Large-scale Antennas Analysis of Untrusted Relay System with Cooperative Jamming

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

***Abstract*—In Rayleigh fading channels, a novel full-duplex destination jamming with optimal antenna selection (FDJ-OAS) scheme is proposed to improve the secrecy performance of the untrusted relay system with multiple-antenna destination. The traditional half-duplex destination jamming scheme and the non-jamming scheme both combined with OAS are presented to compare with FDJ-OAS. The approximate closed-form expressions of ergodic achievable secrecy rate and optimal power allocation factor for FDJ-OAS are significantly derived in the large-scale antennas analysis. Furthermore, simulation results show that, the analytical curves match well with the simulation curves, and the FDJ-OAS is superior to the other two schemes.**

***Index Terms*—Destination based jamming, full-duplex, antenna selection, ergodic achievable secrecy rate, power allocation.**

I. Introduction

Cooperating relays can improve the performance of secure wireless communications by utilizing the complex spatial and time-varying characteristics of wireless channels [1], [2]. In some cases, the cooperative relay may be untrustworthy, which means the relay may acts as an eavesdropper and overhears the message from the source, when it helps the communication between the source and the destination [3]-[7]. Since the decode-and-forward protocol applied at the relay cannot make the untrusted relay system to obtain positive secrecy rate, the relay usually applies the amplify-and-forward (AF) protocol to retransmit the information [5]. According to the definition of secrecy rate, a positive secrecy rate for an untrusted AF relay system without cooperative jamming is not achievable, in the absence of a direct link [3], [4]. In [5], according to the destination based jamming (DBJ) scheme, the interception of untrusted relay is interfered by the noise signal sent by the destination, while this noise can be cancelled from the received signal of the destination, resulting higher secrecy rate. The instantaneous secrecy rate with optimal power allocation (PA) scheme was derived in [6], [8], where large-scale antennas of the source and the destination cases were considered to maximize the ergodic secrecy capacity. When the untrusted relay can harvest wireless energy, the jamming signal from the destination can not only interfere the reception of relay but also provide energy to relay, to improve the secrecy performance [7]. However, the existing DBJ used in untrusted relay system is focused on the half-duplex (HD) mode, which is inferior in terms of secrecy rate to the full-duplex (FD) mode, and FD technology has attracted much attention [9]-[12]. In addition, the self-interference (SI) between the transmit antenna and receive antenna is the key factor preventing the performance improvement of FD node. Fortunately, by using latest SI cancellation (SIC) technologies, i.e., propagation-domain, analog-circuit-domain, and digital-domain approaches [13], [14], SI can be sufficiently suppressed to a low level and made negligible [15].

In this paper, we propose a novel full-duplex destination jamming (FDJ) with optimal antenna selection (OAS) scheme in the untrusted relay system. The main contributions in this paper are summarized as follows:

- With a large-scale antenna array at the destination, the corresponding closed-form expression of ergodic achievable secrecy rate (EASR) is derived. Furthermore, for comparison reason, the other two schemes, i.e., half-duplex destination jamming and non-jamming, both combined with OAS, are mentioned, and the EASR for two schemes are also derived in the large-scale antennas. Simulation results show that, the FDJ-OAS is superior to the other two schemes.
- To further improve the secrecy performance of the untrusted relay system, we derived the optimal PA between the information signal and artificial noise to maximize the secrecy capacity for FDJ-OAS in the large-scale antennas. The analysis results indicate that in the high SNR regime, the optimal PA factor is a constant, which is determined by the channel gains of the source-relay and relay-destination links and the number of antennas. In the low SNR regime, all the power should be allocated to the information signal for FDJ-OAS. Monte-Carlo simulations in MATLAB verify the analytical results and show that the proposed PA scheme can maximize instantaneous secrecy rate even for a finite number of antennas at the destination.

Notation 1: The superscript $(\cdot)^T$ denotes the transpose. The mathematical expectation is denoted by $\mathbb{E}[\cdot]$. We also use $[x]^+$ to denote $\max\{0, x\}$ for a real number x. Bold lower case letters denote vectors, e.g., $\mathbf{h}$.

II. System Model and Transmission Schemes

A. System Model

As shown in Fig. 1, we investigate a two-hop relay communication system, where a source node S transmits the message to a destination node D with the assistant of an AF untrusted relay node R, and a direct link between S and D is assumed to be existent. The destination is equipped with N antennas and operates in the FD mode, and other nodes are equipped with a single antenna and operate in the HD mode. All channels are modeled to be quasi-static with Rayleigh channels, i.e.,

978-3-901882-98-2

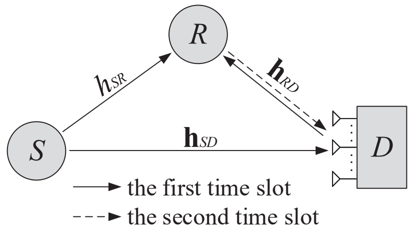


Figure 1: The dual-hop untrusted relaying system.

remain constant during two transmission time slots, and have perfect channel reciprocity. The channel coefficients for the links between S and R, R and D, and S and D are denoted by h_{SR}, $\mathbf{h}_{RD} = [h_{RD,1}, h_{RD,2}, \cdots, h_{RD,N}]^T$, and $\mathbf{h}_{SD} = [h_{SD,1}, h_{SD,2}, \cdots, h_{SD,N}]^T$ respectively, with the average channel power gains represented respectively as $\mathbb{E}\left[|h_{SR}|^2\right] = \Omega_{SR}$, $\mathbb{E}\left[|h_{RD,i}|^2\right] = \Omega_{RD}$, and $\mathbb{E}\left[|h_{SD,i}|^2\right] = \Omega_{SD}$, $i \in \{1, \cdots, N\}$. The total transmit power of the system in each time slot is constrained by P [9], and the transmit power of S and D is denoted by $P_S = \alpha P$ and $P_D = (1-\alpha) P$ respectively, where α is the PA factor with $0 \leq \alpha \leq 1$. The received noises at all nodes are assumed to be the additive white Gaussian noises (AWGNs) with variance N_0.

B. Full-duplex Destination Jamming

The entire transmission process is accomplished in two time slots. In order to prevent the relay from intercepting the useful information, in the first time slot, S broadcasts the signal to R and D, and simultaneously D transmits the artificial noise to interfere the reception of the relay. In order to further promote the secrecy performance of low implementation complexity, a novel transmit and receive antenna selection strategy applied at D is presented in this paper, which will be described and elaborated in detail in the following subsection. The selected transmit and receive antennas at D are denoted by i^* and j^* respectively, $i^*, j^* \in \{1, \cdots, N\}, i^* \neq j^*$. In the second time slot, R amplifies and forwards the received signal to D with the power amplification factor β, $\beta^2 = 1/\left(P_S |h_{SR}|^2 + P_D |h_{RD,i^*}|^2 + N_0\right)$. Assume that D can eliminate it from the received signal. Additionally, since the signals transmitted from S and R to D through two different time slots respectively, D can adopt the maximum ratio combining scheme for reception to maximize the received SNR. Thus, the received SNR at R and D are expressed respectively as

$$\gamma_R = \frac{\alpha\gamma_{SR}}{(1-\alpha)\gamma_{RD} + 1}, \tag{1}$$

$$\gamma_D = \frac{\alpha\gamma_{SD}}{(1-\alpha)\gamma_{SI} + 1} + \frac{\alpha\gamma_{SR}\gamma_{RD}}{\alpha\gamma_{SR} + (2-\alpha)\gamma_{RD} + 1}, \tag{2}$$

where $\gamma_{SR} = \rho |h_{SR}|^2$, $\gamma_{RD} = \rho |h_{RD,i^*}|^2$, $\gamma_{SD} = \rho |h_{SD,j^*}|^2$, $\gamma_{SI} = \rho |h_{SI}|^2$, h_{SI} denotes the SI channel coefficient, and $\rho = P/N_0$ is the transmit SNR. Considering that the SI can be suppressed to the noise level using SIC technologies [13], [14], which have been applied in [11], [15], [16]. We assume that the residual SI term γ_{SI} has little influence on γ_D and can be ignored. For the feasibility of analysis, so (2) can be approximated by

$$\gamma_D \simeq \alpha\gamma_{SD} + \min\left\{\frac{\alpha}{2-\alpha}\gamma_{SR}, \gamma_{RD}\right\}. \tag{3}$$

In our system, since the relay is untrusted, according to definition of the instantaneous secrecy capacity, combining (1) and (3), the secrecy capacity for our considered system can be described as

$$C_S = [C_D - C_R]^+$$
$$= \frac{1}{2}\left[\log_2\left(\frac{1 + \alpha\gamma_{SD} + \min\left\{\frac{\alpha}{2-\alpha}\gamma_{SR}, \gamma_{RD}\right\}}{1 + \frac{\alpha\gamma_{SR}}{(1-\alpha)\gamma_{RD}+1}}\right)\right]^+, \tag{4}$$

where $C_D = \frac{1}{2}\log_2(1+\gamma_D)$ and $C_R = \frac{1}{2}\log_2(1+\gamma_R)$ are the capacity of the legitimate channel and the eavesdropping channel, respectively.

C. Optimal Antenna Selection

Assume that the number of the switched separate-antennas at D is N [10], [17]. According to (4), we can find that the instantaneous secrecy capacity is proportional to the values of γ_{SD} and γ_{RD}. Additionally, once the transmit/receive antenna is selected, the receive/transmit antenna can only be selected from the remaining $N-1$ antennas. Considering the above, we present a full-duplex destination jamming with optimal antenna selection (FDJ-OAS) scheme in the following. The transmit/receive antenna pair can be decided by selecting one transmit antenna from $\widehat{N}$ antennas to maximize the channel gain of the $R-D$ link, and simultaneously selecting one receive antenna from $\widetilde{N}$ antennas to maximize the channel gain of the $S-D$ link, where $\left(\widehat{N}, \widetilde{N}\right) \in \{(N, N-1), (N-1, N)\}$. The indexes of the selected transmit and receive antennas are denoted respectively as

$$\hat{i}^* = \underset{1 \leq i \leq \widehat{N}}{\arg\max}\left\{|h_{RD,i}|^2\right\}, \tag{5}$$

$$\tilde{j}^* = \underset{1 \leq j \leq \widetilde{N}}{\arg\max}\left\{|h_{SD,j}|^2\right\}. \tag{6}$$

Based on the transmit/receive antenna pair selection (5) and (6), the corresponding secrecy capacity achieved by (4) is denoted as C_{S1}^{FD} for $\widehat{N} = N$ and $\widetilde{N} = N-1$, and C_{S2}^{FD} for $\widehat{N} = N-1$ and $\widetilde{N} = N$, respectively. To maximize the secrecy capacity, the optimal antenna indexes and the optimal secrecy capacity by using FDJ-OAS scheme can be given by

$$\left(i_1^*, j_1^*, C_{S,max}^{\mathrm{FDJ}}\right) = \underset{\substack{1 \leq i \leq \widehat{N}, 1 \leq j \leq \widetilde{N}, i \neq j \\ (\widehat{N}, \widetilde{N}) \in \{(N, N-1), (N-1, N)\}}}{\arg\max}\left\{C_{S1}^{\mathrm{FDJ}}, C_{S2}^{\mathrm{FDJ}}\right\}, \tag{7}$$

where C_{S1}^{FDJ} and C_{S2}^{FDJ} are given in (4) by replacing γ_{RD} and γ_{SD} with $\gamma_{RD}^{\mathrm{FDJ}} = \rho\left|h_{RD,\hat{i}^*}\right|^2$ and $\gamma_{SD}^{\mathrm{FDJ}} = \rho\left|h_{SD,\tilde{j}^*}\right|^2$ respectively.

D. Two half-duplex schemes

In the first time slot, D can only send the jamming signal to interfere the reception of R, but cannot receive simultaneously. In the second time slot, R forwards the amplified signal to D. This transmission protocol is called the DBJ, which was investigated in [5], [6]. In addition, D does not transmit any jamming signal, but receives the signal from S directly in the first time slot. This transmission protocol is called the non-jamming (NJ), which was investigated in [3]. To maximize the received SNR, we denote respectively two schemes as the half-duplex destination jamming with optimal antenna selection (HDJ-OAS) and the non-jamming with optimal antenna selection (NJ-OAS) schemes.

III. Ergodic Achievable Secrecy Rate Analysis of the Large-scale antennas

In this section, we will investigate the EASR for FDJ-OAS. The ergodic secrecy capacity (ESC) describes the rate below which any average secure communication rate is achievable [18], and can be expressed for our considered system as

$$\mathbb{E}\left\{C_S\right\} = \mathbb{E}\left\{\left[C_D - C_R\right]^+\right\} \geq \left[\mathbb{E}\left\{C_D\right\} - \mathbb{E}\left\{C_R\right\}\right]^+ \triangleq \overline{C}_S, \tag{8}$$

where the lower bound of the ESC $\overline{C}_S$ comes from the Jensen's inequality, and is called the EASR. Since massive MIMO can improve the system capacity considerably and has become the enabling technology in the 5G communication systems, in the following, we investigate the asymptotic EASR performance for the FDJ-OAS scheme as the number of antennas at destination tends to infinity.

For the FDJ-OAS scheme, as $N \to \infty$, we have $\widehat{N} \simeq \widetilde{N} \simeq N$, which means there is no difference between two antennas pair selection orders, i.e., $C_{S1}^{\mathrm{FDJ}} = C_{S2}^{\mathrm{FDJ}}$. It can be deduced that, the EASR of the FDJ-OAS scheme for the destination with large-scale antennas can be given by

$$\overline{C}_{S,\infty}^{\mathrm{FDJ}} = \left[\mathbb{E}\left\{C_D^{\mathrm{FDJ}}\right\} - \mathbb{E}\left\{C_R^{\mathrm{FDJ}}\right\}\right]^+. \tag{9}$$

In addition, according to the results in [19], as $N \to \infty$, it holds true that $\max\limits_{1 \leq i \leq N}\left\{\left|h_{RD,i}\right|^2\right\} \simeq \Omega_{RD} \ln N + \mathcal{O}\left(\Omega_{RD} \ln\ln N\right)$ and $\max\limits_{1 \leq j \leq N}\left\{\left|h_{SD,j}\right|^2\right\} \simeq \Omega_{SD} \ln N + \mathcal{O}\left(\Omega_{SD} \ln\ln N\right)$. To further improve the secrecy capacity of FDJ scheme, from (4) as $N \to \infty$, $\frac{\alpha}{2-\alpha}\gamma_{SR} \ll \overline{\gamma}_{RD} \ln N$ for $0 \leq \alpha \leq 1$, we have

$$C_{S,\infty}^{\mathrm{FDJ}} = \frac{1}{2}\log_2\left[\frac{1 + \alpha\overline{\gamma}_{SD}\ln N + \frac{\alpha}{2-\alpha}\gamma_{SR}}{1 + \frac{\alpha\gamma_{SR}}{(1-\alpha)\overline{\gamma}_{RD}\ln N + 1}}\right]^+. \tag{10}$$

So based on (10), the ergodic capacity of the legitimate channel and the eavesdropping channel in (9) can be expressed respectively as

$$\mathbb{E}\left\{C_D^{\mathrm{FDJ}}\right\} = \frac{1}{2\ln 2}\mathbb{E}\left\{\ln\left(1 + \alpha\overline{\gamma}_{SD}\ln N + \frac{\alpha}{2-\alpha}\gamma_{SR}\right)\right\}, \tag{11}$$

$$\mathbb{E}\left\{C_R^{\mathrm{FDJ}}\right\} = \frac{1}{2\ln 2}\mathbb{E}\left\{\ln\left(1 + \frac{\alpha\gamma_{SR}}{(1-\alpha)\overline{\gamma}_{RD}\ln N + 1}\right)\right\}. \tag{12}$$

Then, by using [20, Eq.(4.337.1) and Eq.(4.337.2)], the closed-form expressions of (11) and (12) can be given respectively by

$$\mathbb{E}\left\{C_D^{\mathrm{FDJ}}\right\} = \frac{1}{2\ln 2}\left[\ln\left(1 + \alpha\overline{\gamma}_{SD}\ln N\right) - e^{\frac{\alpha\overline{\gamma}_{SD}\ln N + 1}{\frac{\alpha}{2-\alpha}\overline{\gamma}_{SR}}}\right.$$
$$\left.\times\mathbf{Ei}\left(-\frac{\alpha\overline{\gamma}_{SD}\ln N + 1}{\frac{\alpha}{2-\alpha}\overline{\gamma}_{SR}}\right)\right], \tag{13}$$

$$\mathbb{E}\left\{C_R^{\mathrm{FDJ}}\right\} = \frac{e^{\frac{(1-\alpha)\overline{\gamma}_{RD}\ln N + 1}{\alpha\overline{\gamma}_{SR}}}}{-2\ln 2}\mathbf{Ei}\left(\frac{(1-\alpha)\overline{\gamma}_{RD}\ln N + 1}{-\alpha\overline{\gamma}_{SR}}\right), \tag{14}$$

where $\mathbf{Ei}(\cdot)$ is the exponential integral, i.e., $\mathbf{Ei}(x) = \int_{-\infty}^{x} e^t t^{-1} dt$ [20, Eq.(8.211.1)].

In the end, the closed-form expression of the EASR of FDJ-OAS for the case of large-scale antennas is obtained by combining (13), (14), and (9). Furthermore, when $\overline{\gamma}_{SD} = 0$ and $\alpha = 1$, we can obtain the closed-form expressions of the EASR of HDJ-OAS and NJ-OAS for the case of large-scale antennas respectively.

When the number of antennas at D tends to infinity, the transmit power should be carefully allocated between the source and the destination, so the secrecy capacity maximization via power control is presented in the following theorem. Note that as $N \to \infty$, $\frac{\alpha}{2-\alpha}\gamma_{SR} \ll \overline{\gamma}_{SD}\ln N$ for $0 \leq \alpha \leq 1$, thus (10) can be reduced to

$$C_{S,\infty}^{\mathrm{FDJ}} \simeq \frac{1}{2}\log_2\left[\frac{1 + \alpha\overline{\gamma}_{SD}\ln N}{1 + \frac{\alpha\gamma_{SR}}{(1-\alpha)\overline{\gamma}_{RD}\ln N + 1}}\right]^+. \tag{15}$$

Theorem 1: (optimal PA of FDJ-OAS for large N): When $N \to \infty$, the optimal PA factor can be expressed as

$$\alpha^* = \frac{\left(\overline{\gamma}_{RD}\ln N + 1\right)\left[1 - \sqrt{\frac{\gamma_{SR}(\delta + \overline{\gamma}_{RD}\ln N + \overline{\gamma}_{SD}\ln N - \gamma_{SR})}{(\overline{\gamma}_{RD}\ln N + 1)\delta}}\right]}{\overline{\gamma}_{RD}\ln N - \gamma_{SR}}, \tag{16}$$

where $\delta = \overline{\gamma}_{RD}\overline{\gamma}_{SD}\left(\ln N\right)^2$.

Proof: According to (15), we set $\psi(\alpha) = \frac{(1 + \alpha\overline{\gamma}_{SD}\ln N)[(1-\alpha)\overline{\gamma}_{RD}\ln N + 1]}{(1-\alpha)\overline{\gamma}_{RD}\ln N + \alpha\gamma_{SR} + 1}$. The first derivative of $\psi(\alpha)$ w.r.t. α is $\frac{\mathrm{d}\psi(\alpha)}{\mathrm{d}\alpha} = \frac{w(\alpha)}{[\alpha\gamma_{SR} + (1-\alpha)\overline{\gamma}_{RD}\ln N + 1]^2}$, where $w(\alpha) = -\alpha^2\delta\left(\gamma_{SR} - \overline{\gamma}_{RD}\ln N\right) - 2\alpha\delta\left(\overline{\gamma}_{RD}\ln N + 1\right) + \left(\delta + \overline{\gamma}_{SD}\ln N - \gamma_{SR}\right)\left(\overline{\gamma}_{RD}\ln N + 1\right)$, and $\frac{\mathrm{d}w(\alpha)}{\mathrm{d}\alpha} < 0$, so $w(\alpha)$ is a monotonically decreasing function w.r.t. α. It can be shown that $w(0) = \left(\delta + \overline{\gamma}_{SD}\ln N - \gamma_{SR}\right)\left(\overline{\gamma}_{RD}\ln N + 1\right) > 0$ and $w(1) = -\gamma_{SR}\left(\overline{\gamma}_{RD}\ln N + 1\right) - \overline{\gamma}_{SD}\ln N\left(\gamma_{SR}\overline{\gamma}_{RD}\ln N - 1\right) < 0$, such that $w(\alpha) = 0$ has a single root α_1 in the range $0 \leq \alpha \leq 1$. When $0 < \alpha \leq \alpha_1$, we have $w(\alpha) \geq 0$, therefore, $\psi(\alpha)$ is monotonically increasing w.r.t. α. When $\alpha_1 \leq \alpha \leq 1$, we have $w(\alpha) \leq 0$, therefore, $\psi(\alpha)$ is monotonically decreasing w.r.t. α. Thus, the maximal $\psi(\alpha)$ is achieved by $\alpha^* = \alpha_1$. ■

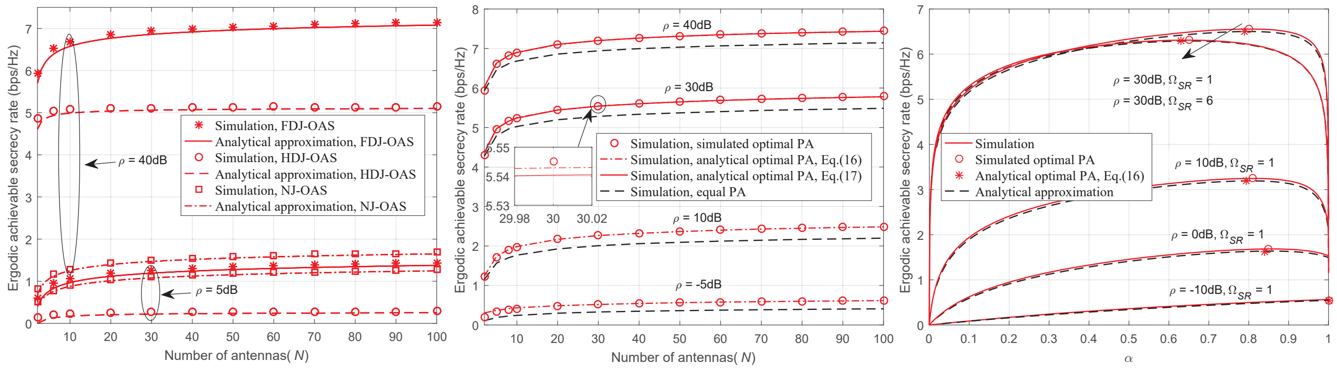
Based on Theorem 1, we provide the optimal PA scheme for the high and low SNR regimes in the following two corollaries.

Corollary 1: (optimal PA of FDJ-OAS for large N and high SNR): As $N \to \infty$, and in the high SNR regime ($\rho \gg 1$), the optimal PA factor of FDJ-OAS is given by

$$\alpha^* = \frac{1}{1 + \sqrt{\eta}}, \tag{17}$$

where $\eta = \frac{\gamma_{SR}}{\overline{\gamma}_{RD}\ln N}$.

Proof: In the high SNR regime, from (16), we can see $\overline{\gamma}_{RD}\ln N \gg 1$ and $\delta \gg \overline{\gamma}_{RD}\ln N + \overline{\gamma}_{SD}\ln N - \gamma_{SR}$, so (17) can be obtained from (16) through asymptotic approximation. ■



(a) Comparison of the EASR for three schemes.

(b) Verification of the proposed PA scheme.

(c) The EASRs for different SNR and Ω_{SR}.

Figure 2: Simulation Results.

Corollary 2: (optimal PA of FDJ-OAS for large N and low SNR): As $N \to \infty$, and in the low SNR regime, the optimal PA factor of FDJ-OAS is given by $\alpha^* = 1$.

Proof: According to the proof of Theorem 1, for low SNR ($\rho \ll 1$) and large N, using high order infinitesimal, we have $\overline{\gamma}_{SD} \ln N > \gamma_{SR}\delta + \gamma_{SR}\left(\overline{\gamma}_{RD} \ln N + 1\right)$, so $\frac{\mathrm{d}\psi(\alpha)}{\mathrm{d}\alpha} > 0$, and $\psi\left(\alpha\right)$ is monotonically increasing w.r.t. α. Thus, the maximal secrecy capacity is achieved by $\alpha^* = 1$. ■

Remark 1: From (17), we see that α^* is a constant only related to η, which is determined by the channel gains of the $S-R$ and $R-D$ links and the number of antennas. For large N, it usually holds true that $\eta \ll 1$, so α approaches 1, which means most power should be allocated for the transmission of useful information. Especially, when R is located close to the source, i.e., large channel gain of the $S-R$ link, the value of α^* decreases, so more power should be allocated for D to transmit artificial noise.

IV. Numerical Results and Discussion

In this section, the theoretical analysis results obtained in the previous section for three transmission schemes are validated through Monte-Carlo simulations in Rayleigh fading channels. The number of Monte-Carlo simulations on the MATLAB platform is 10^6 in all figures. For all the simulations, we assume the AWGN power $N_0 = 1$. In Figs. 2(a)-(b), assume that $\Omega_{SR} = \Omega_{RD} = \Omega_{SD} = 1$.

Fig. 2(a) depicts the Monte-Carlo simulation and analytical results of the EASR for all schemes versus N, with $\alpha = 0.5$. The analytical approximation for FDJ-OAS is obtained by combining (13), (14), and (9). The analytical approximations for HDJ-OAS and NJ-OAS are that for FDJ-OAS by setting $\overline{\gamma}_{SD} = 0$ and $\alpha = 1$ respectively. When N grows large, the EASR of the simulated results matches well with that of analytical approximate results for all schemes. In the low SNR regime, we see that the EASR of FDJ-OAS is close to that of NJ-OAS, and is better than that of HDJ-OAS, indicating that the existence of direct path plays an important role in improving EASR performance. In the high SNR regime, we see that FDJ-OAS and HDJ-OAS can significantly improve the EASR compared with NJ-OAS, since the DBJ strategy can dramatically improve secrecy performance.

Fig. 2(b) shows the EASRs with the Monte-Carlo simulated optimal PA, analytical optimal PA, and equal PA for FDJ-OAS versus N. The simulated optimal PA factor is obtained by the exhaustive search method within $\alpha \in (0, 1)$ with search step 0.01, which can be viewed as the accurate optimal PA factor of FDJ-OAS. The analytical optimal PA factor is obtained by using (16) for general SNR and (17) for high SNR respectively. The equal PA factor refers to $\alpha = 0.5$. We see that the EASR with simulated optimal PA can match well with that with analytical optimal PA, confirming the correctness of Theorem 1 and Corollary 1. Besides, the optimal PA can significantly improve the EASR compared with equal PA for the whole SNR regime, while the transmit power should be carefully allocated to maximize the secrecy capacity.

Fig. 2(c) shows the approximate analytical curves and the simulation curves of EASR as function of the PA factor for FDJ-OAS with $\Omega_{RD} = \Omega_{SD} = 2$, and $N = 500$. We can see that the EASRs with the simulated optimal PA factors match well with that with the analytical optimal PA factors. In the low ρ regime, we can see that the optimal PA factor is close to 1, which confirms the correctness of Corollary 2. In the high ρ regime, the optimal PA factor broadly stays the same, confirming the correctness of Corollary 1. Furthermore, the EASR of FDJ-OAS and the optimal PA factor gradually decrease as the Ω_{SR} grows large, in order to prevent the relay wiretapping more information, so more power should be allocated for the destination D to transmit artificial noise.

V. Conclusion

In this paper, we have investigated the secrecy performance of untrusted relay system based on FDJ in large-scale antennas. The HDJ and NJ schemes were also studied to highlight the superiority of FDJ. And in order to attain more intuitive and meaningful results about the effects of system parameters on the secrecy performance, the asymptotic behavior of EASR and optimal PA factor were analyzed, based on large-scale antennas at the destination. Simulation results have verified the accuracy of the results of mathematical analysis.

Acknowledgement

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.

REFERENCES

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[2] 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.

[3] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jun. 2012.

[4] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[5] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[6] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.

[7] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[8] A. Kuhestani and A. Mohammadi, "Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: resource allocation and performance study," *IET Commun.*, vol. 10, no. 1, pp. 17–23, Jan. 2016.

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

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

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

[12] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[13] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.

[14] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.

[15] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex bob in the MIMO gaussian wiretap channel: Scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.

[16] T.-X. Zheng, Q. Yang, Y. Zhang, H.-M. Wang, and P. Mu, "Secure transmissions in wireless Ad Hoc networks using hybrid half and full duplex receivers," in *Proc. IEEE Int. Conf. on Commun. (ICC)*. IEEE, 2017, pp. 1–6.

[17] M. Zhou, L. Song, Y. Li, and X. Li, "Simultaneous bidirectional link selection in full duplex MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 4052–4062, Jul. 2015.

[18] 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.

[19] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.

[20] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of integrals, series, and products*. 7th ed. Elsevier, 2007.