Secrecy Performance Analysis of Artificial Noise Aided Precoding in Full-Duplex Relay Systems

Yuanjian Li, Rui Zhao, Xing Tan, Zhiqiao Nie
Xiamen Key Laboratory of Mobile Multimedia Communications, Huaqiao University, Xiamen, China
Email: {yjli, rzhao, xtan, zqnie}@hqu.edu.cn;

***Abstract*—In Rayleigh fading channels, we investigate the secrecy performance of a full-duplex relay secure transmission system. To improve the secrecy capacity of the system and efficiently interfere the interception of the eavesdropper, the multiple-antenna source applies the artificial noise aided precoding (ANP) scheme to broadcast the intended signal and the artificial noise simultaneously, and the decode-and-forward relay operates in full-duplex mode. To improve the received signal-to-noise ratio (SNR), the multiple-antenna destination applies maximum ratio combining (MRC) strategy. In the presence of self-interference at the relay, the approximate closed-form expression of ergodic achievable secrecy rate (EASR) for any values of antenna number and the exact closed-form expression of EASR for large-scale antennas array were derived respectively. Both the theoretical analysis and numerical simulations show that the ANP combined with full-duplex scheme can achieve considerable secrecy performance gain.**

***Index Terms*—Physical-layer security, full-duplex, decode-and-forward, artificial noise, achievable secrecy rate**

I. Introduction

SECURITY is the key part in wireless communication networks owing to the broadcast characteristics of radio signal. The security issue has become an increasingly challenging problem for wireless communication systems. Physical layer security has been a promising technique to complement the traditional cryptography due to its benefits in enhancing the secrecy level of wireless communications by directly exploiting the randomness offered by wireless channels [1], [2]. Wyner originally developed the concept of physical layer security for the Wyner wiretap model in [3]. In recent years, more extensive and practical physical layer security problem solutions have been investigated in academia, physical layer security technology has been more and more deeply concerned about.

The full-duplex (FD) relay allows the reception and transmission of information to be performed simultaneously, so that the wireless resources (time and frequency) can be utilized more efficiently. The self-interference (SI) caused by the signal leakage from the transmit antenna to the receive antenna is the main factor limiting the performance of the FD relay system. The presence of SI seriously reduces the received signal-to-interference ratio (SINR) of the relay, which in turn damages the overall performance of the communication system [4]. With the improvement of latest hardware design and the self-interference cancellation (SIC) technologies based on antenna isolation, analog elimination and digital elimination [5], the advantages of FD techinique can be fully exploited.

The existing study of the traditional three-node eavesdropping model show that the positive secrecy transmission rate does not always exist. Cooperative jamming (CJ) technology based on multiple antennas can not only enhance the rate of legitimate channel, but also reduce the risk of being intercepted, so that it can enhance the secrecy performance efficiently [6]. As an efficient CJ scheme employed at the source, artificial noise aided precoding (ANP) beamforms the artificial noise (AN) to the orthogonal space of the legitimate channel to improve the secrecy performance [7]. To maximize the average secrecy rate, the optimal power allocation (PA) solutions were investigated in [8], [9]. The secrecy performance of ANP has been further investigated for specific types of relay secure systems. In [10], the optimal beamforming and PA methods were proposed respectively for cases with known and unknown channel state information (CSI) of the eavesdropper link in decode-and-forward (DF) relay secure systems. In [11], an asymptotic analysis of ergodic secrecy capacity (ESC) and secrecy outage probability (SOP) was made for amplify-and-forward (AF) relay systems. In the presence of the direct links between the source to the destination and eavesdropper, the secrecy rate achievability in AF relay networks without jamming signal was characterized in [12]. When ANP meets FD in the relay secure systems, it becomes natural that significant improvement of secrecy performance can be realized.

In this paper, we consider a FD relay secure transmission system, where an eavesdropper can receive the signal from both the source and the relay, and the destination can only receive the signal from the relay. The multiple-antenna source applies the ANP scheme to broadcast the useful information and AN simultaneously. We fully consider the SI channel at the FD relay node, which increases the difficulty of deriving the closed-from expression of ergodic achievable secrecy rate (EASR). The approximate closed-form expression of EASR for any values of antenna number is obtained by using Gauss-Laguerre integral approximation method in numerical analysis theory. In order to further reveal the secrecy performance of the system with large-scale antennas array, the exact closed-from expression of EASR is derived. Based on the simulation results, the influence of system parameters on EASR is analyzed, and the EASR performance of the FD relay system is compared with that of the traditional half-duplex (HD) relay system, which highlights the superiority of the FD relay scheme and the importance of SIC.

This work was supported by the National Natural Science Foundation of China under Grant 61401165, and the Natural Science Foundation of Fujian Province under Grant 2015J01262.

978-1-5090-5019-2/17/$31.00 ©2017 IEEE
Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.

II. System Model

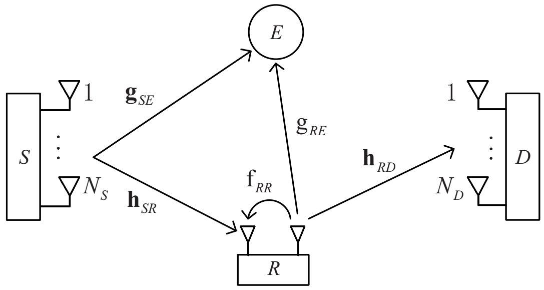

Figure 1. Transmission model of the dual-hop full-duplex relaying secure communication system.

Fig. 1 shows a full-duplex relay secure transmission system model, which is composed of a source (S), a destination (D), a full-duplex DF relay (R), and a passive eavesdropper (E). We assume there is no direct link between S and D due to the propagation loss caused by long distance [13]. The antenna numbers of S, D, R and E are N_S, N_D, 2 and 1, respectively. One of the two antennas at R is specifically for emission, and the other is for reception. 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. The channels $S \rightarrow R$, $R \rightarrow D$, $S \rightarrow E$ and $R \rightarrow E$ are denoted as $\mathbf{h}_{SR} = [h_{1R}, h_{2R}, \cdots, h_{N_S R}]^T$, $\mathbf{h}_{RD} = [h_{R1}, h_{R2}, \cdots, h_{RN_D}]^T$, $\mathbf{g}_{SE} = [g_{1E}, g_{2E}, \cdots, g_{N_S E}]^T$and g_{RE}, respectively. The SI channel at R induced by the full-duplex property is denoted 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 with zero mean and unit variance. In this paper, we assume that the transmit power of S and R are P_S and P_R, respectively. And the noise at each received node is the additive white Gaussian noise (AWGN) with zero mean and unit variance.

To maximize the received SINR of R and meanwhile to interfere the interception of E, S employs the ANP as the transmission strategy. The source signal can be formulated as

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

where $x[i]$ is the intended signal in the i-th time slot, $\mathbf{v}_1 \in \mathbb{C}^{(N_S-1)\times 1}$ is an AN vector and each element of $\mathbf{v}$ is an i.i.d. complex Gaussian random variable with variance σ_v^2, $\mathbf{w}_1$ is the transmit beamforming vector and is chosen to match the first hop channel $\mathbf{h}_{SR}$, i.e., $\mathbf{w}_1 = \mathbf{h}_{SR}/\|\mathbf{h}_{SR}\|$ and $\mathbf{W}_2$ is chosen as the orthogonal basis of the null space of $\mathbf{h}_{SR}$, i.e., $\mathbf{W}_2 = null\left(\mathbf{h}_{SR}^H\right)$ and $\mathbf{W}_2 \in \mathbb{C}^{N_S \times (N_S-1)}$. We denote α $(0 < \alpha < 1)$ as the ratio of the power of the information signal $x[i]$ to the power of the source node P_S, i.e., $\mathbb{E}\{|x[i]|^2\} = \alpha P_S$, and we have $\sigma_v^2 = (1-\alpha) P_S/(N_S-1)$ due to the equal distribution of transmit power among $N_S - 1$ AN elements. Thus, the received signals at R and E can be expressed respectively as

$$\begin{aligned} y_R[i] &= \mathbf{h}_{SR}^H \mathbf{x}_S[i] + f_{RR} t[i] + n_{R[i]} \\ &= \|\mathbf{h}_{SR}\| x[i] + f_{RR} t[i] + n_R[i], \end{aligned} \tag{2}$$

$$\begin{aligned} y_E[i] &= \mathbf{g}_{SE}^H \mathbf{x}_S[i] + g_{RE} t[i] + n_E[i] \\ &= \mathbf{g}_{SE}^H \mathbf{w}_1 x[i] + \mathbf{g}_{SE}^H \mathbf{W}_2 \mathbf{v} + g_{RE} t[i] + n_E[i], \end{aligned} \tag{3}$$

where $t[i]$ is an information signal re-encoded by R, where $\mathbb{E}\left[|t[i]|^2\right] = P_R$, $n_R[i]$ and $n_E[i]$ are the AWGNs received by R and E, respectively.

Since R knows its own forwarding signal, the SIC techniques can be used to reduce the effects of SI at R. After incomplete SIC, the received signal at R can be expressed as

$$\begin{aligned} \hat{y}_R[i] &= \mathbf{h}_{SR}^H \mathbf{x}_S[i] + \hat{f}_{RR} t[i] + n_R[i] \\ &= \|\mathbf{h}_{SR}\| x[i] + \hat{f}_{RR} t[i] + n_R[i], \end{aligned} \tag{4}$$

where $\hat{f}_{RR}$ models the residual SI channel owing to the incomplete SIC, $|\hat{f}_{RR}|^2$ is exponentially distributed with mean $1/K$, which is a key parameter related to the strength of SIC [14]. The forwarding signal at R can be expressed as

$$t[i] = \sqrt{\frac{P_R}{P_S}} x[i-\tau], \tag{5}$$

where τ denotes the time delay generated by the relay when decoding the received signal.

The destination node adopts the maximal ratio combining (MRC) for reception, and the combining vector is $\mathbf{h}_{RD}^H/\|\mathbf{h}_{RD}\|$. Thus, the received signals at D can be expressed as

$$\begin{aligned} y_D[i] &= \frac{\mathbf{h}_{RD}^H}{\|\mathbf{h}_{RD}\|} \mathbf{h}_{RD} t[i] + n_D[i] \\ &= \|\mathbf{h}_{RD}\| t[i] + n_D[i], \end{aligned} \tag{6}$$

where $n_D[i]$ is the AWGN received by D.

From (4) and (6), the instantaneous SINRs of channel $S \rightarrow R$ and $R \rightarrow D$ can be written respectively as

$$\gamma_{SR} = \frac{\alpha P_S \|\mathbf{h}_{SR}\|^2}{|\hat{f}_{RR}|^2 P_R + 1}, \tag{7}$$

$$\gamma_{RD} = \|\mathbf{h}_{RD}\|^2 P_R. \tag{8}$$

Under the assumption that R adopts the fixed DF strategy [15], [16], the received SNR at D can be expressed as

$$\gamma_D = \min\{\gamma_{SR}, \gamma_{RD}\}. \tag{9}$$

Let us assume that the eavesdropper node intends to decode the signal from the source node, seeing other terms as interference and noise [17]. From (3), the received SINR at E can be written as

$$\gamma_E = \frac{\alpha P_S \gamma_1}{a\gamma_2 + \gamma_3 P_R + 1}, \tag{10}$$

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

Note that γ_{SR}, γ_{RD}, and γ_i for $i = 1, 2, 3$ are independent with each other. Since each element of $\mathbf{h}_{SR}$, $\mathbf{h}_{RD}$, $\mathbf{g}_{SE}$, g_{RE} and f_{RR} follows the i.i.d. complex Gaussian distribution with zero mean and unit variance, $\|\mathbf{h}_{RD}\|^2$, γ_{RD} and γ_2 follow the Gamma distribution, i.e., $\|\mathbf{h}_{RD}\|^2 \sim \Gamma(N_S, 1)$, $\gamma_{\mathrm{RD}} \sim \Gamma(N_D, 1/P_R)$, $\gamma_2 \sim \Gamma(N_S - 1, 1)$. Meanwhile, $|f_{RR}|^2$ and γ_i for $i = 1, 3$ follow the exponential distribution with unit expectation, and we denote that the general expression of exponential distribution is $E(\lambda)$.

Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.

III. Ergodic Achievable Secrecy Rate Analysis

In this section, we analyze the EASR of the FD relaying transmission system. In the considered model, the secrecy capacity can be expressed as $C_S = [C_D - C_E]^+$, where $[x]^+ \triangleq \max\{0, x\}$, C_D and C_E are the mutual information of the legitimate channel and the eavesdropping channel, respectively, and can be given by $C_D = \log_2(1+\gamma_D)$ and $C_E = \log_2(1+\gamma_E)$ in our considered system. The ergodic secrecy capacity is defined as the rate below which any average secure communication rate is achievable and can be formulated under block fading channels as [18]

$$\begin{aligned}\mathbb{E}[C_S] &= \int_0^\infty \int_0^\infty [C_D - C_E]^+ f(\gamma_D) f(\gamma_E)\, d\gamma_D d\gamma_E \\ &= \mathbb{E}\left[[C_D - C_E]^+\right]. \end{aligned} \tag{11}$$

However, the exact evaluation of (11) appears to be intractable for our transmission model. Alternatively, we focus our analysis on a lower bound of (11), expressed as

$$\mathbb{E}[C_S] \geq [\mathbb{E}[C_D] - \mathbb{E}[C_E]]^+ \triangleq \overline{C}_S, \tag{12}$$

which is also called the ergodic achievable secrecy rate (EASR).

A. EASR Analysis for Any Values of Antenna Number

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

Lemma 1: The approximate ergodic capacity of the legitimate channel is expressed as

$$\mathbb{E}[C_D] \approx \frac{1}{\ln 2} \sum_{i=1}^{q} \omega_i \Phi(z_i), \tag{13}$$

where q denotes the number of points used to approximate the integral, z_i $(i = 0, 1, ..., q)$ is the i-th root of the Laguerre polynomial $\mathcal{L}_q(z)$ and ω_i which does not depend on $\Phi(z)$ is the i-th weight given by

$$\omega_i = \frac{z_i}{[(q+1)\mathcal{L}_{q+1}(z_i)]^2}. \tag{14}$$

Note that both z_i and ω_i can be calculated efficiently using the algorithm provided in [19]. Hence, we can use (13) to represent the approximate closed-form expression of $\mathbb{E}[C_D]$.

Proof: Applying the change of base formula for logarithm, we can formulate $\mathbb{E}[C_D]$ as

$$\begin{aligned}\mathbb{E}[C_D] &= \frac{1}{\ln 2}\mathbb{E}[\ln(1+\gamma_D)] \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\gamma_D}(x)}{1+x} dx. \end{aligned} \tag{15}$$

Invoking (7), we obtain the CDF of γ_{SR} as

$$\begin{aligned}F_{\gamma_{SR}}(x) = &\; 1 - K e^{-\frac{x}{\alpha P_S}} \sum_{m=0}^{N_S-1} \sum_{n=0}^{m} \binom{m}{n} \\ &\times \frac{x^m P_R^n (\alpha P_S)^{n+1-m} \Gamma(n+1)}{m! (P_R x + K\alpha P_S)^{n+1}}. \end{aligned} \tag{16}$$

From (8), the CDF of γ_{RD} can be expressed as

$$F_{\gamma_{RD}} = 1 - e^{-\frac{x}{P_R}} \sum_{v=0}^{N_D-1} \frac{1}{v!} \left(\frac{x}{P_R}\right)^v. \tag{17}$$

Based on (16) and (17), 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

$$\begin{aligned}F_{\gamma_D}(x) &= 1 - [1 - F_{\gamma_{SR}}(x)][1 - F_{\gamma_{RD}}(x)] \\ &= 1 - K e^{-\left(\frac{1}{\alpha P_S} + \frac{1}{P_R}\right)x} \sum_{m=0}^{N_S-1} \sum_{n=0}^{m} \sum_{v=0}^{N_D-1} \binom{m}{n} \\ &\quad \times \frac{x^{m+v} P_R^{n-v} (\alpha P_S)^{n+1-m} \Gamma(n+1)}{m! v! (P_R x + K\alpha P_S)^{n+1}}. \end{aligned} \tag{18}$$

Substituting (18) into (15) yields the half closed-form expression of $\mathbb{E}[C_D]$ as follow

$$\mathbb{E}[C_D] = \frac{1}{\ln 2} \int_0^{+\infty} e^{-x} \Phi(x)\, dx, \tag{19}$$

where

$$\begin{aligned}\Phi(x) = &\sum_{m=0}^{N_S-1} \sum_{n=0}^{m} \sum_{v=0}^{N_D-1} \binom{m}{n} \\ &\times \frac{K x^{m+v} P_R^{n-v} (\alpha P_S)^{n+1-m} \Gamma(n+1)}{m! v! (P_R x + K\alpha\vartheta P_S)^{n+1} (\vartheta + x) \vartheta^{m+v-n-1}}, \end{aligned} \tag{20}$$

where $\vartheta = 1/(\alpha P_S) + 1/P_R$.

The integral in (19) can not be further reduced to a closed form. As such, we resort to the Gauss-Laguerre quadrature (GLQ) method to solve it [20]. By the rules of GLQ method, (13) can be obtained. ■

Lemma 2: The approximate ergodic capacity of the eavesdropping channel is expressed as

$$\mathbb{E}[C_E] \approx \frac{1}{\ln 2} \sum_{i=1}^{q} \omega_i \mathcal{H}(z_i), \tag{21}$$

where

$$\begin{aligned}\mathcal{H}(z_i) = &\frac{(N_S - 1)^{N_S-1} (\alpha P_S)^{N_S} e^{\left(1 - \frac{1}{\alpha P_S}\right)x}}{(1+x)(\alpha P_S + P_R x)} \\ &\times \frac{1}{[\alpha P_S (N_S - 1) + (1-\alpha) P_S x]^{N_S-1}}. \end{aligned} \tag{22}$$

Proof: The derivation is similar to the proof of (13).

Invoking (10), the CDF of γ_E can be written as

$$\begin{aligned}F_{\gamma_E}(x) = 1 - &\frac{(N_S - 1)^{N_S-1} (\alpha P_S)^{N_S} e^{-\frac{x}{\alpha P_S}}}{(\alpha P_S + P_R x)} \\ &\times \frac{1}{[\alpha P_S (N_S - 1) + (1-\alpha) P_S x]^{N_S-1}}. \end{aligned} \tag{23}$$

Applying the change of base formula for logarithm, we can formulate $\mathbb{E}[C_E]$ as

$$\begin{aligned}\mathbb{E}[C_E] &= \frac{1}{\ln 2}\mathbb{E}[\ln(1+\gamma_E)] \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\gamma_E}(x)}{1+x} dx. \end{aligned} \tag{24}$$

Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.

Substituting (23) into (24) yields the half closed-form expression of $\mathbb{E}\left[C_E\right]$ as follow

$$\mathbb{E}\left[C_E\right] = \frac{1}{\ln 2}\int_0^{+\infty} e^{-x}\mathcal{H}\left(x\right)dx. \tag{25}$$

We note that the exact closed-form expression of the integral in (25) is mathematically intractable. Fortunately, by applying the GLQ method, (21) can be obtained. ∎

Finally, from (12), (13) and (21), the approximate closed-form EASR for any values of antenna number can be written as

$$\overline{C}_S \approx \frac{1}{\ln 2}\left[\sum_{i=1}^{q}\omega_i\Phi\left(z_i\right) - \sum_{i=1}^{q}\omega_i\mathcal{H}\left(z_i\right)\right]^+. \tag{26}$$

B. EASR Analysis for Large-scale Antennas Array

Theorem 1: As $N_S \to \infty$, $N_D \to \infty$, the EASR for the FD DF relaying secure communication system can be expressed as

$$\overline{C}_S|_{\text{large}} = \left\{\mathbb{E}\left[C_D\right]|_{\text{large}} - \mathbb{E}\left[C_E\right]|_{\text{large}}\right\}^+. \tag{27}$$

where

$$\begin{aligned}\mathbb{E}\left[C_D\right]|_{\text{large}} = & \tfrac{1}{\ln 2}\Big\{\ln\left(1+\Omega\right) - e^{\frac{K}{P_R}}\Big[\Gamma\left(0, \tfrac{K\alpha N_S P_S}{P_R\Omega}\right) \\ & -e^{\frac{K\alpha N_S P_S}{P_R}}\Gamma\left(0, \tfrac{K\alpha N_S P_S}{P_R}\left(1+\tfrac{1}{\Omega}\right)\right)\Big]\Big\},\end{aligned} \tag{28}$$

$$\begin{aligned}\mathbb{E}\left[C_E\right]|_{\text{large}} = & \tfrac{\alpha P_S}{\ln 2\left(\alpha P_S - P_R\right)}\Big[e^{\frac{(1-\alpha)P_S+1}{P_R}}\text{Ei}\left(-\tfrac{(1-\alpha)P_S+1}{P_R}\right) \\ & -e^{\frac{(1-\alpha)P_S+1}{\alpha P_S}}\text{Ei}\left(-\tfrac{(1-\alpha)P_S+1}{\alpha P_S}\right)\Big],\end{aligned} \tag{29}$$

where $\Omega = \min\left\{\alpha N_S P_S, N_D P_R\right\}$, $\Gamma\left(\cdot,\cdot\right)$ denotes the incomplete Gamma function, $\text{Ei}(\cdot)$ is the exponential integral function.

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

$$\begin{aligned}\gamma_{SR} &= \frac{\alpha P_S\left\|\mathbf{h}_{SR}\right\|^2}{|\hat{f}_{RR}|^2 P_R + 1} = \frac{\alpha P_S\sum_{i=1}^{N_S}|h_{iR}|^2}{|\hat{f}|^2 P_R + 1} \\ &\approx \frac{\alpha N_S P_S\mathbb{E}\left[|h_{iR}|^2\right]}{|\hat{f}_{RR}|^2 P_R + 1}.\end{aligned} \tag{30}$$

Since $|h_{iR}|^2$ follows the exponential distribution with unit mean, i.e., $\mathbb{E}\left[|h_{iR}|^2\right] = 1$, we have

$$\gamma_{SR} \approx \frac{\alpha N_S P_S}{|\hat{f}_{RR}|^2 P_R + 1}. \tag{31}$$

Similarly, $\gamma_{RD} \approx N_D P_R$, $\gamma_2 \approx N_S - 1$.

Under the assumption of large-scale antennas array, the ergodic capacity of the legitimate channel can be written as

$$\mathbb{E}\left[C_D\right]|_{\text{large}} = \frac{1}{\ln 2}\int_0^{\infty}\frac{1 - F_{\gamma_D|\text{large}}\left(x\right)}{1+x}dx. \tag{32}$$

The CDF of $\gamma_D|_{\text{large}}$ is as follow

$$\begin{aligned}F_{\gamma_D|\text{large}}\left(x\right) &= \Pr\left[\min\left(\frac{\alpha N_S P_S}{|\hat{f}_{RR}|^2 P_R + 1}, N_D P_R\right) \le x\right] \\ &= 1 - \left[1 - \Pr\left(\frac{\alpha N_S P_S}{|\hat{f}_{RR}|^2 P_R + 1} \le x\right)\right] \\ &\quad \times\left[1 - \Pr\left(N_D P_R \le x\right)\right] \\ &= \begin{cases} 1 & , x \ge N_D P_R \\ \Pr\left(\frac{\frac{\alpha N_S P_S}{x} - 1}{P_R} \le |\hat{f}_{RR}|^2\right) & , x < N_D P_R \end{cases}.\end{aligned} \tag{33}$$

When $x < N_D P_R$ and $x \ge \alpha N_S P_S$, the following equation holds true

$$\Pr\left(\frac{\frac{\alpha N_S P_S}{x} - 1}{P_R} \le |\hat{f}_{RR}|^2\right) = 1. \tag{34}$$

When $x < N_D P_R$ and $x < \alpha N_S P_S$, applying $|\hat{f}_{RR}|^2 \sim \text{E}\left(K\right)$, we obtain

$$\Pr\left(\frac{\frac{\alpha N_S P_S}{x} - 1}{P_R} \le |\hat{f}_{RR}|^2\right) = e^{-K\frac{\alpha N_S P_S - x}{P_R x}}. \tag{35}$$

After some simple mathematical operations, the CDF of $\gamma_D|_{\text{large}}$ can be expressed as

$$F_{\gamma_D|\text{large}}\left(x\right) = \begin{cases} 1 & , x \ge \Omega \\ e^{-K\frac{\alpha N_S P_S - x}{P_R x}} & , x < \Omega \end{cases}. \tag{36}$$

Substituting (36) into (32) yields (28). By a similar derivation procedure as above, we can attain (29). ∎

IV. Numerical Results and Discussion

In this section, we show the numerical results to validate the derived analytical expressions by using Monte Carlo simulations. In all figures, without other indecation, the FD curves are the analytical results of (26) by setting $q = 300$, the simulation points are the exact Monte Carlo simulation results, and are the average values obtained by 10^6 random channel realizations.

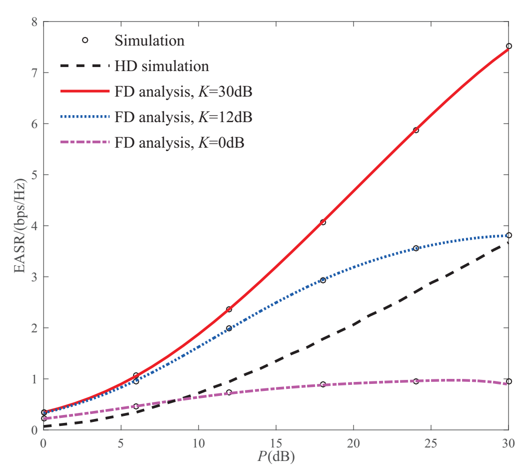

Figure 2. EASR comparison between FD scheme in this paper and traditional HD scheme ($N_S = 2$, $N_D = 4$, $\alpha = 0.5$).

Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.

Fig. 2 compares the EASR of the FD and the traditional half-duplex (HD) modes [7] under the same total transmit power P. The HD curve is the Monte Carlo simulation of the traditional dual-hop HD mode. For the fairness of the comparison, we set the total power of every time slot for the two transmission modes as a constant P, where $P_S + P_R = P$. In every time slot of the FD mode and the second time slot of the HD mode, the power allocated to S and R are all half of P. Note that the source transmits only random AN and the relay forward information simultaneously in the second time slot of the HD mode, which is different from [7]. In the first time slot of HD mode, since R works in the receive mode, we allocate all the power P to S. We can see that the approximate closed-form expression of EASR (26) matches well with the Monte Carlo simulation results, which proves the feasibility of GLQ method in this paper. When $K = 0$dB, i.e., without SIC, the performance of EASR in the FD mode is not always better than that of the HD mode, especially in the middle to high level of total transmit power. When $K = 12$dB, the EASR of FD mode is better than that of HD mode for various total power of interest. When $K = 30$dB, the EASR of the FD mode is almost twice than that of HD mode for various total power of interest, revealing the superiority of the FD mode and the necessity and importance of SIC.

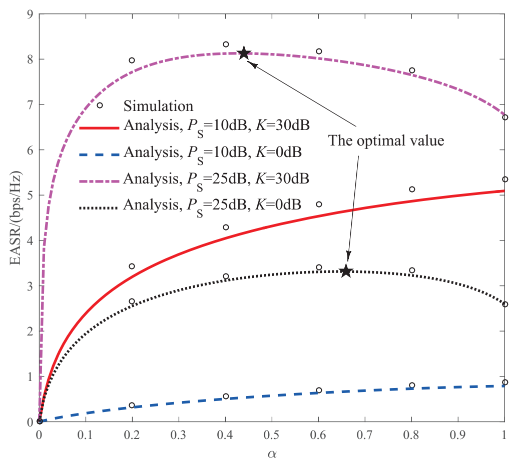

Figure 3. EASR for ANP versus α for different P_S and K ($N_S = N_D = 6$, $P_R = 20$dB).

Fig. 3 shows the EASR performance versus the PA factor α for different P_S and K. From this figure, we can see that, the impact of the SI on EASR is significant. When P_S approaches the value of P_R, such as $P_S = 25$dB, there exits an optimal PA factor in the the range of (0,1), since the dual hop of relay link is balanced and the adjustment of α has a distinctive effect on EASR. The optimal PA factor decreases when K increases from 0dB to 30dB. This is because that, with the increase of the degree of SIC, the ergodic capacity of the $S \to R$ link increases, and the source does not need to allocate too much power to the useful information. Meanwhile, with the decrease of PA factor, the power allocated to the AN increases, further suppressing the ergodic capacity of eavesdropping channel. However, when P_S is much smaller than P_R, such as $P_S = 10$dB, all power should be allocated to useful information for various values of K, since the capacity of the legitimate link is constrained by the first hop.

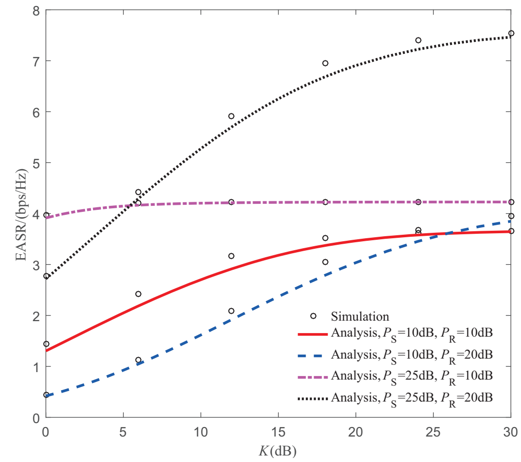

Figure 4. EASR for ANP versus K for different P_S and P_R ($N_S = N_D = 4$, $\alpha = 0.5$).

Fig. 4 shows the EASR performance as function of K for different P_S and P_R. It is observed that with the increase of the degree of SIC, the EASR increases for all transmit power settings. When the degree of SIC is strong and P_S is low, upgrading P_R appropriately can improve EASR. When the degree of SIC is moderate or weak and P_S is low, P_R should not be too high. When the degree of SIC is moderate or strong and P_S is high, it is better to make P_R higher. It is worth noting that, for moderate-to-high P_S and lower P_R, the impact of the SI on EASR can be negligible.

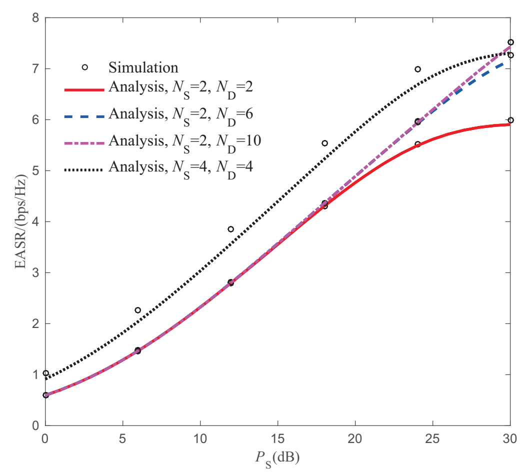

Figure 5. EASR for ANP versus P_S for different N_S and N_D ($\alpha = 0.5$, $P_R = 20$dB, $K = 20$dB).

Fig. 5 shows the EASR performance versus P_S for different N_S and N_D. When P_S is moderate or low and N_S is a constant, EASR is nearly not affected by N_D due to the DF protocol. Increasing N_S for comparatively smaller N_S or increasing N_D for high P_S will effectively increase EASR.

Fig. 6 confirms the correctness of (27). Comparing Fig. 3 and Fig. 6, we observed that large-scale antenna technology can significantly improve the EASR performance. With the

Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.

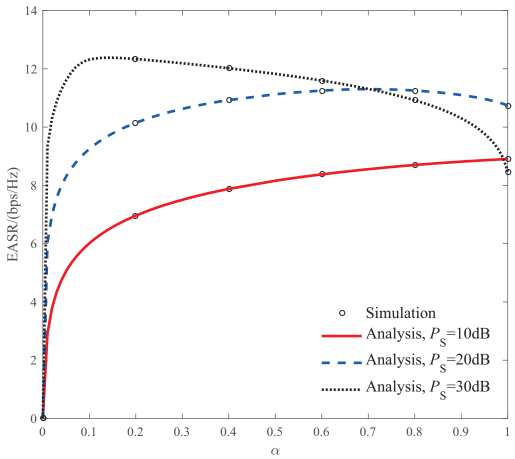

Figure 6. EASR for large-scale antennas array versus α for different P_S ($N_S = N_D = 100$, $K = 20$dB, $P_R = 18$dB).

increase of P_S, the optimal PA factor decreases. This is because, in the moderate-to-high level of P_S, the SINR of the eavesdropping channel is high, and S should allocate more power to the AN to ensure the security of system.

V. Conclusion

In this work, an ANP combined with FD scheme is utilized in the DF relay secure communication system to promote the secrecy performance. We derived the approximate closed-form expression of EASR for any values of antenna number. Furthermore, the exact closed-form expression of EASR with large-scale antennas array was derived. Simulation results have demonstrated that GLQ method is valid to approximate the integral in this paper. Based on the theoretical analysis and simulation results, the influence of the system parameters on the performance of EASR is described and analyzed, and the effectiveness of the proposed ANP combined with full-duplex scheme is verified.

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, Aug. 2016.

[2] Y. Yuan, R. Zhao, H. Lin, and A. Liu, "Secrecy outage probability of cognitive decode-and-forward relay networks," in *Proc. Int. Conf. Commun. (ICC)*, May. 2016, pp. 260–265.

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

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

[5] 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, Jul. 2011.

[6] 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, Mar. 2014.

[7] 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.

[8] 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.

[9] 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.

[10] 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, Jul. 2011.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] J. N. Laneman, D. N. 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.

[16] 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.

[17] 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. Topics Signal Process.*, vol. 10, no. 8, pp. 1359–1374, Dec. 2016.

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

[19] G. W. Recktenwald, *Numerical Methods with MATLAB: Implementation and Application*, 2000.

[20] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Antenna switching for security enhancement in full-duplex wiretap channels," in *Proc. GLOBECOM Workshops (GC Wkshps)*, 2014, pp. 1308–1313.

Authorized licensed use limited to: KINGS COLLEGE LONDON. Downloaded on October 31,2022 at 17:12:25 UTC from IEEE Xplore. Restrictions apply.