N+j+1}} e^{-(2^{\mathscr{R}_s}+1)\gamma_e/\rho_s\overline{\gamma}_e} d\gamma_e. \end{aligned} \tag{21}$$

Using change of variables and Binomial expansion, the outage probability can be obtained in closed-form in (22)

where $a = (2^{\mathscr{R}_s} + 1)/P_J\overline{\gamma}_e$, $b = \rho_s/P_J$, and $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function:

$$\begin{aligned} P_{\text{out}}(\mathscr{R}_s) = 1 &- \sum_{l=0}^{N_b-1} \frac{P_J^N}{l!\overline{\gamma}_b{}^l \rho_s{}^l} \\ &\cdot \sum_{k=0}^{N_e-1}\sum_{j=0}^{k} \frac{(N+j-1)!\rho_s{}^{N+j-k}}{j!\,(k-j)!\,(N-1)!\overline{\gamma}_e^{k-j}} \\ &\cdot \sum_{m=0}^{l}\sum_{n=0}^{m} \binom{l}{m}\binom{m}{n}(-1)^{l-m} 2^{m\mathscr{R}_s} e^{-2^{\mathscr{R}_s}-1/\rho_s\overline{\gamma}_e} \\ &\times \left\{ \frac{1}{\rho_s\overline{\gamma}_e} \sum_{p=0}^{n+k+1} \binom{n+k+1}{p} (-b)^{n+k+1-p} \left(\frac{b}{a}\right)^{p+1} \right. \\ &\cdot \Gamma(p-N-j,a) + \left(N+j-k+\frac{1}{P_J\overline{\gamma}_e}\right) \\ &\cdot \sum_{q=0}^{n+k} \binom{n+k}{q} \times (-b)^{n+k-q} \left(\frac{b}{a}\right)^{q+1} \Gamma(q-N-j,a) \\ &- kb \sum_{r=0}^{n+k-1} \binom{n+k-1}{r} (-b)^{n+k-1-r} \Gamma(r-N-j,a) \\ &\left. \cdot \left(\frac{b}{a}\right)^{r+1} \right\} e^{-a/b}. \end{aligned} \tag{22}$$

3.4. Average Bit Error Probability

3.4.1. ABEP of Bob. In this part, the theoretical ABEP of Bob is derived. Based on the analysis of [26, 27], the end-to-end ABEP is expressed as

$$P_{\text{Bob}}(\gamma_1,\gamma_2) = P_1(\gamma_1) + P_2(\gamma_2) - P_1(\gamma_1)P_2(\gamma_2). \tag{23}$$

Here, $P_1(\gamma_1)$ is the ABEP between Alice and the RN, during the first time slot, for a given transmit SJNR γ_1 and $P_2(\gamma_2)$ is the ABEP between the RN and Bob, during the second slot, for a given transmit SNR γ_2. Hence the evaluation of the ABEP of Bob requires the evaluation of $P_1(\gamma_1)$ and $P_2(\gamma_2)$.

During the first slot, assuming ZF precoding at Alice with

$$\mathbf{P} = \mathbf{H}_{\mathbf{AR}}^H \left(\mathbf{H}_{\mathbf{AR}}\mathbf{H}_{\mathbf{AR}}^H\right)^{-1}, \tag{24}$$

the received signal at the RN is given as

$$\mathbf{y}_{\text{R}} = \sqrt{P_A d_{\text{AR}}^{-\alpha}}\mathbf{D}\mathbf{x} + \widetilde{\mathbf{w}}. \tag{25}$$

Here, it holds that $\mathbf{H}_{\mathbf{AR}} = \sqrt{d_{\text{AR}}^{-\alpha}}\widetilde{\mathbf{H}}_{\text{AR}}$, with $\widetilde{\mathbf{H}}_{\text{AR}} \sim \mathscr{CN}(\mathbf{0},\mathbf{I})$. In (25), P_A denotes Alice's transmit power and $\widetilde{\mathbf{w}}$ is a vector denoting the composite effect of noise plus jamming from Bob. Also, $\mathbf{D}$ is the $N_r \times N_r$ diagonal normalization matrix defined as $\mathbf{D} = \sqrt{d_{\text{AR}}^{-a}}\mathbf{diag}(d_1,\ldots,d_{N_r})$, where

$$d_i = \sqrt{\frac{1}{\left[\left(\widetilde{\mathbf{H}}_{\text{AR}}\widetilde{\mathbf{H}}_{\text{AR}}^H\right)^{-1}\right]_{i,i}}}. \tag{26}$$

Here, we note that the ZF precoder defined in (24) is equivalent to the one defined in (2). We use the new definition only for analytical tractability and for the sake of the simplicity of the derived ABEP results. This also enriches the paper by giving two different ways of defining the ZF precoder used at Alice under the same assumptions.

Since jamming is treated as noise at the RN, the detector at the RN is given as

$$(\overline{\mathbf{x}}) = \arg\min_{\mathbf{x}} \left\|\mathbf{y}_{\text{R}} - \mathbf{D}\mathbf{x}\right\|_2^2. \tag{27}$$

In particular, (27) is the ML detector of PSM. Therefore, $P_1(\gamma_1)$ is the ABEP of PSM with the jamming effect. Hence, the ABEP during the first hop at the RN is given as

$$P_1(\gamma_1) \le \frac{1}{Mk_t}\sum_{\mathbf{x}}\sum_{\mathbf{x}\neq\widehat{\mathbf{x}}} d(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})\,P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}}), \tag{28}$$

where $d(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})$ is the Hamming distance between the bit sequences represented by $\mathbf{x}$ and $\widehat{\mathbf{x}}$. $k_t = (k_1+k_2)/2$ is equal to the total number of bits transmitted per symbol period. We note that $k_1 + k_2$ is divided by two because the transmitted bitstream requires two symbol periods to reach Bob. Also, $P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}})$ is the PEP of transmitting $\mathbf{x}$ at Alice and erroneously detecting $\widehat{\mathbf{x}}$ at the relay nodes.

Based on the analysis presented in [28, Section IV], the instantaneous PEP is given as

$$P_{\text{R-SM}}\left(\mathbf{x}\longrightarrow\widehat{\mathbf{x}},\gamma_1 \mid \mathbf{D}^2\right) = Q\left(\sqrt{\frac{\mathbf{c}^H\mathbf{D}^2\mathbf{c}}{2}P_A d_{\text{AR}}^{-a}\gamma_1}\right), \tag{29}$$

where $\mathbf{c} = \mathbf{x} - \widehat{\mathbf{x}}$. Considering the following upper bound of the Q-function [29]:

$$Q(x) \le \sum_{i=1}^{3}\beta_i e^{-\mu_i x^2}, \tag{30}$$

in (29) and averaging over all possible realizations of the Alice-RN channel, the average PEP of PSM is expressed as [28, Section IV]

$$\begin{aligned} P_{\text{R-SM}}(\mathbf{x}\longrightarrow\widehat{\mathbf{x}}) \le \sum_{i=1}^{3} &\frac{\beta_i\left[\prod_{l=1}^{N}(\alpha_1/\alpha_l)^L\right]}{2\left(\mu_i\alpha_1 P_A d_{\text{AR}}^{-a}\gamma+1\right)^L} \\ &\times \sum_{k=0}^{+\infty}\delta_k\left(\mu_i\alpha_1 P_A d_{\text{AR}}^{-a}\gamma+1\right)^{-k}. \end{aligned} \tag{31}$$

Here, it holds that $\beta_1 = 1/2$, $\beta_2 = 1/12$, $\beta_3 = 1/4$, $\mu_1 = 2$, $\mu_2 = 1$, and $\mu_3 = 1/2$. Furthermore, for a given pair of $\mathbf{x}_i$ and $\widehat{\mathbf{x}}_i$, N is the number of nonzero elements of $\mathbf{c}$. Also, α_l, $l = 1,\ldots,N$, stand for the eigenvalues of $\mathbf{A} = \mathbf{BR}$ in ascending order. Here, $\mathbf{B}$ is a diagonal matrix, defined as $\mathbf{B} = \mathbf{diag}(b_1,\ldots,b_N)$, where b_l, $l = 1,\ldots,N$, is the absolute

value of the lth nonzero element of $\mathbf{c}_i$. In addition, $\mathbf{R}$ is a $N \times N$ matrix given as shown in (33).

$$\delta_{k+1} = \begin{cases} 1, & k = -1, \\ \dfrac{k}{k+1} \displaystyle\sum_{i=1}^{k+1} \left[\sum_{j=1}^{N} \left(1 - \frac{\alpha_1}{\alpha_j} \right)^i \right] \delta_{k+1-i}, & k = 0, 1, 2, \ldots. \end{cases} \tag{32}$$

$$\mathbf{R} = \begin{bmatrix} 1 & \sqrt{\rho_c} & \cdots & \sqrt{\rho_c} \\ \sqrt{\rho_c} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \sqrt{\rho_c} \\ \sqrt{\rho_c} & \cdots & \sqrt{\rho_c} & 1 \end{bmatrix}. \tag{33}$$

In (33), ρ_c denotes the Pearson product-moment correlation coefficient between any pair of two different random variables (RVs) $d_1^2, \ldots, d_R^2$. Moreover, δ_k, $k = 0, 1, 2, \ldots$, are given in (32). Finally, it holds that $L = N_t - N_r + 1$.

During the second hop, the received signal at Bob is expressed as

$$\mathbf{y}_{\mathrm{B}} = \sqrt{P_R} \mathbf{H}_{\mathbf{RB}} \overline{\mathbf{x}} + \mathbf{w}_{\mathrm{B}}, \tag{34}$$

after the ideal removal of the jamming signal. In (34), it holds that $\mathbf{H}_{\mathbf{RB}} = \sqrt{d_{\mathrm{RB}}^{-a}} \widetilde{\mathbf{H}}_{\mathrm{RB}}$, with $\widetilde{\mathbf{H}}_{\mathrm{RB}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. Also, P_R is the transmission power at the RN. Note that the value of P_R is selected such that the transmitted signal at the RN is normalized. As the RN retransmits binary information by using SM, Bob can deploy the following ML detector [8]:

$$(\check{\mathbf{x}}) = \arg \min_{\mathbf{x}} \left\| \mathbf{y}_{\mathrm{B}} - \sqrt{P_B d_{\mathrm{RB}}^{-a}} \widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{x} \right\|_2^2. \tag{35}$$

Therefore, the ABEP of the second hop is given as

$$P_2(\gamma_2) \leq \frac{1}{M k_t} \sum_{\mathbf{x}} \sum_{\mathbf{x} \neq \widehat{\mathbf{x}}} d(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}), \quad P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}), \tag{36}$$

where $P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}})$ is the average PEP of transmitting $\mathbf{x}$ at the RN, while the detector of Bob decides in favor of $\widehat{\mathbf{x}}$. Considering the statistical characteristics of the noise at Bob, it can be shown that the instantaneous PEP is given as

$$P_{\mathrm{SM}}\left(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}, \gamma_2 \mid \widetilde{\mathbf{H}}_{\mathrm{RB}}\right) = Q\left(\sqrt{\frac{\left\| \widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{c} \right\|_2^2}{2} P_R d_{\mathrm{RB}}^{-a} \gamma_2} \right). \tag{37}$$

In (37), it is shown that the RV $X = \|\widetilde{\mathbf{H}}_{\mathrm{RB}} \mathbf{c}\|_2^2$ follows an Erlang distribution with the following PDF [30]:

$$f_X(x) = \frac{1}{\|\mathbf{c}\|_2^{2N_r} \Gamma(N_r)} x^{N_r} e^{x/\|\mathbf{c}\|_2^2} H_0(x), \tag{38}$$

where $H_0(x)$ is the Heaviside step function defined as $H_0(x) = 0$ for $x < 0$ and $H_0(x) = 1$ for $x \geq 0$. Considering (30) and (38) in (37), the average PEP of the second hop is given as

$$P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}) \leq \sum_{i=1}^{3} \frac{\beta_i}{\|\mathbf{c}\|_2^{2N_r} \Gamma(\mathrm{N}_r)} \times \int_0^{+\infty} x^{N_r - 1} e^{-(P_R d_{\mathrm{RB}}^{-a} \mu_i \gamma_2 + 1/\|\mathbf{c}\|_2^2) x} \mathrm{d}x, \tag{39}$$

by averaging over possible realizations of the RV X. From [25, p.346, 3.381, 4], it holds that

$$\int_0^{+\infty} x^{\nu - 1} e^{-\mu x} dx = \mu^{-\nu} \Gamma(\nu). \tag{40}$$

The use of (30) and (40) into (39), after a straightforward elaboration, results in

$$P_{\mathrm{SM}}(\mathbf{x} \longrightarrow \widehat{\mathbf{x}}) \leq \sum_{i=1}^{3} \beta_i \left(\|\mathbf{c}\|_2^2 \mu_i P_R d_{\mathrm{RB}}^{-a} \gamma_2 + 1 \right)^{-N_r}. \tag{41}$$

In this way, the ABEP of Bob is computed via (23) by using (28), (31), (36), and (41).

3.4.2. ABEP of Eve. In this part, the theoretical ABEP of Eve is derived. As previously shown in Figure 2, the Signal-to-Jamming-Plus-Noise Ratio at Eve during the second phase is much higher than the SJNR during the first phase for different simulation scenarios and parameters. Thus, the ABEP of Eve during the first phase is much worse than the ABEP during the second phase. Accounting for the worst-case scenario (i.e., taking the highest SNR at Eve and assuming perfect detection at the relays during the first phase), the SJNR at Eve when the ith relay is used during the second phase is given by

$$\gamma_E = \frac{P_s \left\| \mathbf{h}_{R_i E} \right\|_{\mathrm{F}}^2}{P_J \sum_{k \neq i} \left\| \mathbf{h}_{R_k E} \right\|_{\mathrm{F}}^2 \sigma_g^2 + \sigma_e^2}. \tag{42}$$

In light of the above, the asymptotic performance bound of the ABEP at Eve with optimal detection is derived using the union bound as

$$P_E \leq \sum_{q=1}^{M} \sum_{\widehat{q}=1}^{M} \frac{N_r N(q, \widehat{q})}{M} P\left(x_{jq} \longrightarrow x_{\widehat{jq}} \right), \tag{43}$$

where $N(q, \widehat{q})$ is the number of bits in error between the symbol x_q and $x_{\widehat{q}}$, and $P(x_{jq} \longrightarrow x_{\widehat{jq}})$ denotes the PEP of deciding on the constellation vector $x_{\widehat{jq}}$ given that x_{jq} is transmitted and can be formulated as

$$P\left(x_{jq} \longrightarrow x_{\widehat{jq}} \right) = \int_{v=0}^{\infty} Q\left(\sqrt{v} \right) f_\kappa(v) \, dv, \tag{44}$$

where $f_\kappa(\cdot)$ is the PDF and is a chi-squared random variable with $2N_e$ degrees of freedom given by [31, p. 41] as

$$f_\kappa(v) = \frac{v^{N_e - 1} \exp\left(-v / \left(2\alpha^2 \right) \right)}{\left(2\alpha^2 \right)^{N_e} (N_e - 1)!}, \tag{45}$$

where

$$\alpha^2 = \frac{\delta_2 \rho}{(1-\delta_2)\rho + 1}\left(\frac{\left|x_q\right|^2 + \left|x_{\widehat{q}}\right|^2}{4}\right). \quad (46)$$

Thus, the PEP in (44) is obtained in closed-form as

$$P\left(x_{jq} \longrightarrow x_{\widehat{jq}}\right) = \gamma^{N_e} \sum_{w=0}^{N_e-1} \binom{N_e + w - 1}{w} (1-\gamma)^w, \quad (47)$$

where

$$\gamma = \frac{1}{2}\left(1 - \sqrt{\frac{\alpha^2}{1+\alpha^2}}\right). \quad (48)$$

Finally, plugging in (47) in (43), the ABEP at Eve is obtained as

$$P_E \leq \sum_{q=1}^{M} \sum_{\widehat{q}=1}^{M} \frac{N_r N(q,\widehat{q})\, \gamma^{N_e} \sum_{w=0}^{N_e-1} \binom{N_e+w-1}{w} (1-\gamma)^w}{M}. \quad (49)$$

4. Numerical Results

In this section, we present selected numerical examples to confirm the ergodic secrecy capacity and the secrecy outage probability results derived in the previous section. We also present the bit error rate (BER) comparison for Bob and Eve by simulations. In these results, we assume that the secrecy during the first phase is guaranteed thanks to the use of PSM [10]. Indeed, the received SNR at Eve during the second phase exceeds that of the first phase with very high probability as discussed in Section 3.2 and shown in Figure 2.

As discussed earlier, the total power is allocated during the first and second phases using the power allocation factors δ_1 and δ_2, respectively. While both power allocation factors have effect on the performance of the proposed scheme, δ_2 has more weight and affects the BER performance more than δ_1. Indeed, the beamforming used at Alice during the first phase maximizes the received SNR at the intended relay which reduces the effect of the power allocation factor δ_1. In what follows, we study the effect of δ_2 and show that it has more weight and affects the performance more than δ_1. In this context, Figure 3 presents the effect of the power allocation coefficient δ_2 during the second phase on the secrecy outage probability. We can see from this figure that the value of the optimal power allocation coefficient δ_2^* depends on different parameters including the number of antennas at different nodes. For instance, while δ_2^* is equal to 0.3 for $N_b = 4$ and $N_e = 2$, it is equal to 0.45 for $N_b = 4$ and $N_e = 16$. The exact values for the optimal power allocation coefficient can be mathematically derived by optimizing the SOP expression in (22). It can also be obtained through the asymptotic outage secrecy performance and we look at addressing this as a future extension to this work in order to further enhance the performance of the proposed scheme. In the following results, we use the optimal power allocation coefficient values obtained by simulations when generating the SOP curves.

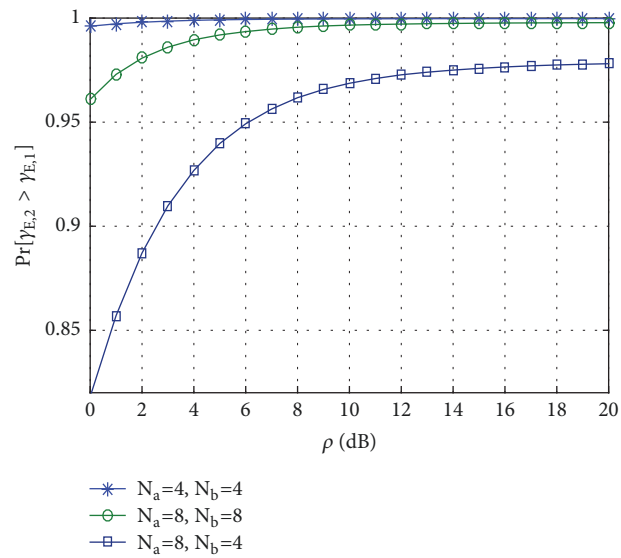

Figure 2: Probability that $\gamma_{E,2}$ exceeds $\gamma_{E,1}$ as a function of the average SNR with different N_a and N_b for $N_r = N_e = 4$ and $\delta_1 = \delta_2 = 0.5$.

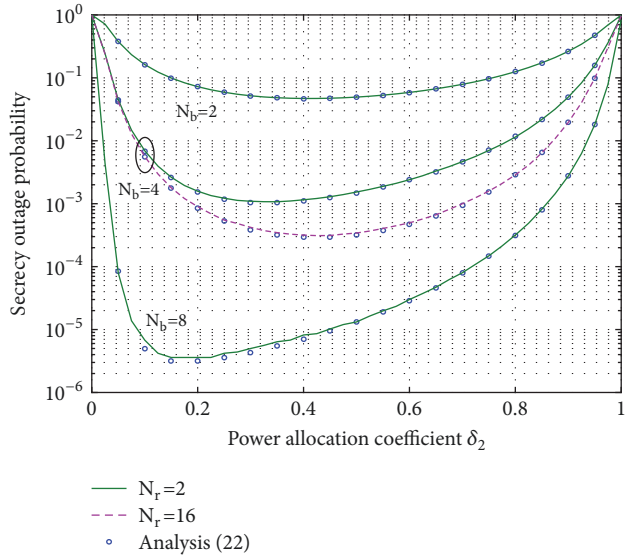

Figure 3: Effect of the power allocation at the second phase on the SOP with different N_b and N_r, for $N_e = 4$, $\rho = 20$ dB, $\mathscr{R}_s = 1$, and $\delta_1 = 0.5$.

In Figure 4, we present the secrecy outage probability as a function of the average received SNR with both simulation and analysis. This figure is given for a secrecy rate threshold $\mathscr{R}_s = 1$ bits/s/Hz, $N_r = 4$, $N_e = 4$, and for different number of antennas at Bob. The power allocation coefficient δ_2 is selected as discussed above and is equal to δ_2^* corresponding to each number of antennas at Bob. Figure 4 also compares the performance of the proposed scheme to the case where a single relay participates in transmitting the jamming signal at the second phase. We can clearly see the advantage of using

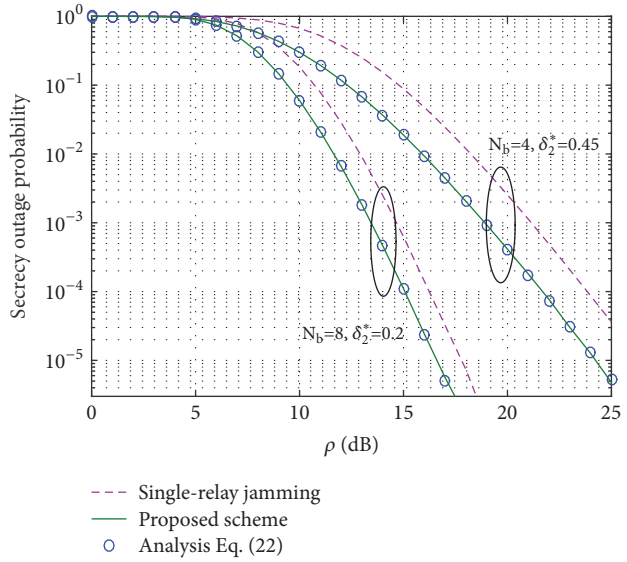

FIGURE 4: SOP comparison with the case where a single relay is used for jamming, for $\mathscr{R}_s = 1$ bits/s/Hz, $N_a = 4$, $N_r = 4$, $N_e = 4$, and $\delta_1 = 0.5$.

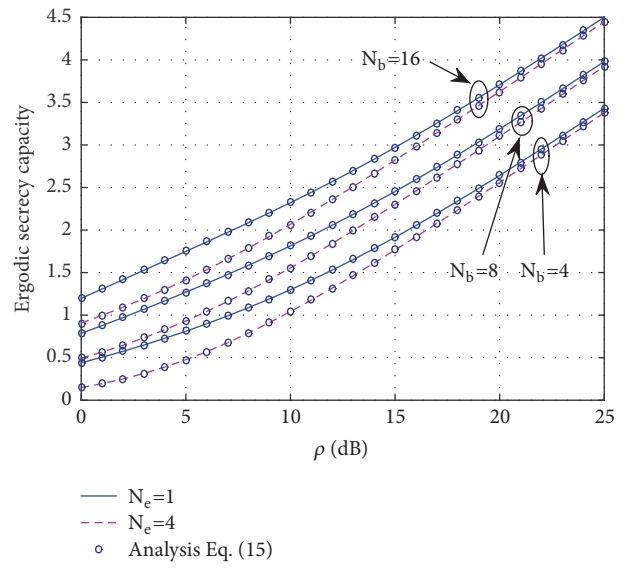

FIGURE 5: ESC with different number of antennas at Bob and Eve, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.75$.

multiple relays for jamming as it enhances the secrecy outage probability by further degrading the received SNR at Eve.

Figure 5 presents the ESC in bits/s/Hz as a function of the average SNR $\rho = P/(2\sigma^2)$ with different number of antennas at Bob and Eve, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.75$. These results show the accuracy of the analytical derivations presented in the previous section. We can also see from this figure the effect of different parameters on the ESC. In this context, we can confirm the improvement of the secrecy rate through increasing the number of antennas at Bob and its degradation by increasing the number of antennas at Eve. We can also see that, for high average SNRs, the number of

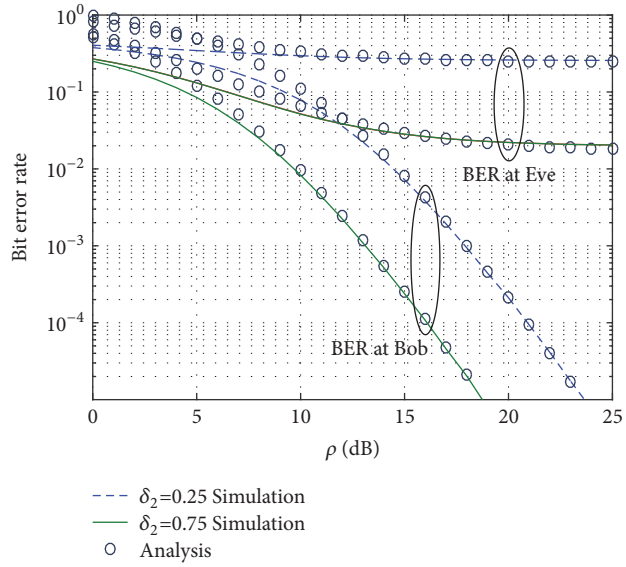

FIGURE 6: BER comparison at Bob and Eve for different power allocations during the second phase, for $N_a = 4$, $N_r = 4$, $N_b = 4$, $N_e = 4$, and $\delta_1 = 0.5$.

antennas at Eve has less effect of the ESC performance and the curves for $N_e = 1$ and $N_e = 4$ converge.

Figure 6 depicts the BER at Bob and Eve as a function of ρ for different power allocation coefficients δ_2. This figure confirms the tightness of the ABEP bounds derived in the previous section. The main goal of the proposed scheme is to make sure that Eve is not able to detect the information exchanged between Alice and Bob. To this end, we use precoding-aided spatial modulation and cooperative jamming. Thanks to these techniques, the SNR at Eve becomes very low and, thus, the error performance degrades. The simulation results shown in Figure 6 confirm the improvement of the BER at Bob compared to the BER at Eve thanks to the use of the multirelay jamming. From this figure, we can also see that the BER at both Bob and Eve improves when more power is allocated for the relay selected by PSM (i.e., the relay transmitting the message). On the other hand, the BER at both receivers degrades when more power is allocated to the jamming relays.

In Figure 7, we study the effect of the number of receive antennas on the BER at Bob and Eve as a function of ρ for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.7$. These simulation results show the improvement of the BER at Bob and Eve for higher number of receive antennas at each of these nodes. From this figure, we can also confirm that the use of multirelay jamming comes with improved BER at Bob compared to the BER at Eve. Indeed, Eve experiences much worse detection performance thanks to the use of PSM and jamming from Bob in the first phase and the use of jamming from $N_r - 1$ relays in the second phase.

In the above results, we note that we used a fixed number of relays, equal to four, only to simplify the simulations. However, we need to highlight that the performance of the proposed scheme depends on the number of available relays.

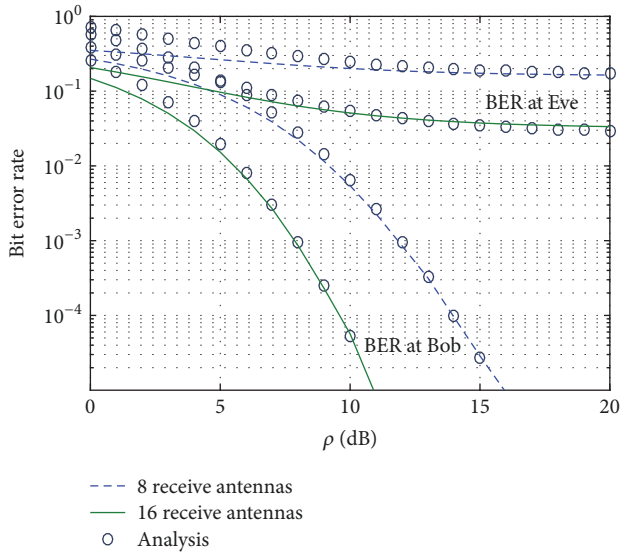

FIGURE 7: BER comparison at Bob and Eve for different number of receive antennas, for $N_a = 4$, $N_r = 4$, $\delta_1 = 0.5$, and $\delta_2 = 0.7$.

Indeed, in the proposed work, while increasing the number of relays enhances the spectral efficiency as a property of precoding-aided spatial modulation, it causes a degradation in the BER performance [32]. Indeed, the increase in N_r is equivalent to increasing the constellation size of the index modulation used during the second phase while keeping the same transmit power. This case will generate more errors at the ML detector as the distance between different constellation points shrinks with a higher N_r and a constant transmit power, divided between all relays using the power allocation factor δ_2.

5. Conclusion

In this paper, we have studied the physical-layer security of a wiretap channel using a PSM-based relay-selection scheme with multiple relays' jamming. The performance of the proposed system is evaluated in terms of the ergodic secrecy capacity, secrecy outage probability, and bit error rate performances. Numerical results, confirmed by analysis, show an enhanced secrecy performance when compared to selected schemes. Using simulations, we use power allocation optimization in order to divide the power between the relay transmitting the useful information and the jamming relays, and thus we further improve the secrecy performance of the proposed scheme. In this paper, we have also provided closed-form expressions for the ESC and SOP and we derive very tight upper-bounds for the BER. These results confirm the ESC, SOP, and BER performance improvements at Bob and its degradation at Eve, which confirms the high secrecy performance of the proposed scheme.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

The statements made herein are solely the responsibility of the authors. This work was presented in part at the 2017 IEEE WCNC Conference, San Francisco, CA, USA [33].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Qatar National Research Fund (a member of Qatar Foundation) under National Priorities Research Program (NPRP) Grant NPRP 8-052-2-029.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 29, no. 4, pp. 656–715, 1949.

[2] R. Liu and W. Trappe, *Securing Communications at the Physical Layer*, Springer-Verlag, New York, NY, USA, 2010.

[3] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications Magazine*, vol. 19, no. 1, pp. 40–47, 2012.

[4] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[6] 5GPPP, *5G Vision*, 2015. [Online]. Available: http://5g-ppp.eu/wpcontent/uploads/2015/02/5G-Vision-Brochure-v1.pdf.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[8] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Spatial modulation: Optimal detection and performance analysis," *IEEE Communications Letters*, vol. 12, no. 8, pp. 545–547, 2008.

[9] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: challenges, opportunities, and implementation," *Proceedings of the IEEE*, vol. 102, no. 1, pp. 56–103, 2014.

[10] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2016.

[11] F. Wu, C. Dong, L. Yang, and W. Wang, "Secure Wireless Transmission Based on Precoding-Aided Spatial Modulation," in *Proceedings of the GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, pp. 1–6, San Diego, CA, USA, December 2015.

[12] F. Wu, L.-L. Yang, W. Wang, and Z. Kong, "Secret Precoding-Aided Spatial Modulation," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1544–1547, 2015.

[13] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure Multiuser MIMO Downlink Transmission Via Precoding-Aided Spatial Modulation," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1116–1119, 2016.

[14] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3692–3703, 2009.

[15] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proceedings of the IEEE PIMRC*, pp. 1–5, Cannes, France, 2008.

[16] L. Yang, "Transmitter Preprocessing Aided Spatial Modulation for Multiple-Input Multiple-Output Systems," in *Proceedings of the 2011 IEEE Vehicular Technology Conference (VTC 2011-Spring)*, pp. 1–5, Budapest, Hungary, May 2011.

[17] R. Zhang, L.-L. Yang, and L. Hanzo, "Generalised pre-coding aided spatial modulation," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5434–5443, 2013.

[18] C.-X. Wang, F. Haider, X. Gao et al., "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 122–130, 2014.

[19] D. A. Basnayaka, M. Di Renzo, and H. Haas, "Massive but few active MIMO," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6861–6877, 2016.

[20] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1756–1770, 2015.

[21] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[22] A. Mabrouk, K. Tourki, and N. Hamdi, "Relay selection for optimized cooperative jamming scheme," in *Proceedings of the 23rd European Signal Processing Conference, EUSIPCO 2015*, pp. 86–90, Nice, France, September 2015.

[23] Y. Huo, X. Dong, and W. Xu, "5G cellular user equipment: From theory to practical hardware design," *IEEE Access*, vol. 5, pp. 13992–14010, 2017.

[24] A. Stavridis, D. Basnayaka, S. Sinanovic, M. Di Renzo, and H. Haas, "A virtual MIMO dual-hop architecture based on hybrid spatial modulation," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3161–3179, 2014.

[25] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.

[26] M. O. Hasna and M.-S. Alouini, "End-to-end performance of transmission systems with relays over Rayleigh-fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 6, pp. 1126–1131, 2003.

[27] N. Serafimovski, S. Sinanovic, M. Di Renzo, and H. Haas, "Dual-Hop Spatial Modulation (Dh-SM)," in *Proceedings of the 2011 IEEE Vehicular Technology Conference (VTC 2011-Spring)*, pp. 1–5, Budapest, Hungary, May 2011.

[28] A. Stavridis, M. Di Renzo, and H. Haas, "Performance Analysis of Multistream Receive Spatial Modulation in the MIMO Broadcast Channel," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1808–1820, 2016.

[29] M. Chiani, D. Dardari, and M. K. Simon, "New exponential bounds and approximations for the computation of error probability in fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 840–845, 2003.

[30] E. Bjornson, D. Hammarwall, and B. Ottersten, "Exploiting quantized channel norm feedback through conditional statistics in arbitrarily correlated MIMO systems," *IEEE Transactions on Signal Processing*, vol. 57, no. 10, pp. 4027–4041, 2009.

[31] J. Proakis, *Digital Communications*, McGraw-Hill, 4th edition, 2001.

[32] Z. Bouida, A. Ghrayeb, and K. A. Qaraqe, "Adaptive spatial modulation for spectrally-efficient MIMO spectrum sharing systems," in *Proceedings of the 2014 25th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communication, IEEE PIMRC 2014*, pp. 354–358, Washington, DC, USA, September 2014.

[33] Z. Bouida, A. Stavridis, A. Ghrayeb, H. Haas, and M. Hasna, "Precoded spatial modulation for the wiretap channel with relay selection and cooperative jamming," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, WCNC 2017*, pp. 1–6, San Francisco, CA, USA, March 2017.