IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 18, 2018, accepted June 20, 2018, date of publication July 2, 2018, date of current version August 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2851598

Artificial Noise Aided Precoding With Imperfect CSI in Full-Duplex Relaying Secure Communications

YUANJIAN LI[1], RUI ZHAO[1], (Member, IEEE), YI WANG[2,3], GAOFENG PAN[4,5], (Member, IEEE), AND CHUNGUO LI[6], (Senior Member, IEEE)

[1]Xiamen Key Laboratory of Mobile Multimedia Communications, College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China
[2]School of Electronics and Communication Engineering, Zhengzhou University of Aeronautics, Zhengzhou 450046, China
[3]China National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China
[4]Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China
[5]School of Computing and Communications, Lancaster University, Lancaster LA1 4YW, U.K.
[6]School of Information Science and Engineering, Southeast University, Nanjing 210096, China

Corresponding author: Rui Zhao (rzhao@hqu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61401165 and Grant 61671144, in part by the Promotion Program for Young and Middle-Aged Teacher in Science and Technology Research of Huaqiao University under Grant ZQN-PY407, in part by the Project funded by China Postdoctoral Science Foundation under Grant 2018M633733, and in part by the Scientific and Technological Key Project of Henan Province under Grant 182102210449.

ABSTRACT In Rayleigh fading channels, to enhance the secrecy performance of wireless communication systems and efficiently disturb the interception of eavesdroppers, the multiple-antenna source node utilizes the artificial noise aided precoding (ANP) strategy with imperfect channel state information to emit the confidential information and the artificial noise simultaneously. Besides, the two-antenna decode-and-forward relay node applies the full-duplex (FD) relaying protocol, and the destination node which contains multiple antennas adopts the maximum ratio combining technique. Taking into account the existence of self-interference at the relay, the closed-form expression of approximate ergodic achievable secrecy rate (EASR) for any value of antenna number and that of exact EASR in the case of large-scale antenna array are derived, respectively. To extract more distinct insights from the considered system and hence obtain some simple and meaningful conclusions, the asymptotic performance analyses in two different asymptotic cases are studied. The numerical simulations validate the correctness of our theoretical derivation and analysis, which indicates that the ANP scheme combined with the FD relaying can achieve considerable secrecy performance.

INDEX TERMS Physical layer security, full-duplex relaying, artificial noise aided precoding, imperfect CSI, ergodic achievable secrecy rate.

I. INTRODUCTION

The broadcast characteristics of the radio frequency (RF) signal cause that the information emitted from the source can be easily intercepted by the eavesdropper. The eavesdropping problem is an essential challenge in wireless communication systems and therefore the secure transmission of information has become an important research topic. In the context of rapid development of modern processor, the traditional upper layer encryption coding scheme is getting increasingly unreliable. Physical layer security (PLS) which can improve the secrecy performance of wireless transmissions by directly exploiting the randomness provided by wireless fading channels has been considered as an outstanding approach to complement the conventional cryptography [1]–[9]. The concept of PLS was developed originally by Wyner for the Wyner wiretap channel in [10]. Recently, more and more practical and distinctive PLS problems have been studied, PLS technique has attracted enormous academic and industrial interest.

The full-duplex (FD) technique which can make wireless resources (time and frequency) be utilized more efficiently allows information reception and emission to be performed

simultaneously. Unfortunately, self-interference (SI) caused by the signal leakage from the transmit antenna to the receive antenna is the main factor limiting the performance of FD transmission systems [9], [11]. The SI seriously decays the received signal-to-interference-and-noise ratio (SINR) at the FD node, which in turn damages the overall performance of wireless transmissions [12]. Thanks to the rapidly development of the latest hardware design and self-interference cancellation (SIC) technologies that are based on antenna isolation, analog elimination and digital elimination [13], the SI can be suppressed to noise level, which makes the advantages of FD technique be further released.

Cooperative jamming (CJ) approach can not only reduce the probability of being eavesdropped by sending the jamming signal, e.g., artificial noise (AN), but also maintain the fine reception of intended information, hence it can improve the secrecy performance efficiently [14], [15]. As a promising CJ scheme applied at the source, artificial noise aided precoding (ANP) method can beamform the AN to the null space of legitimate link to enhance the secrecy performance [16]–[20]. The ANP scheme can transmit the legitimate information and the AN at the same time utilizing the additional spatial degrees of freedom of antenna array. To avoid interfering the intended destination and reduce the eavesdropping channel capacity, the AN signal should be beamformed into the orthogonal space of legitimate channel. The effectiveness of ANP scheme is strongly related to the accuracy of channel state information (CSI) obtained by the source node. In practical wireless communication scenarios, CSI is normally obtained by the following techniques, pilot training, channel estimation and feedback [21], [22]. The errors of pilot training or channel estimation and the time delay of feedback inevitably result in CSI imperfection [23], [24]. The imperfect CSI would lead to a severe problem called AN leakage, namely, the AN signal is not aligned perfectly in the orthogonal space of legitimate channel and thus the intended destination node will be obstructed to some certain degrees [25]. With imperfect CSI, a robust beamforming scheme was proposed in multiple-input multiple-out (MIMO) system in [26]. The impact of channel quantized feedback on the performance of ANP scheme was discussed in [27] and [28]. Wang *et al.* in [29] studied training as well as feedback and proposed a joint optimization proposal.

In order to optimize the average secrecy rate performance of wireless communication systems applying the ANP scheme, the optimal power allocation (PA) solutions were researched in [30] and [31]. In many distinctive types of secure relaying communication systems, the secrecy performance of ANP scheme has been deeply investigated. In [32], with known or unknown eavesdropping CSI, the optimal beamforming and PA solutions were proposed respectively in decode-and-forward (DF) relaying wireless transmission systems. In amplify-and-forward (AF) relaying wireless communication systems, [33] studied asymptotic analyses of the ergodic secrecy capacity (ESC) and the secrecy outage probability (SOP). Considering about direct link between the source and the destination, the secrecy rate performance of AF relaying transmissions without any jamming strategies was investigated in [34]. However, to the best of the authors' knowledge, there is no prior work that providing the closed-form expression of ergodic achievable secrecy rate (EASR) or related asymptotic secrecy performance analysis for FD relaying wireless communication systems which apply the ANP scheme under the imperfect CSI condition.

This paper is an extension of our previous work [9] in which we analyzed the EASR performance of ANP scheme combined with FD relaying wireless transmissions under the assumption of perfect legitimate CSI obtained by the source. In this paper, we consider the more practical scenario that only the imperfect CSI can be aware by the source. Meanwhile, this practical consideration introduces a new system parameter, i.e., the correlation coefficient between the real channel and its estimation, which makes our proposed model much more complicated than our previous work. Most importantly, a novel asymptotic secrecy performance analysis is added into this extension, which makes our work more complete and provides several significative conclusions.

In this paper, we consider the secure transmission system with a FD relay, where a portable single-antenna eavesdropper can wiretap the confidential information from both the source and the relay, and the destination can only receive the signal from the relay for the reason of the long distance to the source. The multiple-antenna source utilizes the ANP scheme to transmit the intended information and the AN simultaneously. The two-antenna relay node works in the FD mode, which can enhance the utilization efficiency of wireless resources (time and frequency). The multiple-antenna destination node applies the maximum ratio combining (MRC) strategy to receive information in order to maximize the received SNR. The main contributions of this paper are concluded in the following.

- We take full account of a very practical communication scenario, in which imperfect legitimate channel CSI obtained by the source node and the existance of SI link at the relay are considered. Due to this practical assumption, the closed-form expression of EASR for any value of antenna number is mathmatically untrackable. To obtain the closed-form expression of approximate EASR for any value of antenna number, the Gauss-Laguerre Quadrature (GLQ) integral approximation method from the numerical analysis theory is applied. Monte Carlo simulation has verified that the approximation meets the simulation result very well.
- To reveal secrecy performance in the case of massive antennas condition, the closed-form expression of exact EASR for large-scale antenna array is derived. Simulation results have validated the correctness of our theoretical derivation and proved that large-scale antenna technique can enhance the EASR performance significantly.
- The asymptotic secrecy performances for any value of antenna and large-scale antenna array in two asymptotic cases, i.e., $P_S \to \infty$ and $P_R \to \infty$, are investigated,

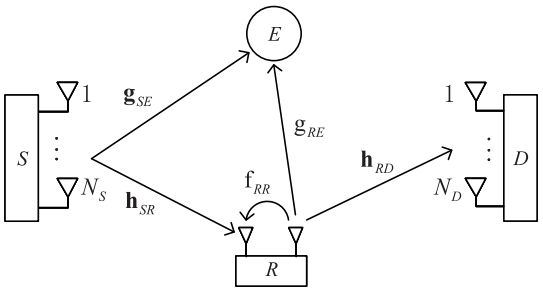


FIGURE 1. Communication model of the secure transmission system with a FD relay.

where P_S and P_R denote the transmit power at the source and the relay respectively. The asymptotic expressions are all in closed-form, and based on that, we gain several concise and meaningful conclusions.

The paper is organized as follows. Section II presents the transmission model and the ANP method. Section III provides the closed-form expressions for any value of antenna number and large-scale antenna array. Section IV shows the asymptotic secrecy performance analysis. Simulation results are presented in Section V and conclusions are drawn in Section VI.

Notation: Bold lower case letters denote vectors, e.g., $\mathbf{v}$. Bold upper case letters denote matrices, e.g., $\mathbf{M}$; $(\cdot)^T$, $(\cdot)^H$, $\mathbb{E}\{\cdot\}$, $|\cdot|$ and $\|\cdot\|$ indicate transpose, Hermitian transpose, mathematical expectation, modulo operator and Frobenius norm, respectively. Besides, $\mathcal{CN}\left(\mu, \sigma^2\right)$ stands for the complex Gaussian distribution with mean μ and variance σ^2.

II. SYSTEM MODEL

A. THE CONSIDERED SINGLE-ANTENNA EAVESDROPPER SCENARIO

Fig. 1 shows the secure FD relaying wireless communication system, which is composed of a N_S-antenna source (S), a N_D-antenna destination (D), a two-antenna FD DF relay (R), and a single-antenna passive eavesdropper (E). One of the two antennas at R is used to broadcast the intended signal, and the other is applied to receive. This paper considers the circumstance that direct transmission link between S and D does not exist owing to the severe propagation loss caused by long distance [35]. All links are modeled as block Rayleigh fading channels, i.e., the channel remains static for one coherence interval and changes independently in different coherence intervals [9]. The channels $S \rightarrow R$, $R \rightarrow D$, $S \rightarrow E$ and $R \rightarrow E$ are denoted as $\mathbf{h}_{SR} = \left[h_{1R}, h_{2R}, \cdots, h_{N_SR}\right]$, $\mathbf{h}_{RD} = \left[h_{R1}, h_{R2}, \cdots, h_{RN_D}\right]^T$, $\mathbf{g}_{SE} = \left[g_{1E}, g_{2E}, \cdots, g_{N_SE}\right]$ and g_{RE}, respectively. The SI link at R introduced by the FD technique is indicated as f_{RR}. Each element of $\mathbf{h}_{SR}$, $\mathbf{h}_{RD}$, $\mathbf{g}_{SE}$, g_{RE} and f_{RR} follows independently and identically distributed (i.i.d.) complex Gaussian distribution. In this paper, the transmit power of S and R are assumed as P_S and P_R, respectively.

To maximize the received SINR at R and disturb the interception of E, S applies the ANP scheme to broadcast the confidential information and the AN simultaneously. The signal emitted form the source can be expressed as

$$\mathbf{x}_S = \mathbf{w}_1 x + \mathbf{W}_2 \mathbf{v}, \tag{1}$$

where $x \sim \mathcal{CN}(0, \alpha P_S)$ is the intended information, $\mathbf{v} \in \mathbb{C}^{(N_S-1)\times 1}$ is the AN vector, and each element of $\mathbf{v}$ is an i.i.d. complex Gaussian random variable with zero mean and variance σ_v^2. Note that α $(0 < \alpha < 1)$ is the ratio of the power of information signal x to the total transmit power of source node P_S, and we have $\sigma_v^2 = (1-\alpha) P_S / (N_S - 1)$ owing to the equal distribution of transmit power among $N_S - 1$ AN variables.

This paper considers a frequency-division duplex (FDD) channel estimation system in which the channel reciprocity no longer holds. We assume that the relay node estimates the legitimate channel between S and R with estimation error and sends the estimated channel information to S through an ideal feedback channel which is a high-quality link with negligible quantization error [23]. This assumption is widely used and is based on the minimum mean square error (MMSE) estimation technique. The beamforming vector and AN precoding matrix are designed at the source by using the imperfect CSI of legitimate channel $S \rightarrow R$. Due to the existence of estimation error, the feedback error model of legitimate channel estimation can be formulated as

$$\mathbf{h}_{SR} = \sqrt{\rho}\widetilde{\mathbf{h}}_{SR} + \sqrt{1-\rho}\mathbf{h}_{err}, \tag{2}$$

where $\widetilde{\mathbf{h}}_{SR}$ denotes the estimated channel, $\mathbf{h}_{err} \sim \mathcal{CN}\left(0, \sigma_{err}^2 \mathbf{I}\right)$ represents the channel estimation error vector, and $\rho \in [0, 1]$ is the correlation coefficient between $\mathbf{h}_{SR}$ and $\widetilde{\mathbf{h}}_{SR}$. The larger ρ yields better channel estimation accuracy, and $\rho = 1$ means that the source obtains the perfect CSI of legitimate channel.

Based on the above, the transmit precoding vector $\mathbf{w}_1$ is designed to match the legitimate channel $\widetilde{\mathbf{h}}_{SR}$, i.e., $\mathbf{w}_1 = \widetilde{\mathbf{h}}_{SR}^H / \|\widetilde{\mathbf{h}}_{SR}\|$, and $\mathbf{W}_2$ is made as the orthogonal weight of the null space of $\widetilde{\mathbf{h}}_{SR}$, i.e., $\mathbf{W}_2 = null\left(\widetilde{\mathbf{h}}_{SR}\right)$ with $\mathbf{W}_2 \in \mathbb{C}^{N_S \times (N_S-1)}$. Note that the imperfect CSI will result in the AN leakage problem, i.e., AN is not perfectly mapped into the null space of legitimate channel and D will be interfered by the AN.

In the time slot i, S emits the signal $\mathbf{x}_s[i]$. Due to the FD mechanism, R receives the information transmitted from S and simultaneously broadcasts the re-encoded signal $t[i] = \sqrt{P_R/P_S}x[i-\tau]$ to D through its transmit antenna, where the integer $\tau \geq 1$ represents the information processing (i.e., the information decoding and encoding) time delay at the relay, which is typically long enough to guarantee that the relay transmits each time instant a symbol that is uncorrelated from the simultaneously received symbol [36]. Hence, the received signals at R and E can be separately calculated as

$$y_R[i] = \mathbf{h}_{SR}\mathbf{x}_S[i] + f_{RR}t[i] + n_R, \tag{3}$$

$$\begin{aligned} y_E[i] &= \mathbf{g}_{SE}\mathbf{x}_S[i] + g_{RE}t[i] + n_E \\ &= \mathbf{g}_{SE}\mathbf{w}_1 x[i] + \mathbf{g}_{SE}\mathbf{W}_2\mathbf{v} + g_{RE}t[i] + n_E, \end{aligned} \tag{4}$$

where f_{RR} represents the SI channel at R, $n_R \sim \mathcal{CN}\left(0, \sigma_R^2\right)$ and $n_E \sim \mathcal{CN}\left(0, \sigma_E^2\right)$ are the additional white Gaussian noises (AWGNs) at R and E, separately.

Because R is well aware of its own broadcasting signal, the effects of SI can be efficiently suppressed by the existing SIC techniques. In this paper, we consider the practical situation that the SIC at R is imperfect, the received signal at R after the incomplete SIC can be written as

$$\begin{aligned}\hat{y}_R[i] &= \mathbf{h}_{SR}\mathbf{x}_S[i] + \hat{f}_{RR}t[i] + n_R \\ &= \sqrt{\rho}\|\widetilde{\mathbf{h}}_{SR}\|x[i] + \underbrace{\sqrt{1-\rho}\mathbf{h}_{err}\mathbf{w}_1 x[i]}_{\text{estimation error}} \\ &\quad + \underbrace{\sqrt{1-\rho}\mathbf{h}_{err}\mathbf{W}_2\mathbf{v}}_{\text{AN leakage}} + \hat{f}_{RR}t[i] + n_R, \end{aligned} \tag{5}$$

where $\hat{f}_{RR}$ models the residual SI channel owing to the incomplete SIC and indicates the degree of SIC [37].

To maximize the received SNR, D applies the maximal ratio combining (MRC) technique, and the MRC combining vector is denoted as $\mathbf{h}_{RD}^H / \|\mathbf{h}_{RD}\|$. As a result, the received signals at D can be derived as

$$\begin{aligned} y_D[i] &= \frac{\mathbf{h}_{RD}^H}{\|\mathbf{h}_{RD}\|}\left(\mathbf{h}_{RD}t[i] + \mathbf{n}_D\right) \\ &= \|\mathbf{h}_{RD}\|\, t[i] + \frac{\mathbf{h}_{RD}^H}{\|\mathbf{h}_{RD}\|}\mathbf{n}_D, \end{aligned} \tag{6}$$

where $\mathbf{n}_D \sim \mathcal{CN}\left(0, \sigma_D^2\mathbf{I}\right)$ is the AWGN at D.

This paper focuses on the worst circumstance in the practical communication systems, which means that the CSI estimation error and the AN leakage are both modeled as independent Gaussian noise [25]. From (5), SINR at R is expressed as

$$\gamma_{SR} = \frac{\rho\alpha P_S \left\|\widetilde{\mathbf{h}}_{SR}\right\|^2}{G + |\hat{f}_{RR}|^2 P_R + \sigma_R^2}, \tag{7}$$

where

$$G = (1-\rho)P_S\mathbb{E}\left[\frac{(1-\alpha)\|\mathbf{h}_{err}\mathbf{W_2}\|^2}{N_S - 1} + \alpha|\mathbf{h}_{err}\mathbf{w_1}|^2\right]. \tag{8}$$

From (6), SNR of channel $R \to D$ can be derived as

$$\gamma_{RD} = \frac{\|\mathbf{h}_{RD}\|^2 P_R}{\sigma_D^2}. \tag{9}$$

Owing to the fixed DF strategy adopted at R [38], [39], the received SINR at D can be calculated as

$$\gamma_D = \min\left(\gamma_{SR}, \gamma_{RD}\right). \tag{10}$$

The eavesdropper can receive signals from the source and the relay simultaneously, and there is a time delay for the signal processing at the relay, (4) can be modeled as inter-symbol interference model [40]. In this paper, we focus on the specific circumstance that E intends to decode $x[i]$, treating other terms as interference and noise [41]. Therefore, the received SINR at E can be derived as

$$\gamma_E = \frac{\alpha P_S \gamma_1}{a\gamma_2 + \gamma_3 P_R + \sigma_E^2}, \tag{11}$$

where $\gamma_1 = |\mathbf{g}_{SE}\widetilde{\mathbf{h}}_{SR}^H|^2 / \|\widetilde{\mathbf{h}}_{SR}\|^2$, $\gamma_2 = \|\mathbf{g}_{SE}\mathbf{W}_2\|^2$, $\gamma_3 = |g_{RE}|^2$, and $a \triangleq (1-\alpha)P_S / (N_S - 1)$.

It is worthy to note that γ_{SR}, γ_{RD}, and γ_i for $i = 1, 2, 3$ are independent with each other. Each element of $\widetilde{\mathbf{h}}_{SR}$, $\mathbf{h}_{RD}$, $\mathbf{g}_{SE}$, g_{RE} and $\hat{f}_{RR}$ follows the i.i.d. complex Gaussian distribution with zero mean and variance Ω_{SR}, Ω_{RD}, Ω_{SE}, Ω_{RE} and Ω_{RR}/K, respectively, where K represents the strength of SIC. Thus, $\|\widetilde{\mathbf{h}}_{SR}\|^2$ and γ_{RD} follow the Gamma distribution, i.e., $\|\widetilde{\mathbf{h}}_{SR}\|^2 \sim \Gamma\left(N_S, 1/\Omega_{SR}\right)$, $\gamma_{\mathrm{RD}} \sim \Gamma\left(N_D, \sigma_D^2/\left(P_R\Omega_{RD}\right)\right)$. Meanwhile, $|\hat{f}_{RR}|^2$ and γ_3 follow the exponential distribution with expectation Ω_{RR}/K and Ω_{RE} respectively. Note that $\mathbf{w}_1$ and $\mathbf{W}_2$ can constitute unitary matrix $[\mathbf{w}_1, \mathbf{W}_2]$ and each element of $\mathbf{h}_{err}$ follows i.i.d. Gaussian distribution with zero mean and variance σ_{err}^2, thus we get $|\mathbf{h}_{err}\mathbf{w}_1|^2 \sim \mathrm{E}\left(1/\sigma_{err}^2\right)$, $\|\mathbf{h}_{err}\mathbf{W}_2\|^2 \sim \Gamma\left(N_S - 1, 1/\sigma_{err}^2\right)$, $\gamma_2 \sim \Gamma\left(N_S - 1, 1/\Omega_{SE}\right)$ and $\gamma_1 \sim \mathrm{E}\left(1/\Omega_{SE}\right)$.

Combining (8) and the above analysis, we can calculate that $G = (1-\rho)P_S\sigma_{err}^2$, and (7) can be reformulated as

$$\gamma_{SR} = \frac{\rho\alpha P_S \left\|\widetilde{\mathbf{h}}_{SR}\right\|^2}{(1-\rho)P_S\sigma_{err}^2 + |\hat{f}_{RR}|^2 P_R + \sigma_R^2}. \tag{12}$$

B. THE DISCUSSION ABOUT MULTIPLE-ANTENNA EAVESDROPPER SCENARIO

For fairness of the system setting, the eavesdropper should be set to equip multiple antennas. In the case of multiple-antenna eavesdropper, the received signal at E, i.e., (4), should be revised as

$$\begin{aligned}\mathbf{y}_E[i] &= \mathbf{G}_{SE}\mathbf{x}_S[i] + \mathbf{g}_{RE}t[i] + \mathbf{n}_E \\ &= \mathbf{G}_{SE}\mathbf{w}_1 x[i] + \mathbf{G}_{SE}\mathbf{W}_2\mathbf{v} + \mathbf{g}_{RE}t[i] + \mathbf{n}_E, \end{aligned} \tag{13}$$

where $\mathbf{G}_{SE}$ represents the MIMO channel between the source and the eavesdropper, $\mathbf{g}_{RE}$ denotes the single-input multiple-out (SIMO) channel between the relay and the eavesdropper, and $\mathbf{n}_E$ indicates the AWGN vector at the eavesdropper.

Unfortunately, to the best of the authors' knowledge, the distribution of the MIMO channel $\mathbf{G}_{SE}$ is still unknown in open literature [42]. Therefore, it is extremely difficult to derive the statistical functions for (13), and further derivations are impossible to be done. To make the ensuing mathematical analysis tractable and to attain meaningful results, we have to consider the compromised scenario, i.e., the single-antenna eavesdropper scene.

The compromised scenario we consider can be practical in the following situation. While the source communicates with the destination with the help of a FD relay, the eavesdropper tries to intercept the confidential information from both the source and the relay, which means that the geographical

position of the eavesdropper is much better than that of the destination. To occupy a better geographical position, the eavesdropper must be portable and flexible, e.g., hand-carried eavesdropping equipment. The portable eavesdropper always has low system complexity and small size for the sake of portability, which means it contains low data storage, limited processing power and a small number of antennas.

III. ERGODIC ACHIEVABLE SECRECY RATE ANALYSIS

In this section, we will analyze the EASR performance of FD relaying communication systems. In our proposed model, the secrecy capacity can be calculated as $C_S = [C_D - C_E]^+$, where $[x]^+ \triangleq \max\{0, x\}$. The mutual information of legitimate link is indicated as C_D and that of eavesdropping link is denoted as C_E, where $C_D = \log_2(1+\gamma_D)$ and $C_E = \log_2(1+\gamma_E)$. The rate below which any average secure communication rate is achievable is named as the ergodic secrecy capacity, which can be given in the case of block fading channels by [43]

$$\begin{aligned}\mathbb{E}[C_S] &= \int_0^\infty \int_0^\infty [C_D - C_E]^+ f(\gamma_D) f(\gamma_E)\, d\gamma_D d\gamma_E \\ &= \mathbb{E}\left[[C_D - C_E]^+\right]. \end{aligned} \tag{14}$$

Unfortunately, the exact evaluation of (14) is intractable in our considered wireless communication model. Alternatively, we focus our analysis on the lower bound of (14), given by

$$\mathbb{E}[C_S] \geq [\mathbb{E}[C_D] - \mathbb{E}[C_E]]^+ \triangleq \overline{C}_S, \tag{15}$$

which is known as the ergodic achievable secrecy rate (EASR).

A. EASR ANALYSIS FOR ANY VALUE OF ANTENNA NUMBER

In this subsection, we will calculate and derive the closed-form expressions of approximate $\mathbb{E}[C_D]$ and $\mathbb{E}[C_E]$, respectively.

Lemma 1: The approximate ergodic capacity of legitimate channel is given by

$$\mathbb{E}[C_D] \approx \frac{1}{\ln 2} \sum_{i=1}^{q} \omega_i \Phi(z_i), \tag{16}$$

where $\Phi(x)$ is defined as (23) at the top of the next page, q indicates the approximation points utilized to approximate the integral, z_i $(i = 0, 1, ..., q)$ indicates the i-th root of the Laguerre polynomial $\mathcal{L}_q(z)$ and ω_i denotes the i-th weight given by

$$\omega_i = \frac{z_i}{\left[(q+1)\mathcal{L}_{q+1}(z_i)\right]^2}, \tag{17}$$

which is independent of $\Phi(z)$ [9]. Note that both z_i and ω_i can be computed efficiently by applying the method proposed in [44].

Proof: We can formulate $\mathbb{E}[C_D]$ as

$$\begin{aligned}\mathbb{E}[C_D] &= \frac{1}{\ln 2}\mathbb{E}[\ln(1+\gamma_D)] \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\gamma_D}(x)}{1+x} dx. \end{aligned} \tag{18}$$

Combining (7), we can derive the CDF of γ_{SR} as (19) which is shown at the top of the next page.

From (9), the CDF of γ_{RD} can be expressed as

$$F_{\gamma_{RD}} = 1 - e^{-\frac{\sigma_D^2 x}{P_R \Omega_{RD}}} \sum_{n=0}^{N_D-1} \frac{1}{n!} \left(\frac{\sigma_D^2 x}{P_R \Omega_{RD}}\right)^n. \tag{20}$$

Based on (19) and (20), and applying the equation $F_{\min(\mathbf{X},\mathbf{Y})}(\cdot) = 1 - [1 - F_{\mathbf{X}}(\cdot)][1 - F_{\mathbf{Y}}(\cdot)]$, the CDF of γ_D can be given by (21) which is written at the top of the next page.

Substituting (21) into (18), we can obtain the semi closed-form expression of $\mathbb{E}[C_D]$ as

$$\mathbb{E}[C_D] = \frac{1}{\ln 2}\int_0^{+\infty} e^{-x}\Phi(x)\, dx. \tag{22}$$

The integral in (22) can not be further derived to a closed-form expression. To solve the problem, we resort it to the GLQ method [45]. According to the GLQ method, (16) can be obtained. ∎

Lemma 2: The approximate ergodic eavesdropping capacity can be given by

$$\mathbb{E}[C_E] \approx \frac{1}{\ln 2} \sum_{i=1}^{q} \omega_i \mathcal{H}(z_i), \tag{24}$$

where

$$\begin{aligned}\mathcal{H}(z_i) = &\left[\frac{N_S - 1}{\alpha(N_S - 1) + (1-\alpha)x}\right]^{N_S - 1} \\ &\times \frac{\alpha^{N_S} P_S \Omega_{SE} e^{1 - \frac{\sigma_E^2}{\alpha P_S \Omega_{SE}} x}}{(1+x)(\alpha P_S \Omega_{SE} + P_R \Omega_{RE} x)}. \end{aligned} \tag{25}$$

Proof: Invoking (11), the CDF of γ_E can be written as

$$\begin{aligned}F_{\gamma_E}(x) = 1 - &\left[\frac{N_S - 1}{\alpha(N_S - 1) + (1-\alpha)x}\right]^{N_S - 1} \\ &\times \frac{\alpha^{N_S} P_S \Omega_{SE} e^{1 - \frac{\sigma_E^2}{\alpha P_S \Omega_{SE}} x}}{\alpha P_S \Omega_{SE} + P_R \Omega_{RE} x}. \end{aligned} \tag{26}$$

The following derivation is similar to the proof of (16), and is omitted here. ∎

Finally, from (15), (16) and (24), the closed-form expression of approximate EASR for any value of antenna number can be derived as

$$\overline{C}_S \approx \frac{1}{\ln 2}\left[\sum_{i=1}^{q} \omega_i \Phi(z_i) - \sum_{i=1}^{q} \omega_i \mathcal{H}(z_i)\right]^+. \tag{27}$$

B. EASR ANALYSIS FOR LARGE-SCALE ANTENNA ARRAY

Theorem 1: As $N_S \to \infty$, $N_D \to \infty$, the EASR expression of the considered wireless relaying model can be given by

$$\overline{C}_S|_{\text{large}} = \left\{\mathbb{E}[C_D]|_{\text{large}} - \mathbb{E}[C_E]|_{\text{large}}\right\}^+, \tag{28}$$

$$F_{\gamma_{SR}}(x) = 1 - Ke^{-\frac{\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]x}{\rho\alpha P_S\Omega_{SR}}} \sum_{m=0}^{N_S-1}\sum_{v=0}^{m} \frac{P_R^{m-v}\Omega_{RR}^{m-v}x^m\left(\rho\alpha K P_S\Omega_{SR}+P_R\Omega_{RR}x\right)^{v-m-1}\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]^v}{\left(\rho\alpha P_S\Omega_{SR}\right)^{v-1}v!} \tag{19}$$

$$F_{\gamma_D}(x) = 1 - Ke^{-\left[\frac{(1-\rho)P_S\sigma_{err}^2+\sigma_R^2}{\rho\alpha P_S\Omega_{SR}}+\frac{\sigma_D^2 x}{P_R\Omega_{RD}}\right]x} \times \sum_{m=0}^{N_S-1}\sum_{v=0}^{m}\sum_{n=0}^{N_D-1} \frac{P_R^{m-v-n}x^{m+n}\Omega_{RR}^{m-v}\sigma_D^{2n}\left(\rho\alpha K P_S\Omega_{SR}+P_R\Omega_{RR}x\right)^{v-m-1}\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]^v}{\left(\rho\alpha P_S\Omega_{SR}\right)^{v-1}v!n!\Omega_{RD}^n} \tag{21}$$

$$\Phi(x) = Ke^{\left[1-\frac{(1-\rho)P_S\sigma_{err}^2+\sigma_R^2}{\rho\alpha P_S\Omega_{SR}}-\frac{\sigma_D^2 x}{P_R\Omega_{RD}}\right]x} \times \sum_{m=0}^{N_S-1}\sum_{v=0}^{m}\sum_{n=0}^{N_D-1} \frac{P_R^{m-v-n}x^{m+n}\Omega_{RR}^{m-v}\sigma_D^{2n}\left(\rho\alpha K P_S\Omega_{SR}+P_R\Omega_{RR}x\right)^{v-m-1}\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]^v}{(1+x)\left(\rho\alpha P_S\Omega_{SR}\right)^{v-1}v!n!\Omega_{RD}^n} \tag{23}$$

where $\mathbb{E}[C_D]|_{\text{large}}$ and $\mathbb{E}[C_E]|_{\text{large}}$ are written as (29) and (30) respectively, both shown at the top of the next page;

$$\Xi = \min\left(\frac{\rho\alpha P_S N_S\Omega_{SR}}{(1-\rho)P_S\sigma_{err}^2+\sigma_R^2}, \frac{P_R N_D\Omega_{RD}}{\sigma_D^2}\right),$$

$\Gamma(\cdot,\cdot)$ indicates the incomplete Gamma function, and $\text{Ei}(\cdot)$ denotes the exponential integral function.

Proof: As $N_S \to \infty$, by the law of large numbers, we get

$$\begin{aligned}\gamma_{SR}|_{\text{large}} &= \frac{\rho\alpha P_S\|\mathbf{h}_{SR}\|^2}{(1-\rho)P_S\sigma_{err}^2+|\hat{f}_{RR}|^2P_R+\sigma_R^2} \\ &= \frac{\rho\alpha P_S\sum_{i=1}^{N_S}|h_{iR}|^2}{(1-\rho)P_S\sigma_{err}^2+|\hat{f}_{RR}|^2P_R+\sigma_R^2} \\ &\approx \frac{\rho\alpha P_S N_S\mathbb{E}\left[|h_{iR}|^2\right]}{(1-\rho)P_S\sigma_{err}^2+|\hat{f}_{RR}|^2P_R+\sigma_R^2}.\end{aligned} \tag{31}$$

Since $|h_{iR}|^2$ follows the exponential distribution with mean Ω_{SR}, i.e., $\mathbb{E}\left[|h_{iR}|^2\right] = \Omega_{SR}$, we have

$$\gamma_{SR}|_{\text{large}} \approx \frac{\rho\alpha P_S\Omega_{SR}N_S}{(1-\rho)P_S\sigma_{err}^2+|\hat{f}_{RR}|^2P_R+\sigma_R^2}. \tag{32}$$

Similarly, we get $\gamma_{RD}|_{\text{large}} \approx N_D P_R\Omega_{RD}/\sigma_D^2$, $\gamma_2|_{\text{large}} \approx (N_S-1)\Omega_{SE}$.

In the case of large-scale antenna array, the ergodic legitimate capacity can be calculated as

$$\mathbb{E}[C_D]|_{\text{large}} = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_{\gamma_D|\text{large}}(x)}{1+x}dx. \tag{33}$$

The CDF of $\gamma_D|_{\text{large}}$ is written as (34) at the top of the next page.

When $x \geq \rho\alpha P_S\Omega_{SR}N_S/\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]$ and $x < N_D P_R\Omega_{RD}/\sigma_D^2$, the following equation holds true

$$\Pr\left(\frac{\frac{\rho\alpha P_S N_S\Omega_{SR}}{x}-\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]}{P_R} \leq |\hat{f}_{RR}|^2\right) = 1. \tag{35}$$

When $x < \rho\alpha P_S\Omega_{SR}N_S/\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]$ and $x < N_D P_R\Omega_{RD}/\sigma_D^2$, applying $|\hat{f}_{RR}|^2 \sim \text{E}(K/\Omega_{RR})$, we obtain

$$\Pr\left(\frac{\frac{\rho\alpha P_S N_S\Omega_{SR}}{x}-\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]}{P_R} \leq |\hat{f}_{RR}|^2\right) = e^{-K\frac{\rho\alpha P_S N_S\Omega_{SR}-\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]x}{P_R\Omega_{RR}x}}$$

As a result, the CDF of $\gamma_D|_{\text{large}}$ can be given by

$$F_{\gamma_D|\text{large}}(x) = \begin{cases} 1, & x \geq \Xi \\ e^{-K\frac{\rho\alpha P_S N_S\Omega_{SR}-\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]x}{P_R\Omega_{RR}x}}, & x < \Xi. \end{cases} \tag{36}$$

Substituting (36) into (33), we can obtain (29). Similarly, we can get (30). ■

Note that, in this subsection, we applied the law of large numbers to analyze the EASR performance for large-scale antenna array. In addition, it is potential to perform the large system analysis by using the methods in [46] and show its corresponding performance. However, the study about performing the large system analysis is beyond the scope of this paper and we will study the large system analysis in the future research.

IV. ASYMPTOTIC PERFORMANCE ANALYSIS

The closed-form expression of approximate EASR for any value of antenna number and that of exact EASR for large-scale antenna array have been calculated in the last section. However, the closed-form expressions of EASR are too complicated to obtain some simple and meaningful conclusions. To analyze the secure performance of the system more effectively and find some concise and significative verdicts, this section will provide the analysis of EASR in two asymptotic cases, i.e., $P_S \to \infty$ and $P_R \to \infty$.

$$\mathbb{E}\left[C_D\right]|_{\text{large}} = \frac{1}{\ln 2}\left\{\ln\left(1+\Xi\right) - e^{\frac{K\left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]}{P_R\Omega_{RR}}}\left[\Gamma\left(0, \frac{K\rho\alpha P_S N_S\Omega_{SR}}{P_R\Omega_{RR}\Xi}\right)\right.\right.$$
$$\left.\left. - e^{\frac{K\rho\alpha P_S N_S\Omega_{SR}}{P_R\Omega_{RR}}}\Gamma\left(0, \frac{K\rho\alpha P_S N_S\Omega_{SR}}{P_R\Omega_{RR}}\left(1+\frac{1}{\Xi}\right)\right)\right]\right\} \quad (29)$$

$$\mathbb{E}\left[C_E\right]|_{\text{large}} = \begin{cases} \frac{\alpha P_S\Omega_{SE}}{\left(\alpha P_S\Omega_{SE} - P_R\Omega_{RE}\right)\ln 2}\left[e^{\frac{(1-\alpha)P_S\Omega_{SE}+\sigma_E^2}{P_R\Omega_{RE}}}\text{Ei}\left(-\frac{(1-\alpha)P_S\Omega_{SE}+\sigma_E^2}{P_R\Omega_{RE}}\right)\right. \\ \left. - e^{\frac{(1-\alpha)P_S\Omega_{SE}+\sigma_E^2}{\alpha P_S\Omega_{SE}}}\text{Ei}\left(-\frac{(1-\alpha)P_S\Omega_{SE}+\sigma_E^2}{\alpha P_S\Omega_{SE}}\right)\right], & \alpha P_S\Omega_{SE} \neq P_R\Omega_{RE} \\ \frac{1}{\ln 2}\left[1+\frac{P_S\Omega_{SE}-P_R\Omega_{RE}+\sigma_E^2}{P_R\Omega_{RE}}e^{\frac{P_S\Omega_{SE}-P_R\Omega_{RE}+\sigma_E^2}{P_R\Omega_{RE}}}\text{Ei}\left(-\frac{P_S\Omega_{SE}-P_R\Omega_{RE}+\sigma_E^2}{P_R\Omega_{RE}}\right)\right], & \alpha P_S\Omega_{SE} = P_R\Omega_{RE} \end{cases} \quad (30)$$

$$F_{\gamma_D|\text{large}}\left(x\right) = \begin{cases} 1, & x \geq \frac{N_D P_R\Omega_{RD}}{\sigma_D^2} \\ \Pr\left(\frac{\frac{\rho\alpha P_S N_S\Omega_{SR}}{x} - \left[(1-\rho)P_S\sigma_{err}^2+\sigma_R^2\right]}{P_R} \leq |\hat{f}_{RR}|^2\right), & x < \frac{N_D P_R\Omega_{RD}}{\sigma_D^2} \end{cases} \quad (34)$$

A. EASR ANALYSIS FOR ANY VALUE OF ANTENNA NUMBER WHEN $P_S \to \infty$

Theorem 2: The closed-form expression of EASR for any value of antenna number when $P_S \to \infty$ can be derived as

$$\overline{C}_{\text{S}}^{P_S\to\infty} = \left\{\mathbb{E}\left[C_D\right]^{P_S\to\infty} - \mathbb{E}\left[C_E\right]^{P_S\to\infty}\right\}^+, \quad (37)$$

where $\mathbb{E}\left[C_D\right]^{P_S\to\infty}$ and $\mathbb{E}\left[C_E\right]^{P_S\to\infty}$ are expressed respectively as (42) and (43) at the top of the next page, where ${}_2F_1\left(\cdot,\cdot;\cdot;\cdot\right)$ means hypergeometric function.

Proof: When $P_S \to \infty$, (12) can be revised as

$$\gamma_{SR}^{P_S\to\infty} = \frac{\rho\alpha\left\|\mathbf{h}_{SR}\right\|^2}{\left(1-\rho\right)\sigma_{err}^2}. \quad (38)$$

Furthermore, the CDF of $\gamma_{SR}^{P_S\to\infty}$ and $\gamma_E^{P_S\to\infty}$ can be written respectively as

$$F_{\gamma_{SR}^{P_S\to\infty}}\left(x\right) = 1 - e^{-\frac{(1-\rho)\sigma_{err}^2}{\rho\alpha\Omega_{SR}}}\sum_{m=0}^{N_S-1}\frac{\left[\frac{(1-\rho)\sigma_{err}^2}{\rho\alpha\Omega_{SR}}x\right]^m}{m!}, \quad (39)$$

$$F_{\gamma_E^{P_S\to\infty}}\left(x\right) = 1 - \left[\frac{\alpha\left(N_S-1\right)}{\alpha\left(N_S-1\right)+\left(1-\alpha\right)x}\right]^{N_S-1}. \quad (40)$$

The CDF of $\gamma_D^{P_S\to\infty}$ is derived as (41) which is shown at the top of the next page. Finally, we can calculate the closed-form expressions of $\mathbb{E}\left[C_D\right]^{P_S\to\infty}$ and $\mathbb{E}\left[C_E\right]^{P_S\to\infty}$as (42) and (43), respectively. ■

According to (37), when $P_S \to \infty$, the closed-form expression of EASR for any value of antenna number is no longer related to P_S and K, indicating that when P_S is high enough, the degree of SIC can not effect the EASR performance any more, meanwhile there is no need to increase P_S. The reason is that, as $P_S \to \infty$, the strength of the signal transmitted from S is much greater than that of the signal emitted from R. However, (37) is still relative to P_R due to the DF protocol adopted at R.

B. EASR ANALYSIS FOR ANY VALUE OF ANTENNA NUMBER WHEN $P_R \to \infty$

Theorem 3: The closed-form expression of EASR for any value of antenna number when $P_R \to \infty$ can be derived as

$$\overline{C}_{\text{S}}^{P_R\to\infty} = 0. \quad (44)$$

Proof: When $P_R \to \infty$, (12) can be rewritten as $\gamma_{SR}^{P_R\to\infty} = 0$. Thus, the relay cannot decode the signal from the source correctly, resulting in $\mathbb{E}\left[C_D\right]^{P_R\to\infty} = 0$. Similarly, it can be obtained from (11) that $\gamma_E^{P_R\to\infty} = 0$ and $\mathbb{E}\left[C_E\right]^{P_R\to\infty} = 0$. Therefore, when $P_R \to \infty$, $\overline{C}_{\text{S}}^{P_R\to\infty} = 0$. ■

From *Theorem 3* and its proof, we see that the EASR expressions for any value of antenna number and the ergodic capacity of the legitimate channel and the eavesdropping channel all equal zero. This is because the high transmit power of the relay results in high level of SI so that the relay cannot decode information correctly, and also seriously affects the reliable reception of the legitimate node and the eavesdropper node.

C. EASR ANALYSIS FOR LARGE-SCALE ANTENNA WHEN $P_S \to \infty$

Theorem 4: The closed-form EASR expression for large-scale antenna array when $P_S \to \infty$ can be derived as

$$\overline{C}_{\text{S}}|_{large}^{P_S\to\infty} = \left\{\mathbb{E}\left[C_D\right]|_{large}^{P_S\to\infty} - \mathbb{E}\left[C_E\right]|_{large}^{P_S\to\infty}\right\}^+, \quad (45)$$

$$F_{\gamma_D^{P_S\to\infty}}(x) = 1 - e^{-\frac{(1-\rho)P_R\Omega_{RD}\sigma_{err}^2+\rho\alpha\sigma_D^2\Omega_{SR}}{\rho\alpha P_R\Omega_{SR}\Omega_{RD}}x}\sum_{m=0}^{N_S-1}\sum_{n=0}^{N_D-1}\frac{(1-\rho)^m\sigma_{err}^{2m}\sigma_D^{2n}x^{m+n}}{m!n!\left(\rho\alpha\Omega_{SR}\right)^m\left(P_R\Omega_{RD}\right)^n} \tag{41}$$

$$\mathbb{E}[C_D]^{P_S\to\infty} = \sum_{m=0}^{N_S-1}\sum_{n=0}^{N_D-1}\frac{(1-\rho)^m\sigma_{err}^{2m}\sigma_D^{2n}(m+n)!}{m!n!\left(\rho\alpha\Omega_{SR}\right)^m\left(P_R\Omega_{RD}\right)^n} \times e^{\frac{(1-\rho)P_R\Omega_{RD}\sigma_{err}^2+\rho\alpha\sigma_D^2\Omega_{SR}}{\rho\alpha P_R\Omega_{SR}\Omega_{RD}}}\Gamma\left(-m-n, \frac{(1-\rho)P_R\Omega_{RD}\sigma_{err}^2+\rho\alpha\sigma_D^2\Omega_{SR}}{\rho\alpha P_R\Omega_{SR}\Omega_{RD}}\right) \tag{42}$$

$$\mathbb{E}[C_E]^{P_S\to\infty} = \frac{(1-N_S)(1-\alpha N_S)+N_S(1-\alpha)}{(N_S-1)(1-\alpha)N_S}{}_2F_1\left(1,1;1+N_S;\frac{1-\alpha N_S}{1-\alpha}\right) \tag{43}$$

where $\mathbb{E}[C_D]|_{large}^{P_S\to\infty}$ and $\mathbb{E}[C_E]|_{large}^{P_S\to\infty}$ are written as (47) and (50), respectively.

Proof: When $P_S \to \infty$, (32) can be rewritten as

$$\gamma_{SR}|_{large}^{P_S\to\infty} = \frac{\rho\alpha N_S\Omega_{SR}}{(1-\rho)\sigma_{err}^2}. \tag{46}$$

Furthermore, we can get the closed-form expression of ergodic capacity of the legitimate channel as (47) which is shown at the bottom of the next page.

Similarly, (11) can be revised as

$$\gamma_E|_{large}^{P_S\to\infty} = \frac{\alpha\gamma_1}{(1-\alpha)\Omega_{SE}}. \tag{48}$$

Thus, the CDF of $\gamma_E|_{large}^{P_S\to\infty}$ and the closed-form expression of the ergodic eavesdropping capacity in the case of large-scale antenna array can be respectively calculated as

$$F_{\gamma_E|_{large}^{P_S\to\infty}}(x) = 1 - e^{-\frac{1-\alpha}{\alpha}x}, \tag{49}$$

$$\mathbb{E}[C_E]|_{large}^{P_S\to\infty} = \frac{1}{\ln 2}e^{\frac{1-\alpha}{\alpha}}\Gamma\left(0, \frac{1-\alpha}{\alpha}\right). \tag{50}$$

The proof is completed. ■

From *Theorem 4*, we can obtain the following conclusions. In the case of $P_R \geq \rho\alpha N_S\Omega_{SR}\sigma_D^2/\left[(1-\rho)\sigma_{err}^2 N_D\Omega_{RD}\right]$, $\overline{C}_S|_{large}^{P_S\to\infty}$ is not related to P_S, P_R, and N_D any more and is a monotonically increasing function w.r.t. ρ or N_S. Namely, when the transmit power of the relay is extremely high, the EASR performance for large-scale antenna array can be improved effectively as N_S increases, and a good channel estimation is also an essential issue for the EASR performance. In the case of $P_R < \rho\alpha N_S\Omega_{SR}\sigma_D^2/\left[(1-\rho)\sigma_{err}^2 N_D\Omega_{RD}\right]$, $\overline{C}_S|_{large}^{P_S\to\infty}$ has nothing to do with P_S or N_S and increases monotonically w.r.t. P_R or N_D. In this case, the EASR performance can be strengthened significantly by increasing P_R or N_D. Note that P_R should not be set too high, to prevent P_R from exceeding the threshold $\rho\alpha N_S\Omega_{SR}\sigma_D^2/\left[(1-\rho)\sigma_{err}^2 N_D\Omega_{RD}\right]$, which will make the EASR irrelevant to P_R or N_D. Moreover, ρ is not a parameter in the EASR expression any more, indicating that the impact of CSI estimation accuracy to the EASR performance can be ignored.

In addition, when $P_S \to \infty$, $\mathbb{E}[C_E]|_{large}^{P_S\to\infty}$ is related to α solely and increases monotonically w.r.t. α. Ω_{SE} and Ω_{RE} are no longer parameters in the EASR expression, and increasing N_S or N_D can effectively improve the performance of EASR. The reason is that with high P_S, large-scale antenna angular resolution can form powerful null-space which is strong enough to ensure secure communication even that the eavesdropper has perfect channel quality (e.g., the distance between the eavesdropper and the legitimate nodes is very close).

D. EASR ANALYSIS FOR LARGE-SCALE ANTENNA WHEN $P_R \to \infty$

Theorem 5: The closed-form EASR expression for large-scale antenna when $P_R \to \infty$ can be derived as

$$\overline{C}_S|_{large}^{P_R\to\infty} = 0. \tag{51}$$

Proof: When $P_R \to \infty$, (32) becomes $\gamma_{SR}|_{large}^{P_R\to\infty} = 0$, so the relay can not decode successfully. Thus, the ergodic capacity of legitimate channel for large-scale antenna can be formulated as $\mathbb{E}[C_D]|_{large}^{P_R\to\infty} = 0$. Similarly, (11) can be written as $\gamma_E|_{large}^{P_R\to\infty} = 0$, then $\mathbb{E}[C_E]|_{large}^{P_R\to\infty} = 0$. This completes the proof. ■

In the case of $P_R \to \infty$, the EASR expression for large-scale antenna array equals zero always, and the ergodic capacity of the legitimate and the eavesdropping channel are all zero. The reason is similar with that of EASR performance in the case of any value of antenna number when $P_R \to \infty$. In practical application, one should avoid increasing the relay transmit power blindly.

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we will provide the numerical simulations to validate the derived analytical close-form expressions by using the Monte Carlo method. The AWGN variances of all nodes are normalized without loss of generality, i.e., $\sigma_R^2 = \sigma_D^2 = \sigma_E^2 = 1$. Moreover, we set the variance of channel estimation error and the average channel power gain of all channels as $\Omega_{SR} = \Omega_{SE} = \Omega_{RD} = \Omega_{RE} = \sigma_{err}^2 = 0.1$. The distance of antennas at the relay is much closer than those of

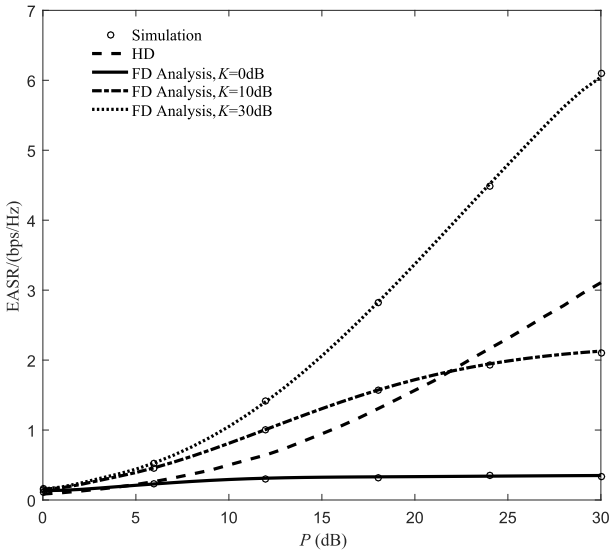


FIGURE 2. EASR performance comparison versus P with different K.

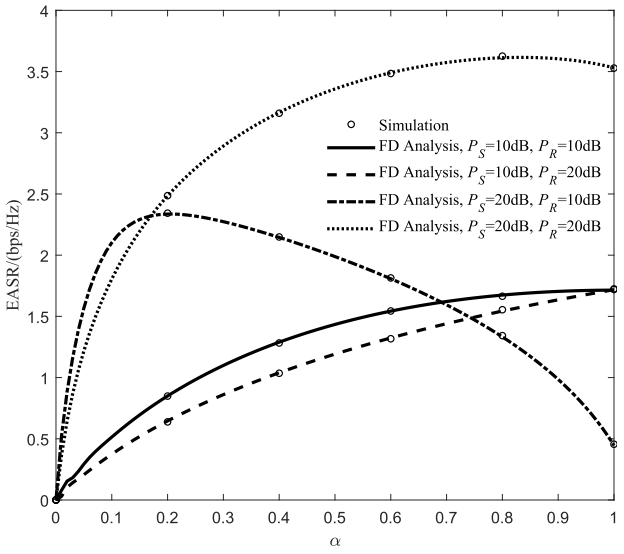


FIGURE 3. EASR performance versus α with different values of P_S and P_R.

other nodes, so we assume the average channel power gain $\Omega_{RR} = 1$. In all figures, the suffix "LS" indicates large-scale antenna condition. The simulation points indicate the average values obtained by 10^6 random channel realizations, according to the Monte Carlo method. Besides, we set $q = 24$ for the GLQ approximation in our paper.

In the case of the same total transmit power P, Fig. 2 compares the EASR performance of the proposed FD relaying scheme and that of the traditional half-duplex (HD) relaying method [16]. Note that the HD relaying scheme transmission model topology is the same as our proposed FD relaying model except that the relay node of the HD relaying scheme equips single antenna and works in the HD mode. The HD curve is generated by the Monte Carlo method, which is used to simulate the EASR performance of the conventional two-hop HD relaying scheme for comparison. Besides, the FD curves are from (27). To compare the EASR performance fairly, the total transmit power of each time slot for the above two transmission modes is set as a constant P, where $P_S + P_R = P$. In this figure, we set $\rho = 1$, which means that we consider the perfect CSI of legitimate channel obtained by the source. Set $N_S = N_D = 6$ and $\alpha = 0.5$. In each time slot of the FD relaying scheme and the second time slot of the HD relaying scheme, we allocate $P/2$ to S and R, respectively. It is important to note that, different from [16], the source broadcasts merely random AN and the relay node transmits forwarding signal simultaneously in the second time slot of the HD relaying scheme. In the first time slot of the HD relaying scheme, because R works in the receive mode, all the transmit power P should be allocated to S. It can be observed from Fig.2 that, the curves of (27) match well with the Monte Carlo simulation points, which approves the feasibility of GLQ method in this paper. In the case of $K = 0$dB, i.e., there is no SIC technique applied, the EASR performance of the proposed FD relaying scheme is very poor and almost stays constant with the increase of P. In the case of $K = 10$dB, the FD relaying scheme is not always superior to that of the HD relaying scheme, particularly in the middle to high level of P. In the case of $K = 30$dB, the EASR performance of the FD relaying scheme is almost twice than that of the HD relaying scheme for various P of interest, demonstrating the superiority of the FD relaying scheme as well as the necessity and importance of SIC.

Fig. 3 demonstrates the EASR performance versus the PA factor α with different P_S and P_R, in the case of $N_S = N_D = 6$, $\rho = 0.9$, and $K = 20$dB. All curves are form (27). From this figure, one can conclude that, the impact of P_R on EASR performance is significant under the condition of a constant P_S. In the case of low P_S ($P_S = 10$dB), the EASR performance will decrease significantly as P_R increases. The reason is that, larger P_R can cause stronger SI which will damage the EASR performance in the case of $P_S \leq P_R$. In the case of high P_S ($P_S = 20$dB), the increase of P_R will not always deteriorate the EASR performance. When there is a

$$\mathbb{E}\left[C_D\right]|_{large}^{P_S\to\infty} = \begin{cases} \log_2\left(1+\dfrac{\rho\alpha N_S\Omega_{SR}}{(1-\rho)\,\sigma_{err}^2}\right), & P_R \geq \dfrac{\rho\alpha N_S\Omega_{SR}\sigma_D^2}{(1-\rho)\,\sigma_{err}^2 N_D\Omega_{RD}} \\ \log_2\left(1+\dfrac{P_R N_D\Omega_{RD}}{\sigma_D^2}\right), & P_R < \dfrac{\rho\alpha N_S\Omega_{SR}\sigma_D^2}{(1-\rho)\,\sigma_{err}^2 N_D\Omega_{RD}} \end{cases} \tag{47}$$

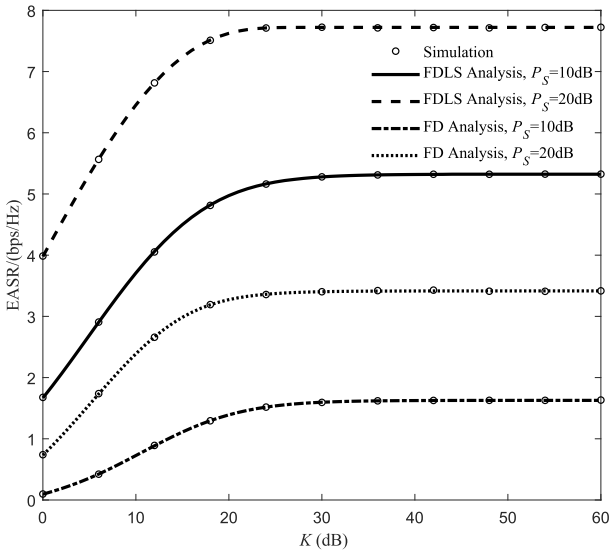


FIGURE 4. EASR performance versus K with different P_S.

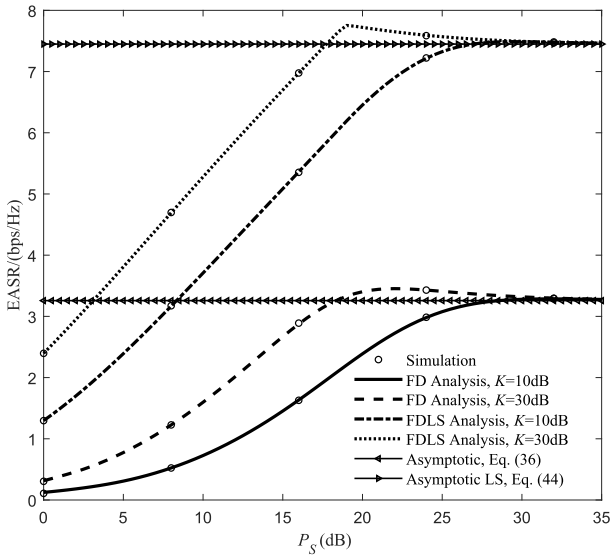


FIGURE 5. EASR performance versus P_S with various K.

large PA factor (e.g. $\alpha > 0.2$), the EASR performance will improve with the increase of P_R. This is due to that, when α is large enough, the power assigned to the intended signal is also relatively high and can offset the negative effect of high level of SI in the case of $P_S \geq P_R$.

Fig. 4 shows the EASR performance for any value of antenna number (27) and large-scale antenna array (28) as the function of K for different P_S. Set that the antenna numbers in (27) and (28) are $N_S = N_D = 6$ and $N_S = N_D = 100$ separately, $P_R = 15$dB, $\rho = 0.9$, and $\alpha = 0.5$. From Fig. 4, it is observed that the EASR performance of any value of antenna number and large-scale antenna array are increasing as K increases, and tend to different fixed values which are irrelevant to K and proportional to P_S. From the above analysis, we know that the improvement on the EASR performance due to the SIC technique exists an upper bound. In the figure, the EASR curves for large-scale antenna array match well with the simulation results, indicating the correctness of (28). Moreover, the large-scale antenna technique can enhance the EASR performance significantly.

Fig. 5 shows the curves of (27) and (28) versus P_S for different K. The values of N_S, N_D, P_R, ρ and α are set the same as that in Fig. 4. It is observed from Fig. 5 that the EASR curves for any value of antenna number and large-scale antenna array tend to different fixed values. The two asymptotic lines match well with the EASR curves in high P_S regime, indicating the correctness of (37) and (45). With the increase of P_S, the reason why the curves in the case of $K = 30$dB firstly increase and then decrease is due to the fixed DF strategy applied at the relay, which introduces the min function into the calculation of the main channel's SINR.

Fig. 6 shows the curves of (27) and (28) versus P_R for different K. The values of N_S, N_D, ρ and α are set the same as that in Fig.4, and we set $P_S = 15$dB. To verify the asymptotic analysis in the case of $P_R \to \infty$, we plot the

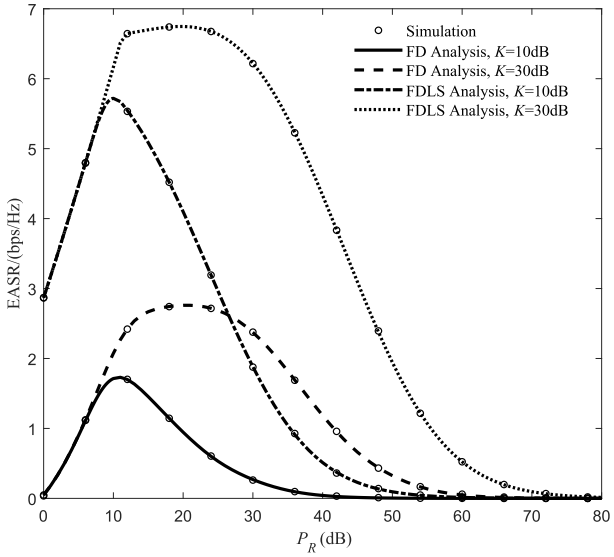


FIGURE 6. EASR performance versus P_R with different K.

EASR performance in the range of $P_R \in [0, 80]$. However, one should know that $P_R \leq 30$dB is our research range of interest. We find that the EASRs for any value of antenna number and large-scale antenna array both approach to zero with the increase of P_R, which approves the correctness of (44) and (51). Meanwhile, in the case of low P_R (e.g., $P_R \leq 10$dB), K is almost irrelevant to the EASR performance. This is because, when the transmit power of the relay is much lower than that of the source, the impact of SI on the EASR performance is negligible. From Fig. 6, it is observed that the curves firstly increase and then decrease with the increase of P_R. This is because that the relay applies the fixed DF strategy which introduces the min function into the derivation of the main channel's SINR.

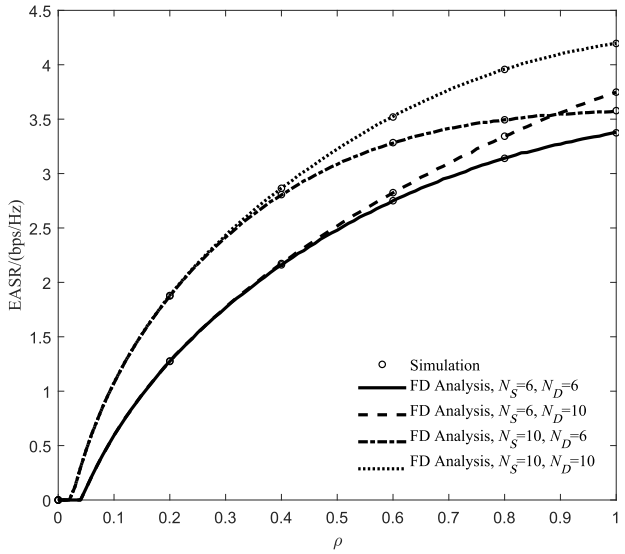


FIGURE 7. EASR performance versus ρ with different N_S and N_D.

Fig.7 plots the curves of (27) versus ρ for different N_S and N_D. In this figure, we set that $P_S = K = 20$dB, $P_R = 15$dB and $\alpha = 0.5$. From Fig.7, the EASR performance increases as ρ increases, and reaches the maximal values when $\rho = 1$, which proves the importance of channel estimation accuracy on the system performance. Meanwhile, increasing N_S can effectively improve the EASR performance. However, only when channel estimation accuracy is well ($\rho \geq 0.5$), increasing N_D can improve the EASR performance of the system as shown in Fig. 7, indicating that N_S definitely has priority over N_D if one wants to enhance the EASR performance by adding antenna number.

VI. CONCLUSION

In this paper, to help the legitimate party fight against the passive eavesdropper and enhance the overall secrecy performance, the ANP scheme adopted in the FD relaying wireless transmission system was proposed and analyzed. The EASR performance was analyzed with the consideration of SI channel at the relay and the imperfect CSI of legitimate channel acquired by the source. We derived and provided the closed-form expression of approximate EASR for any value of antenna number. Furthermore, the closed-form expression of exact EASR for large-scale antenna array was calculated and given. To gain more meaningful conclusions, we analyzed the asymptotic EASR performance in two asymptotic cases, i.e., $P_S \to \infty$ and $P_R \to \infty$. Simulation results validated that the GLQ method which is adopted to approximate the intractable integral in this paper is applicable and valid. According to the theoretical analysis and simulation results, the impacts of the system parameters on the EASR performance were characterized, and the effectiveness of the proposed ANP combined with FD relaying scheme was also authenticated.

REFERENCES

[1] 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.

[2] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[3] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-*m* fading channels," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 549–563, Oct. 2017.

[4] J. S. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, Jun. 2016.

[5] 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.

[6] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[7] C. Li, H. J. Yang, F. Sun, J. M. Cioffi, and L. Yang, "Adaptive overhearing in two-way multi-antenna relay channels," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 117–120, Jan. 2016.

[8] C. Li, H. J. Yang, F. Sun, J. M. Cioffi, and L. Yang, "Multiuser overhearing for cooperative two-way multiantenna relays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3796–3802, May 2016.

[9] Y. Li, R. Zhao, X. Tan, and Z. Nie, "Secrecy performance analysis of artificial noise aided precoding in full-duplex relay systems," in *Proc. IEEE GLOBECOM*, Dec. 2017, pp. 1–6.

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

[11] X. Tan, R. Zhao, and Y. Li, "Large-scale antennas analysis of untrusted relay system with cooperative jamming," in *Proc. 13th IEEE Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2017, pp. 1–5.

[12] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 913–927, Feb. 2014.

[13] Y. Feng, Z. Yang, S. Yan, N. Yang, and B. Lv, "Physical layer security enhancement in multi-user multi-full-duplex-relay networks," in *Proc. IEEE ICC*, May 2017, pp. 1–7.

[14] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[15] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[16] R. Zhao, Y. Huang, W. Wang, and V. K. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537–2551, Apr. 2016.

[17] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[18] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, Oct. 2016.

[19] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[20] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6658–6662, Jul. 2018.

[21] F. Shu, J. Wang, J. Li, R. Chen, and W. Chen, "Pilot optimization, channel estimation, and optimal detection for full-duplex OFDM systems with IQ imbalances," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 6993–7009, Aug. 2017.

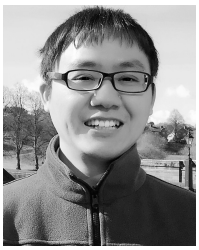
[22] F. Shu *et al.*, "Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2487–2501, Jun. 2018.

[23] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.
[24] Y. Li, R. Zhao, L. Fan, and A. Liu, "Antenna mode switching for full-duplex destination-based jamming secure transmission," *IEEE Access*, vol. 6, pp. 9442–9453, 2018.
[25] H.-M. Wang, C. Wang, T.-X. Zheng, and T. Q. S. Quek, "Impact of artificial noise on cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7390–7404, Nov. 2016.
[26] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[27] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
[28] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, Jan. 2015.
[29] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.
[30] 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.
[31] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357–360, Aug. 2014.
[32] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.
[33] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.
[34] A. M. Akhtar, A. Behnad, and X. Wang, "On the secrecy rate achievability in dual-hop amplify-and-forward relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 5, pp. 493–496, Oct. 2014.
[35] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.
[36] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.
[37] W. Mou, Y. Cai, W. Yang, W. Yang, X. Xu, and J. Hu, "Exploiting full duplex techniques for secure communication in SWIPT system," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Oct. 2015, pp. 1–6.
[38] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
[39] T. Q. Duong, V. N. Q. Bao, and H.-J. Zepernick, "On the performance of selection decode-and-forward relay networks over Nakagami-*m* fading channels," *IEEE Commun. Lett.*, vol. 13, no. 3, pp. 172–174, Mar. 2009.
[40] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
[41] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using alamouti-based rank-two beamforming," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 8, pp. 1359–1374, Dec. 2016.
[42] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.
[43] 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.
[44] G. W. Recktenwald, *Numerical Methods With MATLAB: Implementations and Applications*. Upper Saddle River, NJ, USA: Prentice-Hall, 2000.
[45] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Antenna switching for security enhancement in full-duplex wiretap channels," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2014, pp. 1308–1313.
[46] R. Couillet and M. Debbah, *Random Matrix Methods for Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

YUANJIAN LI received the B.S. degree from Nanjing Tech University, Nanjing, China, in 2015. He is currently pursuing the M.S. degree with the College of Information Science and Engineering, Huaqiao University, Xiamen, China. His current research interests include physical layer security, cooperative relay networks, and wireless networks.

RUI ZHAO (M'12) received the double bachelor's degree from the Harbin Institute of Technology in 2003, and the M.S. and Ph.D. degrees in electrical engineering from Southeast University, China, in 2006 and 2010, respectively. After graduation, he joined the School of Information Science and Engineering, Huaqiao University, China, where he is currently an Associate Professor. From 2014 to 2015, he visited the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong, where he was a Visiting Research Scholar studying the performance analysis of cooperative communication systems. He has published many papers in international journals such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE TRANSACTIONS ON COMMUNICATIONS, and papers in conferences such as the IEEE GLOBECOM and the IEEE ICC. His current research interests include cooperative communications, physical layer security communications, and MIMO communication systems.

YI WANG received the B.S. degree from PLA Information Engineering University, Zhengzhou, China, in 2006, and the M.S. and Ph.D. degrees from the School of Information Science and Engineering, Southeast University, China, in 2009 and 2016, respectively. Since 2016, he has been with the Faculty of the School of Electronics and Communication Engineering, Zhengzhou University of Aeronautics, China. His current research interests include massive MIMO, energy-efficient communication, relay-aided system, and physical layer security. He received the Best Paper Awards of the IEEE WCSP in 2015.



GAOFENG PAN (M'12) received the B.Sc. degree in communication engineering from Zhengzhou University, Zhengzhou, China, in 2005, and the Ph.D. degree in communication and information systems from Southwest Jiaotong University, Chengdu, China, in 2011.

He was with The Ohio State University, Columbus, OH, USA, from 2009 to 2011, as a joint-trained Ph.D. student under the supervision of Prof. E. Ekici. In 2012, he joined the School of Electronic and Information Engineering, Southwest University, Chongqing, China, where he is currently an Associate Professor. He was also with the School of Computing and Communications, Lancaster University, Lancaster, U.K., from 2016 to 2018, where he held a post-doctoral position under the supervision of Prof. Z. Ding. His research interest spans special topics in communications theory, signal processing and protocol design, including visible light communications, secure communications, CR/cooperative communications, and MAC protocols. From 2016 to 2018, he is a TPC Member of the IEEE GLOBECOM, the IEEE ICC, and the IEEE VTC. He has also served as a reviewer for major international journals, e.g., the IEEE JSAC, the IEEE TCOM, the IEEE TWC, the IEEE TSP, and the IEEE TVT. He was awarded as the Examplary Reviewer of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2017.

CHUNGUO LI (SM'16) received the bachelor's degree in wireless communications from Shandong University in 2005, and the Ph.D. degree in wireless communications from Southeast University, Nanjing, in 2010. In 2010, he joined the Faculty of Southeast University, where he became an Associate Professor in 2012 and a Full Professor in 2017. From 2012 to 2013, he was the Post-Doctoral Researcher with Concordia University, Montreal, Canada. From 2013 to 2014, he was with the DSL Laboratory as the Visiting Associate Professor, under the supervision of Prof. J. M. Cioffi. He has been the Supervisor of Ph.D. Candidate since 2016.

His research interests are in the 5G cellular transmission, underwater communications, machine learning for video signal processing, and next generation of WiFi. He is the Senior Member of the Chinese Institute of Electronics. He has served for many IEEE conferences, including the International Conference on Communications and the International Conference on Acoustics, Speech and Signal Processing as a TPC Member, and the IEEE 16th International Symposium on Communications and Information Technologies as the Track Chair of Wireless Communications, Special Session Signal Processing and Air Interface Design Solutions for Beyond 5G Wireless Communications on IEEE PIMRC-2018 as a Chair. He is currently the Area Editor of the *Elsevier AEU-International Journal of Electronics and Communications*, the Editor of *Telecommunications Systems*, the Associate Editor of the *Circuits, Systems and Signal Processing*, the Editor of the *KSII Transactions on Internet and Information Systems*, the Leading Guest Editor of the Special Issue Ultra-Reliable-and-Available Low-Latency Communications for 5G/B5G-enabled IoT on *EURASIP Journal on Wireless Communications and Networking*. He is the regular reviewer for many IEEE Journals.