Secure Multiantenna Transmission With an Unknown Eavesdropper: Power Allocation and Secrecy Outage Analysis

Shaobo Jia, *Member, IEEE*, Jiankang Zhang, *Senior Member, IEEE*, Sheng Chen, *Fellow, IEEE*, Wanming Hao, *Member, IEEE*, and Wei Xu, *Senior Member, IEEE*

***Abstract*— This paper investigates the power allocation problem for secure multiple-input single-output transmission with the injection of artificial noise (AN), in the presence of an unknown eavesdropper (Eve). Two power allocation schemes, the optimal adaptive power allocation (OAPA) and suboptimal fixed power allocation (SFPA) schemes, are proposed to enhance the physical layer security of the considered system. Since the noise power at Eve is unknown, both power allocation schemes are designed for the worst-case scenario in which the noise power at Eve is assumed to be zero, aiming to minimize the secrecy outage probability (SOP). To characterize the performance of the proposed power allocation schemes, approximate closed-form expressions for average SOP under a preset noise power level are derived by applying Gauss-Chebyshev quadrature. We also address the worst-case secrecy outage performance for the proposed OAPA and SFPA schemes. Our analytical and numerical results show that, compared with the exhaustive search method that requires Eve's prior information, the proposed OAPA scheme exhibits comparable secrecy outage performance without Eve's prior information. Additionally, the SFPA scheme, also without Eve's prior information, is capable of achieving almost the same worst-case SOP as the OAPA scheme, with a much lower implementation complexity.**

***Index Terms*— Physical layer security, power allocation, artificial noise, secrecy outage probability.**

I. Introduction

SECURITY issues are of vital importance in wireless transmissions since a large amount of confidential information is transferred over the open medium. Traditionally, cryptographic technologies implemented at upper layer are employed for achieving communication confidentiality against eavesdropping attacks, based on the assumption that eavesdroppers have limited computational resources. However, with the rapid development of computation techniques, these cryptographic methods are not information-theoretically secure. As a complementary approach, physical layer security (PLS) has been envisioned as a promising technique by smartly exploiting the intrinsic randomness of the communications media. In the pioneering work of Wyner on PLS [1], it was proved that perfect secrecy could be ensured provided that the wiretap channel is the degraded version of the main channel, and the secrecy capacity was characterized. The secrecy capacity of the scalar Gaussian wiretap channel was analyzed in [2]. This result was generalized to the wireless fading channel in [3] and [4].

Owing to spatial degrees of freedom and diversity gains, multiantenna techniques have been considered as an efficient solution for combating channel fading and increasing channel capacity, and also have great potential to improve wireless PLS [5]–[13]. In [5], the secure secondary transmission was investigated in multiantenna cognitive radio networks, and new closed-form expressions for the exact and asymptotic secrecy outage probability (SOP) were derived. In [6], the effect of phase noise on the downlink SWIPT in secure massive multiple-input-multiple-output (MIMO) systems was investigated. In [7], the authors exploited the potential benefits of machine learning in selecting the optimal transmit antenna that maximizes the secrecy performance of a MIMO-multiple-eavesdropper (MIMOME) wiretap system. In [8], the secret-key agreement over MIMO quasi-static fading channels was studied. Additionally, the PLS of multiantenna transmission aided by intelligent reflecting surface (IRS) was addressed in [9]–[11]. Secrecy outage performance analyses were carried out for MIMO relaying systems in [12] and [13].

To ensure the existence of a nonzero secrecy rate when the channel quality of the wiretap link is superior to that of the legitimate link, Goel and Negi [14] proposed to employ artificial noise (AN) to improve PLS. Inspired by the work [14], a numerous body of works have studied AN assisted schemes for PLS [15]–[22]. In [15], a robust information and AN precoding scheme was designed for a multiple-input-single-output (MISO) cognitive system with unknown eavesdroppers. PLS for full-duplex multiantenna systems was studied in [16]–[19],

Manuscript received 25 July 2021; revised 16 January 2022, 4 April 2022, and 25 June 2022; accepted 30 July 2022. Date of publication 5 August 2022; date of current version 17 August 2022. This work was supported by the Henan Provincial Key Science and Technology Research Projects under Grant 222102210097. An earlier version of this paper was presented at the GLOBECOM 2020 [DOI: 10.1109/GLOBECOM42002.2020.9348097]. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Matthieu R. Bloch. *(Corresponding author: Jiankang Zhang.)*

Shaobo Jia and Wanming Hao are with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China (e-mail: ieshaobojia@zzu.edu.cn; iewmhao@zzu.edu.cn).

Jiankang Zhang is with the Department of Computing and Informatics, Bournemouth University, Bournemouth BH12 5BB, U.K. (e-mail: jzhang3@bournemouth.ac.uk).

Sheng Chen is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: sqc@ecs.soton.ac.uk).

Wei Xu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: wxu@seu.edu.cn).

Digital Object Identifier 10.1109/TIFS.2022.3197062

wherein the legitimate transceiver simultaneously emits AN to interfere with the eavesdropper while transmitting confidential information. In [20], two PLS techniques were proposed for millimeter-wave (mmWave) vehicular communication systems, and both techniques utilize large antenna arrays to confuse potential eavesdroppers with sensitive receivers. In [21], PLS in multiantenna relay wiretap networks was investigated, where all eavesdroppers in the network are randomly distributed following three independent Poisson point processes. In [22], a joint beamforming and jamming secure transmission scheme was investigated for an IRS assisted MISO wiretap system without the eavesdropper's CSI. In [23], He and Yener even proved that secure communication is possible regardless of the location or channel states of the eavesdropper.

In AN-assisted schemes, characterizing the power allocation between the AN and the information signals is one of the major challenges. In the existing literature, two different power allocation schemes, namely, adaptive power allocation and non-adaptive (or fixed) power allocation, have been proposed (e.g., [24]–[29]). In the non-adaptive power allocation scheme, the power allocation factor (PAF) is fixed for all the instantaneous channel realizations. However, in this scheme, it is usually difficult to obtain further insights due to the complicated closed-form expression of SOP, which results in that the optimal PAFs can only be achieved via an exhaustive search method. Zhou and McKay [24] analyzed the secrecy performance and designed the power allocation scheme over fast fading channels. In [25], AN-assisted optimal cognitive beamforming schemes were proposed, in which the power allocation is optimized to maximize the achievable ergodic secrecy rate. For adaptive power allocation, the PAF is adaptively chosen based on the instantaneous CSI of the legitimate channel. In [26]–[29], the power allocation was optimized by minimizing the SOP under a given realization of the channel between the legitimate transceiver in a MISO wiretap channel. In the aforementioned works, the eavesdroppers' channel state distribution information (CSDI) is required for optimizing the power allocation. However, since eavesdroppers may remain silent in practice, it is challenging to obtain statistical information in real wiretap scenarios.

Motivated by these observations, this paper investigates the secure transmission in a multiantenna wiretap system with an unknown eavesdropper. We optimize the power allocation without any prior information of the eavesdropper, and further conduct the secrecy outage performance analysis on this basis. Part of our work was presented at the Globecom 2020 conference [30]. However, the work [30] only investigated the scenario where the noise power σ_e^2 at the eavesdropper is assumed to be zero. To address a more practical case, in this paper, we conduct the secrecy outage performance analysis of the proposed power allocation schemes under a preset noise power level σ_e^2 at the eavesdropper, and we also carefully examine the influence of σ_e^2 on the secrecy performance using simulation results. Moreover, the instantaneous secrecy outage performance is also addressed in this paper. The main contributions of our paper are summarized as follows.

- We propose an optimal adaptive power allocation (OAPA) to minimize the SOP of the proposed system coexisting with an unknown eavesdropper. In the OAPA, the optimal PAF is adaptively adjusted to the instantaneous CSI of the main channel, and it is updated in real-time. We also propose a suboptimal fixed power allocation (SFPA) to reduce the implementation complexity. In the SFPA, the optimal PAF is designed off-line based on the CSDI of the main channel, and it remains fixed during transmissions. We provide the closed-form solutions to the optimal PAFs for both schemes, which are independent of the eavesdropper's prior information.
- For the proposed OAPA and SFPA schemes, we derive the approximate closed-form expressions of the average SOP with a preset noise power level at the eavesdropper by leveraging the Gauss-Chebyshev quadrature. In order to address the special case in which the average receive signal-to-noise ratio (SNR) at the eavesdropper is relatively high, we also analyze the secrecy outage performance in the worst-case scenario where the noise power at the eavesdropper is zero.
- We provide new insights into secure transmission designs. Without the eavesdropper's prior information, we reveal that for the OAPA, more power should be allocated to the AN to achieve a lower SOP for a larger maximal achievable instantaneous SNR at the legitimate receiver. For the SFPA, the optimal PAF is determined by the maximum achievable average SNR at the legitimate receiver and the number of antennas at the transmitter.
- Compared with the exhaustive search method, which requires Eve's prior information, we confirm that the OAPA achieves the lowest worst-case SOP, and the SFPA achieves a near-optimal secrecy performance, in terms of worst-case SOP, with the lowest complexity.

The rest of this paper is organized as follows. Section II presents the system model. In Section III, both the OAPA and SFPA schemes are designed. In Section IV, the closed-form expressions for the average SOP and worst-case SOP are derived under the proposed OAPA and SFPA schemes, respectively. Numerical results are provided in Section V, followed by conclusions in Section VI.

Throughout this paper, the following notation conventions are adopted. The boldface uppercase and lowercase letters denote matrices and vectors, respectively. $\binom{K}{k} = \frac{K!}{(K-k)!k!}$ is the binomial coefficient. $(\cdot)^{\mathrm{H}}$ is the conjugate transpose operation, while $(\cdot)^{-1}$ and $\|\cdot\|_F$ denote the inverse operator and Frobenius norm of a matrix, respectively. $f_X(\cdot)$, $F_X(\cdot)$ and $R_X(\cdot)$ denote the probability density function (PDF), cumulative distribution function (CDF) and complementary cumulative distribution function (CCDF) of random variable (RV) X, respectively. $\Pr(\cdot)$ denotes the probability operator. $\mathcal{CN}(\mu, \sigma^2)$ denotes the circularly symmetric complex Gaussian distribution with mean μ and variance σ^2. $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1}\exp(-x)dx$ denotes the Gamma function, and $\Gamma(\alpha, x) = \int_x^\infty t^{\alpha-1}\exp(-t)dt$ is the upper incomplete Gamma function. $E[\cdot]$ denotes the expectation operator, and $\boldsymbol{I}_n$ is the $n \times n$ identity matrix, while $[x]^+ \triangleq \max\{0, x\}$.

II. System Model and Problem Formulation

We consider secure communication between a transmitter (Alice) and a receiver (Bob) in the presence of a multi-antenna eavesdropper (Eve). We assume that Bob is equipped with a single antenna, while Alice and Eve have N_t and N_e antennas, respectively. Let $\boldsymbol{h} \in \mathbb{C}^{1\times N_t}$ and $\boldsymbol{G} \in \mathbb{C}^{N_e\times N_t}$ denote the channels from Alice to Bob and Alice to Eve, respectively. All the wireless links are assumed to be independently Rayleigh fading, where the channel gains are modeled as the zero-mean complex Gaussian RVs. Each entry of $\boldsymbol{h}$ and $\boldsymbol{G}$ has a variance of $1/\lambda_B$ and $1/\lambda_E$, respectively. Considering an unknown eavesdropper, we assume that the prior information of Eve, such as $\boldsymbol{G}$, N_e and λ_E, are unavailable for all the nodes in the network.[1]

Since Eve is unknown, the AN-aided secure scheme of [14] is employed to guarantee the security for Alice. Alice transmits an information-bearing signal u with $E[|u|^2]=1$ in conjunction with an $(N_t-1)\times 1$ AN vector $\boldsymbol{v}$ to impair Eve's channel. Accordingly, the transmit signal of Alice is

$$\boldsymbol{x} = \sqrt{\phi P}\boldsymbol{w}u + \sqrt{(1-\phi)P}\boldsymbol{W}\boldsymbol{v}, \tag{1}$$

where P denotes the total transmit power at Alice, $\phi\in(0,\ 1]$ is the PAF which represents the fraction of transmit power allocated to u, $\boldsymbol{w} = \boldsymbol{h}^{\mathrm{H}}/\|\boldsymbol{h}\|$ is the precoding vector of the information-bearing signal, and $\boldsymbol{W}\in\mathbb{C}^{N_t\times(N_t-1)}$ is the precoding matrix of the jamming signal which lies in the null space of $\boldsymbol{h}^{\mathrm{H}}$. Thus, $\widetilde{\boldsymbol{W}} = [\boldsymbol{w}\ \boldsymbol{W}]$ forms an orthogonal basis of $\mathbb{C}^{N_t}$. Since Alice does not know $\boldsymbol{G}$, the transmit power allocated to the AN is distributed equally to each entry of $\boldsymbol{v}$. That is, all the entries of $\boldsymbol{v}$ are independently identically distributed (i.i.d) complex RVs obeying $\mathcal{CN}\left(0, \frac{1}{N_t-1}\right)$.

Consequently, the instantaneous SNRs at Bob and Eve can be respectively written as

$$\Gamma_B = \frac{\phi P}{\sigma_B^2}\|\boldsymbol{h}\|^2, \tag{2}$$

$$\Gamma_E = \phi P\widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\frac{(1-\phi)P}{N_t-1}\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}} + \sigma_E^2\boldsymbol{I}_{N_e}\right)^{-1}\widetilde{\boldsymbol{g}}, \tag{3}$$

where $\widetilde{\boldsymbol{g}} = \boldsymbol{G}\boldsymbol{w}$ and $\widetilde{\boldsymbol{G}} = \boldsymbol{G}\boldsymbol{W}$, while σ_B^2 and σ_E^2 are the channel noise variances at Bob and Eve, respectively. Hence, the channel capacities of the main link and wiretap link are given respectively by $C_B = \log_2(1+\Gamma_B)$ and $C_E = \log_2(1+\Gamma_E)$, and the instantaneous secrecy capacity in the considered wiretap system can be expressed as [31]

$$C_S = [C_B - C_E]^+. \tag{4}$$

For notational convenience, we define $\bar{\gamma}_B \triangleq \frac{P}{\sigma_B^2}$ and $\bar{\gamma}_E \triangleq \frac{P}{\sigma_E^2}$ as the maximum average transmit SNRs to Bob and Eve, respectively. We also define $X \triangleq \|\boldsymbol{h}\|^2$ as the power gain of the main channel.

To avoid undesired transmissions that incur capacity outages, we adopt the on-off transmission scheme proposed in [4], in which Alice does not transmit when $C_B < R_S$. Utilizing the well-known Wyner's wiretap encoding scheme, Alice transmits the codewords and confidential information at constant rates R_B and R_S, respectively. The rate of redundant information $R_E = R_B - R_S$ reflects the cost of providing a security guarantee for message transmission against eavesdropping. For any message transmitted, if Eve's channel is worse than Alice's estimate, i.e., $C_E < R_E$, the information leakage rate for Eve can be arbitrarily small. By contrast, if $C_E > R_E$, information-theoretic security is compromised, and a secrecy outage event occurs. To avoid undesired transmissions that incur capacity outages, we invoke the secrecy outage formulation introduced in [32], in which a secrecy outage event is defined as $\mathcal{O}(R_B, R_S) := \{C_E > R_B - R_S\,|\text{message transmission}\}$ conditioned upon a message actually being transmitted.

In this paper, the value of R_B is chosen dynamically such that $R_B = C_B$ within an infinite blocklength assumption, which has been extensively adopted in the works concerning on PLS, e.g., [33], [34]. To avoid undesired secrecy outages, we have

$$C_B \geq R_S. \tag{5}$$

Substituting (2) into (5), we have

$$X \geq \frac{\varepsilon - 1}{\phi\bar{\gamma}_B}. \tag{6}$$

where $\varepsilon \triangleq 2^{R_S}$. From (6), we know that in order to avoid undesired secrecy outages, the following two constraints should be simultaneously satisfied:

$$X \geq \frac{\varepsilon - 1}{\bar{\gamma}_B}, \tag{7}$$

$$\phi \geq \phi_{\min} \triangleq \frac{\varepsilon - 1}{\bar{\gamma}_B X}. \tag{8}$$

Constraints (7) and (8) provide lower bounds for the power gains of the main channel X and the PAF, respectively.

In the on-off transmission scheme, Alice only transmits on condition that a reliable transmission is guaranteed to avoid undesired secrecy outages. As such, a reliable transmission only happens when X is not below a preset threshold μ; otherwise, it keeps silent. Based on (7), we set $\mu = \frac{\varepsilon-1}{\bar{\gamma}_B}$ without of loss generality. Thus, a secrecy outage event for a given μ and target secrecy rate $R_S > 0$ is defined as

$$\mathcal{O}(R_S) := \{C_S < R_S\,|X \geq \mu\}. \tag{9}$$

Also, the SOP can be formulated as

$$P_{out} = \Pr\left(C_S < R_S\,|X \geq \mu\right). \tag{10}$$

In the following, we will focus our attention on the outage-optimal power allocation schemes. On this basis, we will further conduct the secrecy outage performance analysis.

III. Outage-Optimal Power Allocation

We optimize the PAF for the purpose of minimizing the SOP. Traditionally, this optimization can be formulated as

$$\phi^\star = \arg\min_{\phi_{\min}\leq\phi\leq 1} P_{out}. \tag{11}$$

[1] Notably, the eavesdropper's prior information is employed to conduct the secrecy outage performance analysis in Section IV, but not used for the secure transmission designs. This common assumption has been widely adopted in the literature concerning on PLS, e.g., [15], [22].

To solve this optimization problem, intuitively, the closed-form expression for the SOP as the function of the PAF should first be derived, and then the derivative of the derived SOP with respect to (w.r.t.) the PAF is taken to obtain the optimal solution. However, the analytical expression for the SOP is typically cumbersome, and a closed-form solution for the optimal PAF may be intractable. Moreover, the closed-form expression for P_{out} may require Eve's prior information.

In order to tackle this troublesome problem, our approach is to minimize the possibility of each secrecy outage event instead of the SOP. Observing from (9), we find that to avoid the secrecy outage event $\mathcal{O}(R_S)$ as much as possible, we can maximize the instantaneous secrecy capacity C_S by optimizing the PAF. Substituting (2) and (3) into (4), we have

$$C_S = \log_2\left(\frac{1+\phi\bar{\gamma}_B\|\boldsymbol{h}\|^2}{1+\phi\bar{\gamma}_E\widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\frac{(1-\phi)\bar{\gamma}_E}{N_t-1}\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}}+\boldsymbol{I}_{N_e}\right)^{-1}\widetilde{\boldsymbol{g}}}\right). \quad (12)$$

C_S of (12) involves Eve's prior information which is unknown. Therefore, it is still intractable to find the optimal PAF with an unknown eavesdropper.

Since the noise level at Eve is also unknown, it is reasonable to consider the worst-case scenario to guarantee secure transmission, where the channel noise at Eve is zero [24], [25]. With this worst-case assumption, (12) can be simplified as

$$\widehat{C}_S = \log_2\left(\frac{1+\phi\bar{\gamma}_B X}{1+\frac{\phi(N_t-1)}{1-\phi}\widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}}\right)^{-1}\widetilde{\boldsymbol{g}}}\right). \quad (13)$$

$\widehat{C}_S$ still contains Eve's prior information. In order to optimize the PAF for minimizing the SOP, we make a transformation to remove the influence of Eve's prior information in the worst-case scenario in the following subsection.

A. Optimal Adaptive Power Allocation

Substituting (13) into (9), we have

$$\mathcal{O}(R_S) := \left\{\log_2\left(\frac{1+\phi\bar{\gamma}_B X}{1+\frac{\phi(N_t-1)}{1-\phi}Y}\right) < R_s \,\middle|\, X \geq \mu\right\}. \quad (14)$$

After some algebraic manipulations, the secrecy outage event (14) can be reformulated as

$$\mathcal{O}(R_S) := \{\omega(\phi) < Y \,|X \geq \mu\}, \quad (15)$$

where $\omega(\phi) = \frac{(1-\varepsilon+\phi\bar{\gamma}_B X)(1-\phi)}{\varepsilon(N_t-1)\phi}$ and $Y \triangleq \widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}}\right)^{-1}\widetilde{\boldsymbol{g}}$. As shown in (15), $\omega(\phi)$ involves the instantaneous CSI $\boldsymbol{h}$, which is the prior knowledge at Alice, and Y contains the CSI between Alice and Eve but it is independent of ϕ. Based on this observation, for the case of unknown Eve's prior information, the optimal PAF $\phi^\star$ of the proposed OAPA scheme is attained by solving the following optimization

$$\phi^\star = \arg\max_{\phi_{\min}\leq\phi\leq 1}\omega(\phi). \quad (16)$$

Since $\frac{\partial^2\omega(\phi)}{\partial\phi^2} = -\frac{2(\varepsilon-1)}{\varepsilon(N_t-1)\phi^3} < 0$, $\omega(\phi)$ is a concave function. Hence, we can calculate the first derivative of $\omega(\phi)$ w.r.t. ϕ and set it to zero to obtain the optimal $\phi^\star$, which is given as

$$\phi^\star = \begin{cases}\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}, & X \geq \mu,\\ \varnothing, & X < \mu.\end{cases} \quad (17)$$

Note that when $X < \mu$, the PAF is $\phi^\star = \varnothing$, and this signifies that the message transmission is suspended in order to avoid an undesired capacity outage.

Remark 1: Conditioning on Eve's instantaneous CSI is absent in (17), and the OAPA scheme guarantees the optimal performance, in terms of SOP, in the worst-case scenario whether Eve's prior information is known or not.

Remark 2: The result of (17) reveals that $\phi^\star$ is determined by the maximum achievable instantaneous SNR at Bob $\widetilde{\Gamma}_B = \bar{\gamma}_B\|\boldsymbol{h}\|^2$ and the target secrecy rate R_S. Under the condition that reliable transmission is guaranteed, larger $\widetilde{\Gamma}_B$ or smaller R_S decreases $\phi^\star$. In other words, when $\widetilde{\Gamma}_B$ increases or R_S decreases, more power should be allocated to the AN for minimizing the SOP.

Remark 2 provides insightful guidelines for power allocation design in the absence of Eve's prior information. The legitimate link $\boldsymbol{h}$ can be obtained for Alice through the channel estimation by legitimate node Bob, while the unknown $\boldsymbol{G}$ is not required. Therefore, our proposed OAPA scheme, which adaptively adjusts the PAF based on the instantaneous CSIs of legitimate links, can be effectively applied to the practical networks in the passive eavesdropping environment to achieve optimal performance.

B. Suboptimal Fixed Power Allocation

The optimal PAF of the OAPA scheme needs to be adjusted whenever the channel $\boldsymbol{h}$ changes, which imposes excessive computational complexity. To reduce the computational load, we propose a SFPA scheme. According to the law of large numbers, for sufficiently large N_t and in the limit case, $N_t \to \infty$, Γ_B of (2) can be re-expressed as

$$\lim_{N_t\to\infty}\Gamma_B = \frac{\phi\bar{\gamma}_B N_t}{\lambda_B}. \quad (18)$$

By substituting (13) and (18) into (9), the secrecy outage event (9) can be reformulated as

$$\widetilde{\mathcal{O}}(R_S) := \{\theta(\phi) < Y \,|X \geq \mu\}, \quad (19)$$

where $\theta(\phi) = \left(1-\varepsilon+\frac{\phi\bar{\gamma}_B N_t}{\lambda_B}\right)\frac{1-\phi}{\varepsilon\phi(N_t-1)}$. A similar procedure as the derivation of (17) can be followed to obtain the optimal PAF $\phi^\star_\infty$ of the SFPA scheme that minimizes the SOP, when $X \geq \mu$

$$\phi^\star_\infty = \begin{cases}\sqrt{\frac{\varepsilon-1}{\bar{\Gamma}_B N_t}}, & \bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t},\\ 1, & \bar{\Gamma}_B < \frac{\varepsilon-1}{N_t},\end{cases} \quad (20)$$

where $\bar{\Gamma}_B = \bar{\gamma}_B\lambda_B^{-1}$ represents the maximum achievable average SNR at Bob. Similarly, when $X < \mu$, the message transmission is suspended.

Remark 3: The results of (20) indicate that the optimal PAF $\phi^\star_\infty$ is independent of Eve's prior information. $\phi^\star_\infty$ is

determined by $\bar{\Gamma}_B$, N_t and R_S. If $\bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t}$ holds, increasing $\bar{\Gamma}_B$ and/or N_t decreases $\phi_\infty^\star$, while a smaller R_S leads to a smaller $\phi_\infty^\star$. That is, when $\bar{\Gamma}_B$ and/or N_t increase or when R_S decreases, more power should be allocated to the AN for minimizing the SOP. When $\bar{\Gamma}_B$ is less than a threshold, pure beamforming would be a more preferable choice.

Since the instantaneous CSIs of legitimate links vary rapidly in fast fading environments, the application of the OAPA scheme is limited in such situations owing to its implementation complexity. It is worth noting that the parameters $\bar{\Gamma}_B$, N_t, and R_S can be readily obtained at Alice. Hence, the proposed SFPA scheme provides a simple and efficient way for power allocation design. As will be demonstrated in the numerical results, the SFPA scheme achieves a near-optimal secrecy outage performance in the worst-case scenario.

IV. Secrecy Outage Performance Analysis

In this section, the closed-form expressions for SOP in the considered wiretap systems using the proposed OAPA and SFPA schemes are derived.

A. Optimal Adaptive Power Allocation

Our proposed power allocation schemes are performed in the worst-case scenario. However, the channel noise at Eve σ_E^2 always exists. For an unknown σ_E^2, Alice is still able to perform the AN-aided secure transmission scheme, but in this case, Alice is unable to calculate the true secrecy performance metrics. To address a more practical case, we first proceed to conduct the secrecy outage performance analysis of the proposed power allocation schemes under a preset σ_E^2 value.

1) Secrecy Outage Performance Under a Preset σ_E^2 Value: First, we analyze the SOP over each X, which is referred to as the average SOP. Substituting (12) and (17) into (10), the expression for the average SOP for the OAPA scheme P_{out}^o is derived as

$$P_{out}^o = \Pr\left(\frac{1+\sqrt{(\varepsilon-1)\bar{\gamma}_B X}}{1+\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}\bar{\gamma}_E \widetilde{Y}} < \varepsilon \middle| X \geq \mu\right), \tag{21}$$

where $\widetilde{Y} = \widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\Theta\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}} + \boldsymbol{I}_{N_e}\right)^{-1}\widetilde{\boldsymbol{g}}$ with $\Theta \triangleq \frac{\left(1-\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}\right)\bar{\gamma}_E}{N_t-1}$. Using the total probability theorem and after some algebraic manipulations, P_{out}^o is further derived as

$$\begin{aligned} P_{out}^o &= \frac{\Pr\left(\frac{1+\sqrt{(\varepsilon-1)\bar{\gamma}_B X}}{1+\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}\bar{\gamma}_E \widetilde{Y}} < \varepsilon, X \geq \mu\right)}{\Pr(X \geq \mu)} \\ &= \frac{\overbrace{\Pr\left(\frac{\sqrt{\bar{\gamma}_B X}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\gamma}_E} < \widetilde{Y}, X \geq \mu\right)}^{\Psi_1}}{\Pr(X \geq \mu)}, \end{aligned} \tag{22}$$

Since the quantity $\widetilde{Y}$ is equivalent to the signal-to-interference ratio (SIR) of an N_e-branch MMSE diversity combiner with $N_t - 1$ interferers, the CCDF of $\widetilde{Y}$ is obtained from [35, eq. (11)] as

$$R_{\widetilde{Y}}(y) = \sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m} \frac{\binom{N_t-1}{n}\lambda_E^{m-1}\Theta^n}{(m-1)!}\frac{y^{m+n-1}\exp\left(-\lambda_E y\right)}{(1+\Theta y)^{N_t-1}}. \tag{23}$$

Since X follows a Gamma distribution with the parameters N_t and $1/\lambda_B$, the PDF and CDF of X can be respectively expressed as

$$f_X(x) = \frac{\lambda_B^{N_t}}{\Gamma(N_t)}x^{N_t-1}\exp(-\lambda_B x), \tag{24}$$

$$F_X(x) = 1 - \sum_{k=0}^{N_t-1}\frac{\lambda_B^k x^k}{k!}\exp\left(-\lambda_B x\right). \tag{25}$$

Substituting (23), (24) and (25) into (22), Ψ_1 can be derived as (26), as shown at the bottom of the next page, where $\bar{\Gamma}_E = \bar{\gamma}_E\lambda_E^{-1}$ represents the maximum average received SNR at Eve.

Due to the complicated integral term involved, it is intractable to derive an accurate analytical expression for Ψ_1. To tackle this problem, we give an approximate expression with an arbitrarily small error by invoking the truncation method. To proceed, the integral term in $\mathcal{O}_1$ is recast as

$$T(x) = H_1(x)H_2(x)H_3(x), \tag{27}$$

where

$$H_1(x) = \frac{\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)^{2n}}{\left(1+\frac{\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{N_t-1}}, \tag{28}$$

$$H_2(x) = \exp\left(-\lambda_B x\right)x^{N_t-1}, \tag{29}$$

$$\begin{aligned} H_3(x) = &\left(\sqrt{\bar{\gamma}_B x}\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)\right)^{m-1} \\ &\times\exp\left(-\frac{\sqrt{\bar{\gamma}_B x}\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\Gamma}_E}\right). \end{aligned} \tag{30}$$

We have the following **Proposition 1**.

Proposition 1: $T(x)$ is strictly decreasing for $x \in [A, \infty)$, where $A = \max\{x^*, x^o, x^\#\}$ with $x^* = \frac{\left(\sqrt{\frac{\varepsilon n(N_t-1)}{N_t-1-n}}+\sqrt{\varepsilon-1}\right)^2}{\bar{\gamma}_B}$, $x^o = \frac{N_t-1}{\lambda_B}$ and $x^\# = \frac{\varepsilon\left(1+2\bar{\Gamma}_E(m-1)\right)-1}{2\bar{\gamma}_B} + \frac{\sqrt{\varepsilon-1}\sqrt{\varepsilon-1+4\varepsilon\bar{\Gamma}_E(m-1)}}{2\bar{\gamma}_B}$.

Proof: See Appendix A. ∎

Combining **Proposition 1** with $\lim_{x\to\infty} T(x) = 0$, we conclude that there exists a sufficiently large $\Phi_1 > \max\{A, \mu\}$ which makes the approximate error $\int_{\Phi_1}^{\infty} T(x)dx \approx 0$. By truncating the infinite integral w.r.t. Φ_1, the expression for $\mathcal{O}_1$ is approximately given as

$$\mathcal{O}_1 \approx \int_{\mu}^{\Phi_1} T(x)dx. \tag{31}$$

The integral (31) is still mathematically intractable, and we use Gaussian-Chebyshev quadrature [36] to find an approximation

of $\mathcal{O}_1$. Consequently, $\mathcal{O}_1$ can be approximated as follows:

$$\mathcal{O}_1 \approx \frac{\pi(\Phi_1-\mu)}{2K}\sum_{k=1}^{K}\sqrt{1-v_k^2}\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)^{m+2n-1} \times\left(\sqrt{\bar{\gamma}_B s_k}\right)^{m-1}\left(1+\frac{\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{1-N_t} \times\exp\left(-\frac{\sqrt{\bar{\gamma}_B s_k}\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\Gamma}_E}-\lambda_B s_k\right)s_k^{N_t-1}, \tag{32}$$

where K is a parameter to trade off complexity and accuracy, $v_k=\cos\left(\frac{2k-1}{2K}\pi\right)$ and $s_k=\frac{\Phi_1-\mu}{2}(v_k+1)+\mu$.

For any given values of R_S and μ, we can compute the transmission probability as

$$\Pr(X>\mu)=\sum_{k=0}^{N_t-1}\frac{\lambda_B^k\mu^k}{k!}\exp(-\lambda_B\mu)=\frac{\Gamma(N_t,\lambda_S\mu)}{\Gamma(N_t)}. \tag{33}$$

Substituting (32) into (26), we obtain Ψ_1. Substituting the resulting Ψ_1 and (33) into (22), the average SOP for the OAPA scheme can be approximated as follows[2]

$$P_{out}^{o}\approx\frac{\lambda_B^{N_t}}{\Gamma\left(N_t,\lambda_B\mu\right)}\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\binom{N_t-1}{n}\bar{\Gamma}_E^{1-m}}{(m-1)!(N_t-1)^n\varepsilon^{m+n-1}} \times\frac{\pi(\Phi_1-\mu)}{2K}\sum_{k=1}^{K}\sqrt{1-v_k^2}\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)^{m+2n-1} \times\left(\sqrt{\bar{\gamma}_B s_k}\right)^{m-1}\left(1+\frac{\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{1-N_t} \times\exp\left(-\frac{\sqrt{\bar{\gamma}_B s_k}\left(\sqrt{\bar{\gamma}_B s_k}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\Gamma}_E}-\lambda_B s_k\right)s_k^{N_t-1}. \tag{34}$$

The result (34) is too cumbersome to infer further insights. The optimal PAF of the OAPA scheme is adjusted according to the instantaneous channel between the legitimate transceiver. Therefore, it is reasonable to address the secrecy outage performance under each X. We define the probability of secrecy outage under each X as the instantaneous SOP (ISOP). When $X\geq\mu$ is satisfied, the ISOP can be derived as

$$P_{out}^{io}=\Pr\left(\frac{1+\sqrt{(\varepsilon-1)\bar{\gamma}_B X}}{1+\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}\bar{\gamma}_E\widetilde{Y}}<\varepsilon\right) =\Pr\left(\frac{\sqrt{\bar{\gamma}_B X}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\gamma}_E}<\widetilde{Y}\right). \tag{35}$$

Resorting to (23), P_{out}^{io} can readily be expressed as

$$P_{out}^{io}=\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\binom{N_t-1}{n}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^{m+2n-1}}{(m-1)!\varepsilon^{m+n-1}\left(\bar{\Gamma}_E\right)^{m-1}(N_t-1)^n} \times\frac{\left(\sqrt{\bar{\gamma}_B X}\right)^{m-1}\exp\left(-\frac{\sqrt{\bar{\gamma}_B X}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\Gamma}_E}\right)}{\left(1+\frac{\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{N_t-1}}. \tag{36}$$

As $\sigma_e^2\to 0$, we have

$$\lim_{\sigma_e^2\to 0}P_{out}^{io}=\frac{\sum_{n=0}^{N_e-1}\frac{\binom{N_t-1}{n}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^{2n}}{\varepsilon^n(N_t-1)^n}}{\left(1+\frac{\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{N_t-1}} \overset{(a)}{=}\frac{\sum_{n=0}^{N_e-1}\frac{\binom{N_t-1}{n}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^{2n}}{\varepsilon^n(N_t-1)^n}}{\sum_{n=0}^{N_t-1}\frac{\binom{N_t-1}{n}\left(\sqrt{\bar{\gamma}_B X}-\sqrt{\varepsilon-1}\right)^{2n}}{\varepsilon^n(N_t-1)^n}}, \tag{37}$$

where (a) follows the binomial theorem. From (37), we have the following remark.

Remark 4: If $\sigma_E^2=0$, Eve can eliminate the AN transmitted by Alice, and the ISOP is always one when Eve is equipped with no fewer antennas than Alice.

2) Secrecy Outage Performance in Worst-Case Scenario: To characterize the secrecy outage performance when the average transmit SNR at Eve is relatively high, i.e., $\sigma_E^2\to 0$, we derive the approximate expression for the average SOP for the worst-case scenario in the following theorem.

Theorem 1: The average SOP for the OAPA scheme in the worst-case scenario can be approximated as

$$P_{out}^{o,w}\approx\frac{\Gamma(N_t)}{\Gamma(N_t,\lambda_S\mu)}\mho(\mu), \tag{38}$$

[2]Notably, (34) is the approximation of the exact SOP, and the approximate error mainly arises from the truncation point Φ_1 and K, which is selected to trade off complexity and accuracy. When the values of K and Φ_1 are large, the accuracy is high, while imposing a high computation complexity.

$$\Psi_1=\frac{\lambda_B^{N_t}}{\Gamma(N_t)}\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\binom{N_t-1}{n}\bar{\Gamma}_E^{1-m}}{(m-1)!(N_t-1)^n\varepsilon^{m+n-1}} \times\underbrace{\int_{\mu}^{\infty}\frac{\left(\sqrt{\bar{\gamma}_B x}\right)^{m-1}\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)^{m+2n-1}\exp\left(-\frac{\sqrt{\bar{\gamma}_B x}\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)}{\varepsilon\bar{\Gamma}_E}-\lambda_B x\right)}{\left(1+\frac{\left(\sqrt{\bar{\gamma}_B x}-\sqrt{\varepsilon-1}\right)^2}{(N_t-1)\varepsilon}\right)^{N_t-1}}x^{N_t-1}dx}_{\mathcal{O}_1}, \tag{26}$$

where $\mho(\mu)$ is defined in (39), as shown at the bottom of the page. In (39), $A = \frac{\lambda_B}{\bar{\gamma}_B}$, $B = \sqrt{\varepsilon - 1}$, $C = \sqrt{\varepsilon\left(N_t - 1\right)}$, and $\tau(\mu) \triangleq \frac{\left(\sqrt{\bar{\gamma}_B \mu} - \sqrt{\varepsilon - 1}\right)^2}{\varepsilon(N_t - 1)}$, while T and G are the parameters for the complexity and accuracy trade-off, $\nu_t = \cos\left(\frac{2t-1}{2T}\pi\right)$, $s_t = \frac{\Phi_2 - \sqrt{\tau(\mu)}}{2}\left(\nu_t + 1\right) + \sqrt{\tau(\mu)}$, $\nu_g = \cos\left(\frac{2g-1}{2G}\pi\right)$, $s_g = \frac{\Phi_3 - \sqrt{\tau(\mu)}}{2}\left(\nu_g + 1\right) + \sqrt{\tau(\mu)}$, and $\Phi_3 > \max\left\{\sqrt{\frac{2m+n+1}{2N_t - 2m - n - 1}}, \sqrt{\tau(\mu)}\right\}$. Φ_2 and Φ_3 are the truncation points.

Proof: See Appendix B. ∎

B. Suboptimal Fixed Power Allocation

We now derive the closed-form expression of the average SOP for the SFPA scheme.

1) Secrecy Outage Performance Under a Preset σ_E Value: When $\bar{\Gamma}_B \geq \frac{\varepsilon - 1}{N_t}$ holds, substituting (2), (3), (12) and (20) into (10) leads to the average SOP of the SFPA scheme

$$P_{out}^{s} = \Pr\left(\frac{1 + \widetilde{\phi}\bar{\gamma}_B X}{1 + \widetilde{\phi}\bar{\gamma}_E \widetilde{Z}} < \varepsilon \middle| X > \mu\right), \tag{40}$$

where $\widetilde{\phi} = \sqrt{\frac{\varepsilon - 1}{\bar{\Gamma}_B N_t}}$ and $\widetilde{Z} = \widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\Lambda \widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}} + \boldsymbol{I}_{N_e}\right)^{-1}\widetilde{\boldsymbol{g}}$ with $\Lambda \triangleq \frac{\left(1 - \widetilde{\phi}\right)\bar{\gamma}_E}{N_t - 1}$. With the aid of the total probability formula and resorting to (33), P_{out}^{s} is further derived as

$$\begin{aligned} P_{out}^{s} &= \frac{\Pr\left(\mu < X < \ell_1 + \ell_3 \widetilde{Z}\right)}{\Pr(X > \mu)} \\ &= \frac{\Gamma(N_t)}{\Gamma(N_t, \lambda_B \mu)} \underbrace{\int_{\xi}^{\infty} \int_{\mu}^{\ell_1 + \ell_3 z} f_X(x) dx f_{\widetilde{Z}}(z) dz}_{\Xi_3}, \end{aligned} \tag{41}$$

where $\ell_l = \frac{\varepsilon - 1}{\widetilde{\phi}\bar{\gamma}_B}$, $\ell_3 = \frac{\varepsilon \bar{\gamma}_E}{\bar{\gamma}_B}$ and $\xi = \max\left\{\frac{\mu - \ell_1}{\ell_3}, 0\right\}$. As shown in (41), to obtain the closed-form expression for the Ξ_3, we need to characterize the CDF of the positive random variable $\widetilde{Z}$. The CCDF of $\widetilde{Z}$ is given by [35, eq. (11)]

$$R_{\widetilde{Z}}(z) = \sum_{m=1}^{N_e} \sum_{n=0}^{N_e - m} \frac{\binom{N_t - 1}{n} \lambda_E^{m-1} \Lambda^n}{(m-1)!} \frac{z^{m+n-1} \exp\left(-\lambda_E z\right)}{(1 + \Lambda z)^{N_t - 1}}. \tag{42}$$

Resorting to (25) and binomial series expansion, Ξ_3 can be calculated as (43), as shown at the bottom of the page. Utilizing [37, eq. (2.33.10)], we have

$$\begin{aligned} \mathcal{Q}_1 = R_{\widetilde{Z}}(\xi) \exp(-\lambda_B \ell_3 \xi) \\ - \lambda_B \ell_3 \underbrace{\int_{\xi}^{\infty} R_{\widetilde{Z}}(z) \exp(-\lambda_B \ell_3 z) dz}_{\mathcal{G}_1}. \end{aligned} \tag{44}$$

Substituting $R_{\widetilde{Z}}(z)$ into $\mathcal{G}_1$, we arrive at

$$\begin{aligned} \mathcal{G}_1 = \sum_{m=1}^{N_e} \sum_{n=0}^{N_e - m} \frac{\binom{N_t - 1}{n} \lambda_E^{m-1} \Lambda^{n - N_t + 1}}{(m-1)!} \\ \times \int_{\xi}^{\infty} \frac{z^{m+n-1} \exp\left(-(\lambda_E + \lambda_B \ell_3) z\right)}{\left(\Lambda^{-1} + z\right)^{N_t - 1}} dz. \end{aligned} \tag{45}$$

Applying the binomial series expansion to (45) and utilizing [37], we arrive at

$$\begin{aligned} \mathcal{G}_1 &= \sum_{m=1}^{N_e} \sum_{n=0}^{N_e - m} \sum_{q=0}^{\kappa} \frac{(-1)^{\kappa + q} \binom{N_t - 1}{n} \binom{\kappa}{q} \lambda_E^{m-1} \Lambda^{2+q-m-N_t}}{(m-1)!} \\ &\quad \times \int_{\xi}^{\infty} \frac{\exp\left(-(\lambda_E + \lambda_B \ell_3) z\right)}{\left(\Lambda^{-1} + z\right)^{N_t - 1 - q}} dz \\ &= \sum_{m=1}^{N_e} \sum_{n=0}^{N_e - m} \sum_{q=0}^{\kappa} \frac{(-1)^{\kappa + q} \binom{N_t - 1}{n} \binom{\kappa}{q} \lambda_E^{m-1} \Lambda^{2+q-m-N_t}}{(m-1)!} \Omega(q), \end{aligned} \tag{46}$$

where $\kappa \triangleq m + n - 1$ and

$$\begin{aligned} \Omega(q) \triangleq \exp\left(\frac{\lambda_E + \ell_3 \lambda_B}{\Lambda}\right) \left(\lambda_E + \ell_3 \lambda_B\right)^{N_t - 2 - q} \\ \times \Gamma\left(2 + q - N_t, \left(\Lambda^{-1} + \xi\right)\left(\lambda_E + \ell_3 \lambda_B\right)\right). \end{aligned} \tag{47}$$

$$\begin{aligned} \mho(\mu) = \sum_{k=0}^{N_t - 1} \sum_{m=0}^{N_e - 1} \frac{\binom{N_t - 1}{m} \tau^m(\mu)}{(1 + \tau(\mu))^{N_t - 1}} \frac{\lambda_B^k \mu^k \exp\left(-\lambda_B \mu\right)}{k!} - \sum_{k=0}^{N_t - 1} \frac{A^k}{k!} \left(\sum_{m=0}^{N_e - 1} \sum_{n=0}^{2k} \binom{N_t - 1}{m} \binom{2k}{n} (N_t - 1) B^{2k-n} C^n \right. \\ \times \frac{\pi\left(\Phi_2 - \sqrt{\tau(\mu)}\right)}{T} \sum_{t=1}^{T} \sqrt{1 - \nu_t^2} s_t^{2m+n+1} \left(1 + s_t^2\right)^{-N_t} \exp\left(-A(B + C s_t)^2\right) - \sum_{m=1}^{N_e - 1} \sum_{n=0}^{2k} \binom{N_t - 1}{m} \binom{2k}{n} m B^{2k-n} C^n \\ \left. \times \frac{\pi\left(\Phi_3 - \sqrt{\tau(\mu)}\right)}{G} \sum_{g=1}^{G} \sqrt{1 - \nu_g^2} s_g^{2m+n-1} \left(1 + s_g^2\right)^{1 - N_t} \exp\left(-A\left(B + C s_g\right)^2\right) \right). \end{aligned} \tag{39}$$

$$\begin{aligned} \Xi_3 = \sum_{k=0}^{N_t - 1} \sum_{m=1}^{N_e} \sum_{n=0}^{N_e - m} \frac{\lambda_B^k \mu^k \exp(-\lambda_B \mu) \binom{N_t - 1}{n} \lambda_E^{m-1}}{k!(m-1)!} \frac{\Lambda^n \xi^{m+n-1} \exp(-\lambda_E \xi)}{(1 + \Lambda \xi)^{N_t - 1}} - \exp(-\lambda_B \ell_1) \\ \times \underbrace{\int_{\xi}^{\infty} \exp(-\lambda_B \ell_3 z) f_{\widetilde{Z}}(z) dz}_{\mathcal{Q}_1} - \sum_{k=1}^{N_t - 1} \frac{\lambda_B^k \exp(-\lambda_B \ell_1)}{k!} \underbrace{\int_{\xi}^{\infty} (\ell_1 + \ell_3 z)^k \exp(-\lambda_B \ell_3 z) f_{\widetilde{Z}}(z) dz}_{\mathcal{Q}_2}. \end{aligned} \tag{43}$$

In a similar way, $\mathcal{Q}_2$ can be derived as

$$\mathcal{Q}_2 = R_{\tilde{Z}}(\xi)\exp\big(-\lambda_B\ell_3\xi\big)\big(\ell_1+\ell_3\xi\big)^k + k\ell_3\underbrace{\int_{\xi}^{\infty} R_{\tilde{Z}}(z)\big(\ell_1+\ell_3 z\big)^{k-1}\exp\big(-\lambda_B\ell_3 z\big)dz}_{\Delta_3} - \lambda_B\ell_3\underbrace{\int_{\xi}^{\infty} R_{\tilde{Z}}(z)\big(\ell_1+\ell_3 z\big)^{k}\exp\big(-\lambda_B\ell_3 z\big)dz}_{\Delta_4}. \quad (48)$$

Substituting $R_{\tilde{Z}}(z)$ into Δ_3 and using binomial series expansion, Δ_3 can be computed as

$$\Delta_3 = \sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\binom{N_t-1}{n}\lambda_E^{m-1}\Lambda^{n-N_t+1}}{(m-1)!}\sum_{l=0}^{k-1}\binom{k-1}{l} \times\ell_1^{k-1-l}\ell_3^{l}\int_{\xi}^{\infty}\frac{z^{\zeta}\exp\left(-(\lambda_E+\lambda_B\ell_3)z\right)}{\left(\Lambda^{-1}+z\right)^{N_t-1}}dz, \quad (49)$$

where $\zeta \triangleq m+n+l-1$. Applying the binomial series expansion to (49) and with the aid of [37], we arrive at

$$\begin{aligned}\Delta_3 &= \sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\binom{N_t-1}{n}\lambda_E^{m-1}\Lambda^{n-N_t+1}}{(m-1)!}\sum_{l=0}^{k-1}\binom{k-1}{l}\ell_1^{k-1-l} \times\ell_3^{l}\sum_{q=0}^{\zeta}(-1)^{\zeta+q}\binom{\zeta}{q}\Lambda^{q-\zeta} \times\int_{\xi}^{\infty}\frac{\exp\left(-(\lambda_E+\lambda_B\ell_3)z\right)}{(\Lambda^{-1}+z)^{N_t-1-q}}dz \\ &= \sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\sum_{l=0}^{k-1}\sum_{q=0}^{\zeta}\frac{\binom{N_t-1}{n}\binom{k-1}{l}\binom{\zeta}{q}\lambda_E^{m-1}\Lambda^{2+q-N_t-m-l}}{(m-1)!} \times(-1)^{\zeta+q}\ell_1^{k-1-l}\ell_3^{l}\Omega(q). \end{aligned} \quad (50)$$

Similarly, Δ_4 can be derived as

$$\Delta_4 = \sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\sum_{l=0}^{k}\sum_{q=0}^{\zeta}\frac{\binom{N_t-1}{n}\binom{k}{l}\binom{\zeta}{q}\lambda_E^{m-1}\Lambda^{2+q-N_t-m-l}}{(m-1)!} \times(-1)^{\zeta+q}\ell_1^{k-l}\ell_3^{l}\Omega(q). \quad (51)$$

Substituting (46) into (44), we obtain $\mathcal{Q}_1$. Substituting (50) and (51) into (48), we obtain $\mathcal{Q}_2$. By substituting the obtained $\mathcal{Q}_1$ and $\mathcal{Q}_2$ into (43), and combining with (41), the closed-form expression for the average SOP of the SFPA scheme P_{out}^{s} under $\bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t-1}$ can be finally approximated as (52), as shown at the bottom of the page.

On the other hand, when $\bar{\Gamma}_B \leq \frac{\varepsilon-1}{N_t}$ holds, by substituting (12) and (20) into (10), the SOP of the SFPA scheme can be simplified as

$$\begin{aligned}P_{out}^{s} &= \Pr\left(\frac{1+\bar{\gamma}_B X}{1+\bar{\gamma}_E U} < \varepsilon \middle| X > \mu\right) \\ &= \Pr\left(X < \frac{\bar{\gamma}_E\varepsilon U+\varepsilon-1}{\bar{\gamma}_B}\middle| X>\mu\right) \\ &= \frac{\overbrace{\Pr(\mu < X < \ell_3 U+\ell_4)}^{\Xi_4}}{\Pr(X>\mu)}, \end{aligned} \quad (53)$$

where $\ell_4 = \frac{\varepsilon-1}{\bar{\gamma}_B}$ and $U = \|\boldsymbol{g}\|^2$. Since the positive random variable U follows a Gamma distribution with the parameters N_e and $\frac{1}{\lambda_E}$, similar to (24), the PDF of U can be explicitly expressed as

$$f_U(u) = \frac{\lambda_E^{N_e}}{\Gamma(N_e)}u^{N_e-1}\exp\big(-\lambda_E u\big). \quad (54)$$

Substituting (25) and (54) into Ξ_4, we have

$$\begin{aligned}\Xi_4 &= \int_{\eta}^{\infty}\int_{\mu}^{\ell_3 u+\ell_4} f_X(x)dx f_U(u)du \\ &= \sum_{k=0}^{N_t-1}\sum_{l=0}^{N_e-1}\frac{\lambda_E^{l}\lambda_B^{k}\mu^k\eta^l}{k!l!}\exp\left(-(\lambda_E\eta+\lambda_B\mu)\right) -\frac{\lambda_E^{N_e}\exp\left(-\lambda_B\ell_4\right)}{\Gamma(N_e)}\sum_{k=0}^{N_t-1}\sum_{m=0}^{k}\frac{\lambda_B^k}{k!}\binom{k}{m}\ell_4^{k-m} \times\ell_3^{m}\underbrace{\int_{\eta}^{\infty}u^{N_e-1+m}\exp\left(-(\lambda_B\ell_3+\lambda_E)u\right)du}_{\Xi_5}, \end{aligned} \quad (55)$$

where $\eta = \frac{\mu-\ell_4}{\ell_3}$. Resorting to [37, eq. (3.351.2)], the SOP of the SFPA scheme P_{out}^{s} under $\bar{\Gamma}_B \leq \frac{\varepsilon-1}{N_t-1}$ can be finally derived as

$$P_{out}^{s} = \frac{\Gamma(N_t)}{\Gamma(N_t,\lambda S\mu)}\Bigg(\sum_{k=0}^{N_t-1}\sum_{l=0}^{N_e-1}\exp\left(-(\lambda_E\eta+\lambda_B\mu)\right) \times\frac{\lambda_E^{l}\lambda_B^{k}\mu^k\eta^l}{k!l!} - \frac{\lambda_E^{N_e}\exp\left(-\lambda_B\ell_4\right)}{\Gamma(N_e)}\sum_{k=0}^{N_t-1}\sum_{m=0}^{k}\frac{\lambda_B^k}{k!}\binom{k}{m}$$

$$P_{out}^{s} \approx \frac{\Gamma(N_t)}{\Gamma(N_t,\lambda_B\mu)}\Bigg(\sum_{k=0}^{N_t-1}\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\frac{\lambda_B^k\mu^k\exp(-\lambda_B\mu)\binom{N_t-1}{n}\lambda_E^{m-1}}{k!(m-1)!}\frac{\Lambda^n\xi^{m+n-1}\exp(-\lambda_E\xi)}{(1+\Lambda\xi)^{N_t-1}} - \exp(-\lambda_B\ell_1) \times\Bigg(R_{\tilde{Z}}(\xi)\exp(-\lambda_B\ell_3\xi) - \lambda_B\ell_3\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\sum_{q=0}^{\kappa}\frac{(-1)^{\kappa+q}\binom{N_t-1}{n}\binom{\kappa}{q}\lambda_E^{m-1}\Lambda^{2+q-m-N_t}}{(m-1)!}\Omega(q)\Bigg) - \sum_{k=1}^{N_t-1}\frac{\lambda_B^k\exp(-\lambda_B\ell_1)}{k!}\Bigg(R_{\tilde{Z}}(\xi)\exp(-\lambda_B\ell_3\xi)(\ell_1+\ell_3\xi)^k + k\ell_3\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\sum_{l=0}^{k-1}\sum_{q=0}^{\zeta}\frac{\binom{N_t-1}{n}\binom{k-1}{l}\binom{\zeta}{q}\lambda_E^{m-1}\Lambda^{2+q-N_t-m-l}}{(m-1)!} -\lambda_B\ell_3\sum_{m=1}^{N_e}\sum_{n=0}^{N_e-m}\sum_{l=0}^{k}\sum_{q=0}^{\zeta}\frac{\binom{N_t-1}{n}\binom{k}{l}\binom{\zeta}{q}\lambda_E^{m-1}\Lambda^{2+q-N_t-m-l}}{(m-1)!}(-1)^{\zeta+q}\ell_1^{k-l}\ell_3^{l}\Omega(q)\Bigg)\Bigg). \quad (52)$$

$$\times \frac{\ell_3^m \ell_4^{k-m}}{\eta^{N_e+m}} \Gamma\big(N_e+m, (N_e+m-1)(\lambda_B \ell_3 + \lambda_E)\big)\Bigg). \tag{56}$$

2) Secrecy Outage Performance in Worst-Case Scenario: In the worst-case scenario and under $\bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t}$, by substituting (2), (3) and (20) into (10), the SOP of the SFPA scheme is derived as

$$\begin{aligned} P_{out}^{s,w} &= \Pr\left(\frac{1+\widetilde{\phi}\bar{\gamma}_B X}{1+\frac{\widetilde{\phi}(N_t-1)}{(1-\phi)}Y} < \varepsilon \,|X > \mu\right) \\ &= \Pr\left(X < \ell_1 + \ell_2 Y \,|X > \mu\right), \end{aligned} \tag{57}$$

where $\ell_2 = \frac{\varepsilon(N_t-1)}{\bar{\gamma}_B(1-\widetilde{\phi})}$. According to the total probability formula and recalling (33), $P_{out}^{s,w}$ is further derived as

$$\begin{aligned} P_{out}^{s,w} &= \frac{\Pr\left(\mu < X < \ell_1 + \ell_2 Y\right)}{\Pr(X > \mu)} \\ &= \frac{\Gamma(N_t)}{\Gamma(N_t, \lambda_B \mu)} \underbrace{\int_{\varphi}^{\infty} \int_{\mu}^{\ell_1+\ell_2 y} f_X(x) dx f_Y(y) dy}_{\Xi_2}. \end{aligned} \tag{58}$$

Substituting (24) and (25) into Ξ_2, we have

$$\begin{aligned} \Xi_2 = &\sum_{k=0}^{N_t-1} \sum_{m=0}^{N_e-1} \frac{\lambda_B^k \mu^k \exp(-\mu)}{k!} \frac{\binom{N_t-1}{m} \varphi^m}{(1+\varphi)^{N_t-1}} \\ &- \sum_{k=0}^{N_t-1} \frac{\lambda_B^k \exp(-\lambda_B \ell_1)}{k!} \\ &\times \underbrace{\int_{\varphi}^{\infty} (\ell_1 + \ell_2 y)^k \exp(-\lambda_B \ell_2 y) f_Y(y) dy}_{\mathcal{O}}. \end{aligned} \tag{59}$$

Substituting (74) of Appendix B into $\mathcal{O}$, we have

$$\begin{aligned} \mathcal{O} = &\sum_{p=0}^{k} \binom{k}{p} \ell_1^{k-p} \ell_2^p \Bigg(\sum_{m=0}^{N_e-1} \binom{N_t-1}{m} (N_t-1) \\ &\times \underbrace{\int_{\varphi}^{\infty} \frac{y^{m+p} \exp(-\lambda_B \ell_2 y)}{(1+y)^{N_t}} dy}_{\Delta_1} - \sum_{m=1}^{N_e-1} \binom{N_t-1}{m} m \\ &\times \underbrace{\int_{\varphi}^{\infty} \frac{y^{m+p-1} \exp(-\lambda_B \ell_2 y)}{(1+y)^{N_t-1}} dy}_{\Delta_2} \Bigg). \end{aligned} \tag{60}$$

Applying the binomial series expansion to Δ_1 and using [37], we arrive at

$$\begin{aligned} \Delta_1 &= \sum_{q=0}^{m+p} \binom{m+p}{q} (-1)^{m+p+q} \int_{\varphi}^{\infty} \frac{\exp(-\lambda_B \ell_2 y)}{(1+y)^{N_t-q}} dy \\ &= \sum_{q=0}^{m+p} \binom{m+p}{q} (-1)^{m+p+q} \exp(\lambda_B \ell_2) (\lambda_B \ell_2)^{-1-q+N_t} \\ &\quad \times \Gamma(1+q-N_t, \lambda_B \ell_2 (1+\varphi)). \end{aligned} \tag{61}$$

Similarly, Δ_2 can be derived as

$$\begin{aligned} \Delta_2 &= \sum_{q=0}^{v} \binom{v}{q} (-1)^{v+q} \int_{\varphi}^{\infty} \frac{\exp(-\lambda_B \ell_2 y)}{(1+y)^{N_t-q-1}} dy \\ &= \sum_{q=0}^{v} \binom{v}{q} (-1)^{v+q} (\lambda_B \ell_2)^{-2-q+N_t} \\ &\quad \times \exp(\lambda_B \ell_2) \Gamma(2+q-N_t, \lambda_B \ell_2 (1+\varphi)). \end{aligned} \tag{62}$$

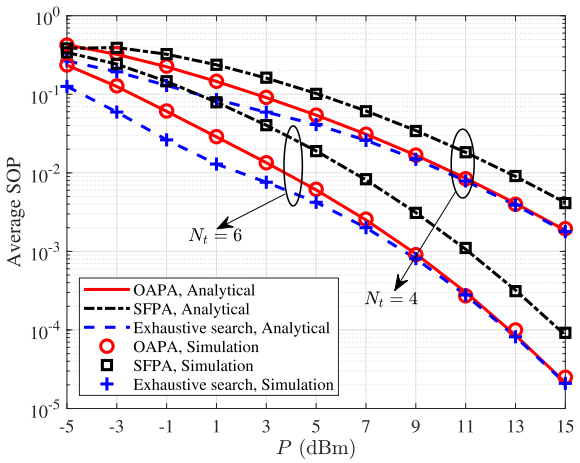


Fig. 1. Average SOP versus P for three schemes with $\sigma_E^2 = 5$ dBm, $N_e = 2$ and two different N_t values.

By combining (59), (60), (61) and (62), the SOP of the SFPA scheme in the worst-case scenario $P_{out}^{s,w}$ under the condition $\bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t-1}$ can be finally approximated as (63), as shown at the bottom of the next page.

When $\bar{\Gamma}_B < \frac{\varepsilon-1}{N_t}$, $\phi_{\infty}^{\star} = 1$, and the average SOP of the SFPA scheme in the worst-case scenario is always one.

V. Numerical Results

In this section, we present numerical results for validating the derived expressions for the secrecy outage performance analysis for our two proposed schemes. Without loss of generality, we set the channel parameters as $\lambda_B = \lambda_E = 1$, the average receive noise power at Bob is $\sigma_B^2 = 0$ dBm, the threshold secrecy rate is $R_S = 1$ bits/s/Hz. We also compare the performance of the proposed schemes with the exhaustive search method based fixed power allocation scheme developed in [25] as the benchmark, which is simply denoted as the exhaustive search. This exhaustive search based scheme provides a lower bound for the OAPA scheme, in terms of ISOP, and for the SFPA scheme, in terms of average SOP, but it relies on Eve's prior information.

A. Secrecy Outage Performance Under a Preset σ_E Value

Fig. 1 plots the average SOP performance as the functions of the total transmit power P for three different power allocation schemes with $N_e = 2$, the noise power level at Eve $\sigma_E^2 = 5$ dBm, and two different values of N_t. Fig. 1 confirm that the analytical results match closely with the simulation results, which validates the accuracy of our derivations. As expected, the exhaustive search scheme outperforms the OAPA and SFPA, because it requires Eve's prior information, including Eve's statistical information λ_E, the noise power level σ_E^2 and the number of antennas at Eve N_e. Also, as expected, the average SOP becomes smaller as N_t or P increases, which confirms the fact that either adding more antennas or increasing total transmit power improves security performance.

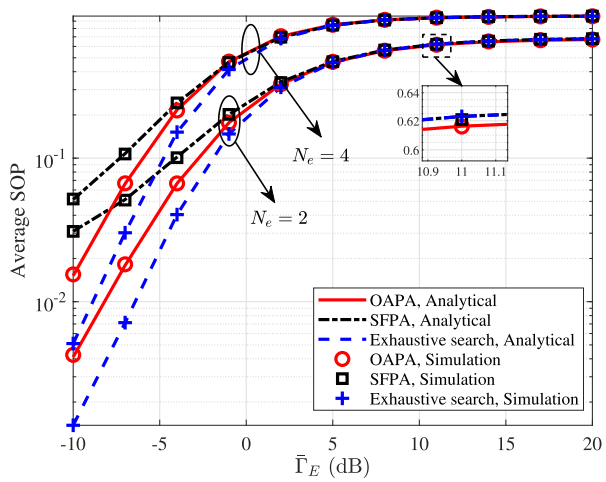


Fig. 2. Average SOP versus $\bar{\Gamma}_E$ for three schemes with $N_t = 6$, $P = 1$ dBm and two different N_e values.

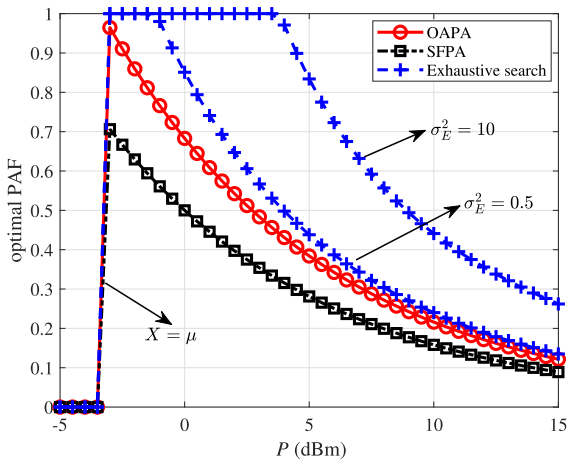


Fig. 3. Optimal PAF versus P for three schemes with $N_t = 4$, $N_e = 2$ and two different values of σ_E^2.

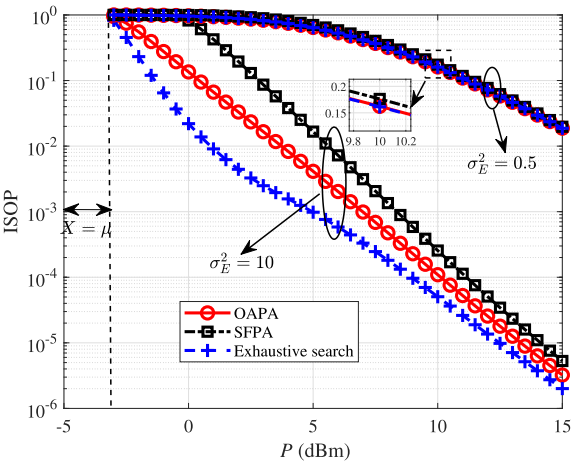


Fig. 4. ISOP versus P for three schemes with $N_t = 4$, $N_e = 2$ and two different values of σ_E^2.

Observe that for sufficiently large P, the performance of our OAPA approaches that of the exhaustive search.

In Fig. 2, we illustrate the average SOP performance versus the maximum achievable average SNR at Eve $\bar{\Gamma}_E$, given $N_t = 6$, $P = 1$ dBm and two different N_e values. It can be seen that the average SOP increases as $\bar{\Gamma}_E$ increases, and it reaches the ceiling value when $\bar{\Gamma}_E > 10$ dB. It can also be observed that the performance gaps between the different schemes become negligible when $\bar{\Gamma}_E \geq 2$ dB. Moreover, it is worth pointing out that the average SOP of our OAPA scheme is actually slightly lower than that of the exhaustive search when $\bar{\Gamma}_E$ is sufficiently large. This confirms our analysis that the OAPA scheme guarantees its optimality in the worst-case scenario even though it requires no Eve's prior information.

Fig. 3 depicts the optimal PAFs as the functions of P for the three schemes, given $N_t = 4$, $N_e = 2$ and two different values of Eve's channel noise variance σ_E^2, under $\boldsymbol{h} = [1.0887 - \text{j}0.1005\ -0.0187 - \text{j}0.2694\ 0.1665 + \text{j}0.2963\ 0.4973 + \text{j}0.7164]$. As discussed previously, Alice only transmits when the condition $X < \mu$ is satisfied; otherwise, it remains silent. Observe that at the beginning when P is very small, the optimal PAF is equal to one for the exhaustive search or is nearly one for the other schemes. The reason is that the current transmit power P is insufficiently large to support the target R_S, so that the full or almost full power is allocated to the information signal to guarantee a reliable link to Bob. As P increases further, the optimal PAF reduces, which indicates that a larger fraction of power is shifted to AN in order to confuse Eve. Evidently, the optimal PAFs for the OAPA and SFPA schemes are independent of Eve's prior information σ_E^2. The optimal PAF for the exhaustive search increases with σ_E^2, which indicates that a large fraction of power is allocated to the information signal when Eve's SNR is relatively low. Under the identical conditions, the corresponding ISOPs versus P are plotted in Fig. 4. It is seen that the exhaustive search achieves the best performance gain in terms of ISOP. It can also be seen that the performance gap between the exhaustive search and the OAPA is indistinguishable when σ_E^2 is sufficiently small.

Under the same channel settings, we plot the optimal PAF versus $\bar{\gamma}_E$ with two different values of R_S in Fig. 5. It is seen that the difference in the optimal PAF between the OAPA and

$$P_{out}^{s,w} \approx \frac{\Gamma(N_t)}{\Gamma(N_t, \lambda_B \mu)} \Bigg(\sum_{k=0}^{N_t-1} \sum_{m=0}^{N_e-1} \frac{\lambda_B^k \mu^k \exp(-\lambda_B \mu)}{k!} \frac{\binom{N_t-1}{m} \varphi^m}{(1+\varphi)^{N_t-1}} - \sum_{k=0}^{N_t-1} \frac{\lambda_B^k}{k!} \sum_{p=0}^{k} \binom{k}{p} \ell_1^{k-p} \ell_2^p \exp(-\lambda_B \ell_1)$$
$$\times \Bigg(\sum_{m=0}^{N_e-1} \binom{N_t-1}{m} (N_t-1) \sum_{q=0}^{m+p} \binom{m+p}{q} (-1)^{m+p+q} \exp(\lambda_B \ell_2) (\lambda_B \ell_2)^{-1-q+N_t} \Gamma\big(1+q-N_t, \lambda_B \ell_2 (1+\varphi)\big)$$
$$- \sum_{m=1}^{N_e-1} \binom{N_t-1}{m} m \sum_{q=0}^{v} \binom{v}{q} (-1)^{v+q} (\lambda_B \ell_2)^{-2-q+N_t} \exp(\lambda_B \ell_2) \Gamma\big(2+q-N_t, \lambda_B \ell_2 (1+\varphi)\big) \Bigg) \Bigg). \quad (63)$$

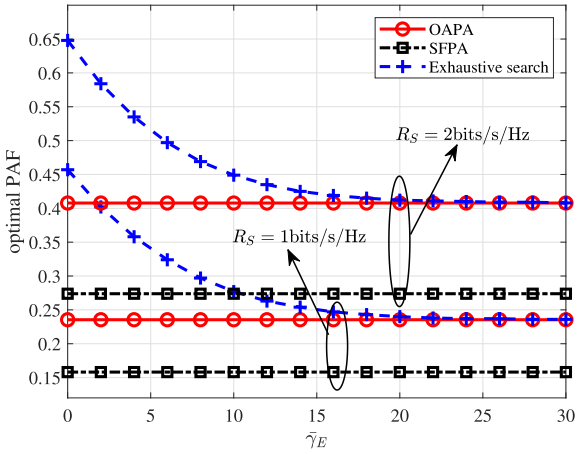


Fig. 5. Optimal PAF versus $\bar{\gamma}_E$ for three schemes with $N_t = 4$, $N_e = 2$, $P = 10$ dB and two different values of R_S.

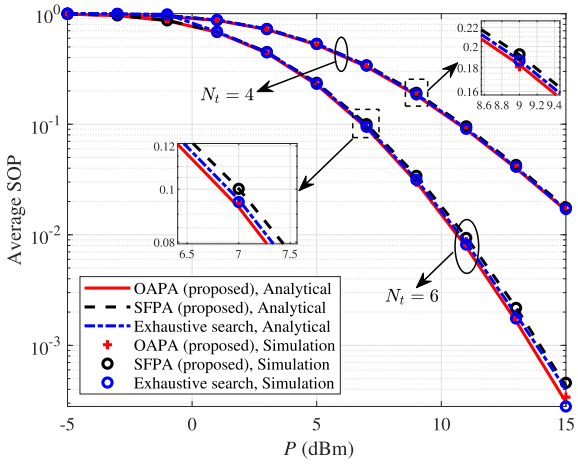


Fig. 6. Average SOP versus P for three schemes with $N_e = 2$ and two different values of N_t.

the exhaustive search becomes small as $\bar{\gamma}_E$ increases, and for sufficiently large $\bar{\gamma}_E$, the two schemes become indistinguishable. Since the exhaustive search method provides a lower bound for the OAPA scheme, in terms of ISOP, it can be seen that the OAPA scheme also guarantees the optimality, in terms of ISOP, in the worst-case scenario. Moreover, unlike the exhaustive search, our OAPA does not require Eve's prior information. It is also seen that the optimal PAF increases as R_S increases, and the reason is that more power is allocated to the information signal to support a larger R_S. This confirms our **Remarks 2** and **3**.

B. Secrecy Outage Performance in Worst-Case Scenario

Fig. 6 depicts the average SOP performance as the functions of P for the three schemes given $N_e = 2$ and two values of N_t. From Fig. 6, it can be seen that the analytical results closely match the simulation results. Observe that our OAPA scheme outperforms the exhaustive search, even though it does not require Eve's prior information. Recalling (15) and (16), we can confirm that the optimal PAF of our OAPA scheme $(\phi^\star)$ satisfies $\omega(\phi^\star) \geq \omega(\alpha^\star)$, where $\alpha^\star$ is the optimal PAF for the exhaustive search, thereby leading to a smaller probability of secrecy outage event for the OAPA case. Observe also that there is only a very slight performance degradation for the proposed SFPA scheme compared with the exhaustive search.

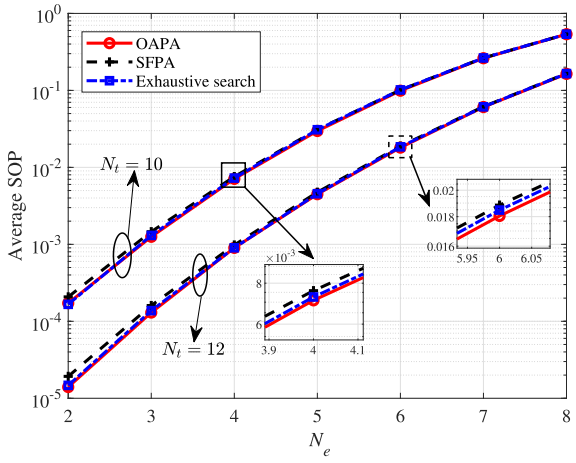


Fig. 7. Average SOP versus N_e for three schemes with $P = 10$ dBm and two different values of N_t.

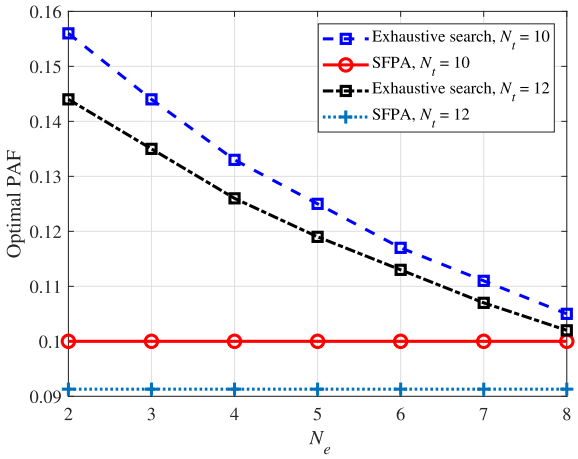


Fig. 8. Optimal PAF versus N_e for two schemes with $P = 10$ dBm and two different values of N_t.

It is worth recalling that the SFPA does not require Eve's prior information, whilst the exhaustive search needs Eve's prior information, including λ_E, N_e, and σ_e^2, for implementation. Therefore, our SFPA offers a simpler and better alternative to the exhaustive search in the worst-case scenario.

Fig. 7 shows the average SOP performance versus N_e for the three schemes given $P = 10$ dBm and two different values of N_t. Again it can be seen that our OAPA outperforms the exhaustive search. Furthermore, the performance of the SFPA is very close to that of the exhaustive search. Under the same system settings, the optimal PAFs for the exhaustive search and the SFPA are also depicted in Fig. 8. As expected, $\phi_\infty^\star$ is independent of N_e, but it can be seen that increasing N_e leads to a decrease in the value of the optimal PAF $\alpha^\star$ for the exhaustive search. The maximum difference between $\alpha^\star$ and $\phi_\infty^\star$ at $N_e = 2$ does not exceed 0.05. These observations suggest that our SFPA scheme can achieve near-optimal secrecy performance. It can be also seen that increasing N_t leads to a decrease in the value of $\phi_\infty^\star$.

VI. Conclusion

The power allocation between the information signal and the AN has been optimized for a MISO system in the presence of an unknown eavesdropper. Without requiring Eve's

prior information, the OAPA and SFPA schemes have been proposed, for which explicit solutions to the optimal PAF have been derived to minimize the SOP in the worst-case scenario. Given a preset noise power level at Eve, approximate closed-form expressions for the average SOP have been derived by applying the Gauss-Chebyshev quadrature. We have also addressed the worst-case secrecy outage performance for the proposed OAPA and SFPA schemes. Simulation results have been presented to corroborate the accuracy of our theoretical derivations. From the results, it has been shown that, even without Eve's prior information, the OAPA scheme is capable of achieving a comparable secrecy outage performance to that of the exhaustive search method. It has also been shown that the OAPA scheme achieves a slightly lower worst-case SOP than the exhaustive search method. Additionally, the SFPA scheme can achieve almost the same worst-case SOP as the OAPA scheme, while its implementation complexity is greatly reduced.

APPENDIX

A. Proof of **Proposition 1**

Proof: Using the variable substitution $t = \sqrt{\bar{\gamma}_B x} - \sqrt{\varepsilon - 1}$ in $H_1(x)$ of (28), where $t \in [0,\ \infty)$, we have

$$H_1(t) = \frac{t^{2n}}{\left(1 + \frac{t^2}{(N_t-1)\varepsilon}\right)^{N_t-1}}. \tag{64}$$

By calculating the derivation of $H_1(t)$ and setting it to zero, it can be seen that $H_1(t)$ has the unique maximum at the point $t^* = \sqrt{\frac{\varepsilon n(N_t-1)}{N_t-1-n}}$. Solving the following equation

$$\sqrt{\frac{\varepsilon n(N_t-1)}{N_t-1-n}} = \sqrt{\bar{\gamma}_B x^*} - \sqrt{\varepsilon - 1}, \tag{65}$$

yields

$$x^* = \frac{\left(\sqrt{\frac{\varepsilon n(N_t-1)}{N_t-1-n}} + \sqrt{\varepsilon - 1}\right)^2}{\bar{\gamma}_B}. \tag{66}$$

The derivation of $H_2(x)$ is given by

$$\frac{dH_2(x)}{dx} = \exp\left(-\lambda_B x\right) x^{N_t-2}\left(N_t - 1 - \lambda_B x\right), \tag{67}$$

where $x \in [\mu,\ \infty)$. Setting it to zero yields the unique maximum point $x^o = \frac{N_t-1}{\lambda_B}$ of $H_2(x)$.

By using the variable substitution $s = \sqrt{\bar{\gamma}_B x}\left(\sqrt{\bar{\gamma}_B x} - \sqrt{\varepsilon - 1}\right)$ in $H_3(x)$ of (30), where $s \in [0,\ \infty)$, we obtain $H_3(s)$, which has a similar form as $H_2(x)$. Using the result for $H_2(x)$, $H_3(s)$ has the unique maximum at $s^{\#} = \varepsilon\bar{\Gamma}_E(m-1)$. Solving the following equation

$$\sqrt{\bar{\gamma}_B x^{\#}}\left(\sqrt{\bar{\gamma}_B x^{\#}} - \sqrt{\varepsilon - 1}\right) = \varepsilon\bar{\Gamma}_E(m-1) \tag{68}$$

yields

$$x^{\#} = \frac{\varepsilon\left(1 + 2\bar{\Gamma}_E(m-1)\right) - 1}{2\bar{\gamma}_B} + \frac{\sqrt{\varepsilon - 1}\sqrt{\varepsilon - 1 + 4\varepsilon\bar{\Gamma}_E(m-1)}}{2\bar{\gamma}_B} \tag{69}$$

It is readily to see that $H_1(x)$, $H_2(x)$ and $H_3(x)$ are strictly decreasing for $x \in [x^*,\ \infty)$, $x \in [x^o,\ \infty)$ and $x \in [x^{\#},\ \infty)$, respectively. We conclude that $T(x) = H_1(x)H_2(x)H_3(x)$ is strictly decreasing for $x \in [A,\ \infty)$ with $A = \max\{x^*, x^o, x^{\#}\}$. This completes the proof. ■

B. Proof of **Theorem 1**

Proof: Substituting (2), (3), (13) and (17) into (10), and after some algebraic manipulations, the expression of the SOP for the OAPA scheme in the worst-case scenario is derived as

$$\begin{aligned} P_{out}^{o,w} &= \Pr\left(\frac{1 + \sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}\bar{\gamma}_B X}{1 + \frac{\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}(N_t-1)}{1-\sqrt{\frac{\varepsilon-1}{\bar{\gamma}_B X}}}Y} < \varepsilon \,\middle|\, X \geq \mu\right) \\ &= \Pr\left(X < \frac{\left(\sqrt{\varepsilon-1} + \sqrt{Y\varepsilon(N_t-1)}\right)^2}{\bar{\gamma}_B} \,\middle|\, X \geq \mu\right), \end{aligned} \tag{70}$$

where $Y = \widetilde{\boldsymbol{g}}^{\mathrm{H}}\left(\widetilde{\boldsymbol{G}}\widetilde{\boldsymbol{G}}^{\mathrm{H}}\right)^{-1}\widetilde{\boldsymbol{g}}$. According to the total probability formula, $P_{out}^{o,w}$ is further derived as

$$\begin{aligned} P_{out}^{o,w} &= \frac{\Pr\left(\mu < X < \frac{\left(\sqrt{\varepsilon-1}+\sqrt{Y\varepsilon(N_t-1)}\right)^2}{\bar{\gamma}_B}\right)}{\Pr(X > \mu)} \\ &= \frac{\overbrace{\int_{\tau(\mu)}^{\infty}\int_{\mu}^{\left(\sqrt{\varepsilon-1}+\sqrt{y\varepsilon(N_t-1)}\right)^2/\bar{\gamma}_B} f_X(x)dx f_Y(y)dy}^{\Xi_1}}{\Pr(X > \mu)}. \end{aligned} \tag{71}$$

With the aid of (24) and (25), Ξ_1 can be derived as

$$\begin{aligned} \Xi_1 = &\int_{\tau(\mu)}^{\infty}\sum_{k=0}^{N_t-1}\frac{\lambda_B^k\mu^k}{k!}\exp\left(-\lambda_B\mu\right) f_Y(y)dy \\ &- \int_{\tau(\mu)}^{\infty}\sum_{k=0}^{N_t-1}\frac{\left(A(B + C\sqrt{y})^2\right)^k}{k!} \\ &\times \exp\left(-A\left(B + C\sqrt{y}\right)^2\right) f_Y(y)dy. \end{aligned} \tag{72}$$

The CDF and PDF of Y can respectively be obtained as [35, eq. 11]

$$F_Y(y) = 1 - \sum_{m=0}^{N_e-1}\frac{\binom{N_t-1}{m}y^m}{(1+y)^{N_t-1}}, \tag{73}$$

$$f_Y(y) = \sum_{m=0}^{N_e-1}\frac{\binom{N_t-1}{m}(N_t-1)y^m}{(1+y)^{N_t}} - \sum_{m=1}^{N_e-1}\frac{\binom{N_t-1}{m}my^{m-1}}{(1+y)^{N_t-1}}. \tag{74}$$

Substituting the CDF of Y (73) into (72), Ξ_1 can be further derived as

$$\Xi_1 = \sum_{k=0}^{N_t-1}\sum_{m=0}^{N_e-1}\frac{(\lambda_B)^k\mu^k\exp\left(-\lambda_B\mu\right)}{k!}\frac{\binom{N_t-1}{m}\tau^m(\mu)}{(1+\tau(\mu))^{N_t-1}}$$

$$-\sum_{k=0}^{N_t-1}\frac{A^k}{k!}\underbrace{\int_{\tau(\mu)}^{\infty}\left(B+C\sqrt{y}\right)^{2k}\exp\left(-A\left(B+C\sqrt{y}\right)^2\right)f_Y(y)dy}_{\Xi_2}. \tag{75}$$

Substituting the PDF of Y (74) into the integral Ξ_2 in (75), we have

$$\begin{aligned}\Xi_2 =& \sum_{m=0}^{N_e-1}\sum_{n=0}^{2k}\binom{N_t-1}{m}\binom{2k}{n}(N_t-1)B^{2k-n}C^n\\ &\times\underbrace{\int_{\tau(\mu)}^{\infty}y^{m+\frac{n}{2}}(1+y)^{-N_t}\exp\left(-A\left(B+C\sqrt{y}\right)^2\right)dy}_{\mathcal{L}_1}\\ &-\sum_{m=1}^{N_e-1}\sum_{n=0}^{2k}\binom{N_t-1}{m}\binom{2k}{n}mB^{2k-n}C^n\\ &\times\underbrace{\int_{\tau(\mu)}^{\infty}y^{m+\frac{n}{2}-1}(1+y)^{1-N_t}\exp\left(-A\left(B+C\sqrt{y}\right)^2\right)dy}_{\mathcal{L}_2}.\end{aligned} \tag{76}$$

We now proceed to derive $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively.

Utilizing the variable substitution $t=\sqrt{y}$, $\mathcal{L}_1$ can be expressed as

$$\mathcal{L}_1=2\int_{\sqrt{\tau(\mu)}}^{\infty}t^{2m+n+1}(1+t^2)^{-N_t}\exp\left(-A(B+Ct)^2\right)dt. \tag{77}$$

Although the expression (77) is intractable to solve directly, we can derive an approximate expression with an arbitrarily small error by invoking the truncation method.

Referring to **Proposition 1**, it is readily to see that the integral term $M_1(t)=t^{2m+n+1}(1+t^2)^{-N_t}$ in (77) is strictly decreasing within $\left[\sqrt{\frac{2m+n+1}{2N_t-2m-n-1}},\ \infty\right)$, and $M_2(t)=\exp\left(-A(B+Ct)^2\right)$ is strictly decreasing within $[0,\ \infty)$. Therefore, $M_1(t)M_2(t)$ is strictly decreasing within $\left[\sqrt{\frac{2m+n+1}{2N_t-2m-n-1}},\ \infty\right)$. Consequently, there exists a sufficiently large $\Phi_2>\max\left\{\sqrt{\frac{2m+n+1}{2N_t-2m-n-1}},\ \sqrt{\tau(\mu)}\right\}$ that makes the approximate error $\int_{\Phi_2}^{\infty}T(x)dx\approx 0$, and $\mathcal{L}_1$ can be approximated as

$$\mathcal{L}_1\approx 2\int_{\sqrt{\tau(\mu)}}^{\Phi_2}t^{2m+n+1}\left(1+t^2\right)^{-N_t}\exp\left(-A(B+Ct)^2\right)dt. \tag{78}$$

Since it is still challenging to obtain the closed-from expressions for $\mathcal{L}_1$, we use Gaussian-Chebyshev quadrature [36] to further find an approximation of (78) as follows:

$$\begin{aligned}\mathcal{L}_1\approx\frac{\pi\left(\Phi_2-\sqrt{\tau(\mu)}\right)}{T}&\sum_{k=1}^{T}\sqrt{1-v_t^2}s_t^{2m+n+1}(1+s_t^2)^{-N_t}\\ &\times\exp\left(-A(B+Cs_t)^2\right).\end{aligned} \tag{79}$$

Following a similar way, we can truncate the infinite integral $\mathcal{L}_2$ w.r.t. $\Phi_3>\max\left\{\sqrt{\frac{2m+n-1}{2N_t-2m-n-1}},\sqrt{\tau(\mu)}\right\}$ to approximate it as

$$\begin{aligned}\mathcal{L}_2 &= 2\int_{\sqrt{\tau(\mu)}}^{\infty}t^{2m+n-1}(1+t^2)^{1-N_t}\exp\left(-A(B+Cs_k)^2\right)dt\\ &\approx 2\int_{\sqrt{\tau(\mu)}}^{\Phi_3}t^{2m+n-1}(1+t^2)^{1-N_t}\exp\left(-A(B+Cs_k)^2\right)dt\\ &\approx\frac{\pi\left(\Phi_3-\sqrt{\tau(\mu)}\right)}{G}\sum_{g=1}^{G}\sqrt{1-v_g^2}s_g^{2m+n-1}\left(1+s_g^2\right)^{1-N_t}\\ &\quad\times\exp\left(-A(B+Cs_g)^2\right).\end{aligned} \tag{80}$$

Substituting (75), (76), (79) and (80) into (71), we obtain the approximate closed-form expression of the SOP for the OAPA scheme in the worst-case scenario as given in (38). This completes the proof. ■

REFERENCES

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

[2] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[6] J. Zhu, Y. Li, N. Wang, and W. Xu, "Wireless information and power transfer in secure massive MIMO downlink with phase noise," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 298–301, Jun. 2017.

[7] D. He, C. Liu, T. Q. S. Quek, and H. Wang, "Transmit antenna selection in MIMO wiretap channels: A machine learning approach," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 634–637, Aug. 2018.

[8] F. Renna, M. R. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 620–627, Feb. 2013.

[9] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[10] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[11] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[12] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2017.

[13] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

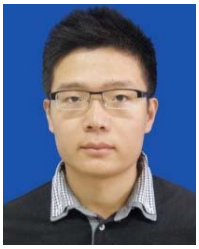
[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[15] J. Xiong, D. Ma, K. K. Wong, and J. Wei, "Robust masked beamforming for MISO cognitive radio networks with unknown eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 744–755, Feb. 2016.

[16] O. Taghizadeh, P. Neuhaus, R. Mathar, and G. Fettweis, "Secrecy energy efficiency of MIMOME wiretap channels with full-duplex jamming," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5588–5603, Aug. 2019.

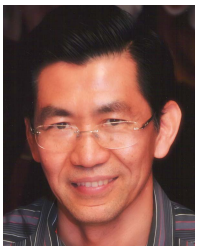
[17] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[18] 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.
[19] R. Sohrabi, Q. Zhu, and Y. Hua, "Secrecy analyses of a full-duplex MIMOME network," *IEEE Trans. Signal Process.*, vol. 67, no. 23, pp. 5968–5982, Dec. 2019.
[20] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, Jr., "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.
[21] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.
[22] H. Wang *et al.*, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300–1304, 2020.
[23] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.
[24] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[25] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1875–1889, Aug. 2018.
[26] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
[27] D. Hu, P. Mu, W. Zhang, and W. Wang, "Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 401–404, Feb. 2020.
[28] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.
[29] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
[30] S. Jia, D. Zhang, S. Mumtaz, and J. J. P. C. Rodrigues, "Power allocation and outage analysis for secure MISO networks with an unknown eavesdropper," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Taiwan, Dec. 2020, pp. 1–6.
[31] 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.
[32] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[33] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[34] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[35] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.
[36] F. B. Hildebrand, *Introduction to Numerical Analysis*. New York, NY, USA: Dover, 1987.
[37] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.



Shaobo Jia (Member, IEEE) received the B.S. and M.S. degrees from the School of Underwater Acoustic Engineering, Harbin Engineering University, China, in 2011 and 2014, respectively, and the Ph.D. degree from the Communication Research Centre, Harbin Institute of Technology, China, in 2019. He is currently a Lecturer with the School of Information Engineering, Zhengzhou University, China. His research interests include physical layer security, cognitive radio networks, ambient backscatter communications, and IRS communications.

Jiankang Zhang (Senior Member, IEEE) is currently a Senior Lecturer with Bournemouth University. Prior to joining at Bournemouth University, he was a Senior Research Fellow at the University of Southampton, U.K. He was a Lecturer from 2012 to 2013 and then an Associate Professor from 2013 to 2014 at Zhengzhou University. His research interests are in the areas of aeronautical communications and networks, evolutionary algorithms, machine learning algorithms, and edge computing. He serves as an Associate Editor for IEEE ACCESS.



Sheng Chen (Fellow, IEEE) received the B.Eng. degree in control engineering from the East China Petroleum Institute, Dongying, China, in 1982, the Ph.D. degree in control engineering from City, University of London, in 1986, and the Doctor of Sciences (D.Sc.) degree from the University of Southampton, Southampton, U.K., in 2005. From 1986 to 1999, he held research and academic appointments at The University of Sheffield, Edinburgh and Portsmouth, U.K. Since 1999, he has been with the School of Electronics and Computer Science, University of Southampton, where he is currently a Professor in intelligent systems and signal processing. He was one of the original ISI highly cited researchers in engineering in March 2004. He has published over 650 research articles. He has more than 17 700 Web of Science citations with H-index 58 and more than 34 900 Google Scholar citations with H-index 80. His research interests include adaptive signal processing, wireless communications, modeling and identification of nonlinear systems, neural network and machine learning, intelligent control system design, and evolutionary computation methods and optimization. He is a fellow of the United Kingdom Royal Academy of Engineering, a fellow of Asia–Pacific Artificial Intelligence Association, and a fellow of IET.

Wanming Hao (Member, IEEE) received the Ph.D. degree from the School of Electrical and Electronic Engineering, Kyushu University, Japan, in 2018. He has worked as a Research Fellow at the 5G Innovation Center, Institute of Communication Systems, University of Surrey, U.K. He is currently an Associate Professor with the School of Information Engineering, Zhengzhou University, China. His research interests include THz, IRS communications, and SWIPT.

Wei Xu (Senior Member, IEEE) received the B.Sc. degree in electrical engineering and the M.S. and Ph.D. degrees in communication and information engineering from Southeast University, Nanjing, China, in 2003, 2006, and 2009, respectively. From 2009 to 2010, he was a Post-Doctoral Research Fellow at the Department of Electrical and Computer Engineering, University of Victoria, Canada. He was an Adjunct Professor at the University of Victoria from 2017 to 2020 and a Distinguished Visiting Fellow at the Royal Academy of Engineering, U.K., in 2019. He is currently a Professor with the National Mobile Communications Research Laboratory, Southeast University. He has coauthored over 100 refereed journal articles in addition to 36 domestic patents and four U.S. patents granted. His research interests include information theory, signal processing, and machine learning for wireless communications. He is a fellow of IET. He has received the Best Paper Awards from a number of prestigious IEEE conferences, including IEEE GLOBECOM/ICCC. He has received the Youth Science and Technology Award of China Institute of Communications in 2018. He was an Editor of IEEE COMMUNICATIONS LETTERS from 2012 to 2017. He is an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and a Senior Editor of IEEE COMMUNICATIONS LETTERS.