Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay

Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay

Yang Cao, Nan Zhao, *Senior Member, IEEE,* Gaofeng Pan, *Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* Lisheng Fan, Minglu Jin, *Member, IEEE* and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—In a downlink non-orthogonal multiple access (NOMA) system, the reliable transmission of cell-edge users cannot be guaranteed due to severe channel fading. On the other hand, the presence of eavesdroppers can severely threaten the secure transmission due to the open nature of wireless channel. Thus, a two-user NOMA system assisted by a multi-antenna decode-and-forward relay is considered in this paper, and a two-stage jamming scheme, full-duplex-jamming (FDJam), is proposed to ensure the secure transmission of NOMA users. In the FDJam scheme, using full-duplex, the relay transmits the jamming signal to the eavesdropper while receiving confidential messages in the first stage, and the base station generates the jamming signal in the second stage. Furthermore, we eliminate the self-interference and the jamming signal at the relay and the legitimate node, respectively, through relay beamforming. To measure the secrecy performance, analytical expressions for secrecy outage probability (SOP) are derived for both the cell-center and cell-edge users, and the asymptotic SOP analysis at high transmit power is presented as well. Moreover, two benchmark schemes, half-duplex-jamming and full-duplex-no-jamming, are also considered. Simulation results are presented to show the accuracy of the analytical expressions and the effectiveness of the proposed scheme.**

***Index Terms*—Beamforming design, full-duplex relay, non-orthogonal multiple access, physical layer security, secrecy outage probability.**

I. Introduction

Owing to the excellent performance of spectrum utilization, non-orthogonal multiple access (NOMA) has been proposed for the 3GPP long term evolution advanced standard [1], and is expected to be used for the fifth-generation (5G) mobile networks, providing massive connectivity and low latency [2], [3]. Unlike the conventional orthogonal multiple access, NOMA introduces a novel power domain based on the time or frequency domains [4], [5]. Specifically, the users in NOMA networks are allocated with different power according to their channels or requirements, and then their signals are superposed and transmitted over the same channel [6]. At each receiver, successive interference cancellation (SIC) is utilized to mitigate the cochannel interference and extract the desired message from the received superposition signal [7], [8].

Recently, to improve the transmission reliability, cooperative NOMA schemes with relay have been widely studied [9], [10], especially for users with long distance or poor channel condition [11]–[17]. In [11], Zhang *et al.* utilized the near user served as the cooperative full-duplex (FD) relay to forward message for the far user in a downlink NOMA system, and the outage probability and ergodic sum rate were derived. In [12], Ding *et al*. proposed a two-stage relay selection strategy for the cooperative NOMA system to achieve better performance than the conventional max-min method. To assist the transmission of the far user, Zhong *et al.* introduced a dedicated FD relay in the NOMA system with two users, and both the secrecy outage probability (SOP) and ergodic sum capacity were analyzed [13]. In [14], performance gains were analyzed by Yue *et al.* for a cooperative NOMA network relayed by the FD/HD user with and without considering direct link between the BS and the far user, respectively. Besides, a two-stage superposed transmission scheme was proposed for the NOMA system with a decode-and-forward (DF) relay by Duan *et al.*, to further enhance the transmission rate [15]. A novel NOMA scheme with multiple relays and distributed space-time coding was proposed by Zhao *et al.* in [16]. In [17], Chen *et al.* leveraged the secondary NOMA relay to assist the primary transmission of long distance in two slots, with power allocation derived.

Although cooperative NOMA schemes can enhance the transmission reliability, the secure transmission is still a key challenge due to the openness of wireless channel. Specifically, eavesdroppers may exist in a NOMA system to intercept the confidential messages of legitimate users, and thus threaten their secure transmission [18]. Traditionally, to combat with eavesdropping, encryption in upper layer is usually adopted, which may become vulnerable with the improvement of computational power and capability [19]. Thus, an alternative mechanism, physical layer security (PLS), was investigated by Wyner [20]. Following this profound work, plenty of research has been conducted to guarantee the security through physical-layer techniques relying on the features of wireless channel,

Manuscript received December 6, 2018; revised March 18, 2019; accepted April 23, 2019. The work of N. Zhao was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065 and 61871139, the open research fund of State Key Laboratory of Integrated Services Networks under Grant ISN19-02, and the Xinghai Scholars Program. This paper will be presented in part at the Proceedings of IEEE/CIC ICCC 2019. The associate editor coordinating the review of this paper and approving it for publication was D. B. da Costa. *(Corresponding author: Nan Zhao.)*

Y. Cao, N. Zhao and M. Jin are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, P. R. China (email: cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn, mljin@dlut.edu.cn).

G. Pan is with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China. (e-mail: Gaofeng.Pan.CN@ieee.org).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China (e-mail: lsfan@gzhu.edu.cn).

Mohamed-Slim Alouini is with the Computer, Electrical, and Mathematical Science and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia. (e-mail: slim.alouini@kaust.edu.sa).

such as secure beamforming design [21], [22], artificial noise [23], interference alignment [24], [25], and especially, relaying [26]–[28]. Wang *et al.* proposed a joint cooperative scheme of beamforming and jamming in [26], to improve the security of an amplify-and-forward (AF) relaying network. In [27], Fan *et al.* analyzed the influence of the cochannel interference on the performance of secure transmission in the network with AF relays. In [28], Chen *et al.* proposed a FD jamming scheme to improve the secrecy capability of the relay network, and its SOP was derived as well.

For NOMA, only a few works have studied its security problem from the perspective of PLS [29]–[34]. In [29], Ding *et al.* studied the security performance of unicasting message in the NOMA system with the hybrid multicast-unicast scheme. Novel transmit antenna selection schemes were designed in [30] by Lei *et al.* to safeguard the secure transmission in the single-input single-output (SISO) and multi-input single-output (MISO) NOMA systems. In [31], the decoding order, transmission rate and power allocation were jointly optimized by He *et al.* in a NOMA system with secrecy outage constraint considered. Secrecy outage performance of large-scale NOMA networks was investigated by Liu *et al.* in both the single-antenna and multi-antenna scenarios [32]. In [33], Lv *et al.* proposed a novel secrecy beamforming scheme assisted by artificial noise (AN) to enhance the security of MISO NOMA systems when a multi-antenna eavesdropper exists. Beamforming and jamming are jointed optimized in [34] by Zhao *et al.* to guarantee the secure transmission for MISO NOMA. Furthermore, relaying has also been adopted in cooperative NOMA networks to guarantee the secure transmission [35]–[37]. Chen *et al.* analyzed the secrecy performance of cooperative NOMA systems for both AF and DF half-duplex (HD) relays [35]. In [36], a two-way FD relay was utilized to prevent both single and multiple eavesdroppers overhearing the confidential information, with the help of AN. Sun *et al.* considered the resource allocation problem in [37] for FD MISO multicarrier NOMA systems, where a FD base station (BS) was introduced to improve the security for both multiple downlink and uplink users via AN.

For a downlink NOMA network, the BS can serve both the cell-center and cell-edge users simultaneously. However, the transmission between the BS and the cell-edge user may be interrupted due to severe fading. Moreover, the message of cell-edge user is much easier to be intercepted by potential eavesdroppers than that of the cell-center user, due to the fact that more transmit power should be allocated to the users with poor channel conditions according to NOMA. Thus, in this paper, we consider a two-user NOMA system with a multi-antenna FD relay [38], providing reliable and secure transmission for NOMA users. The main contributions of this paper are summarized as follows.

- In downlink NOMA systems, the reliable and secure transmission is almost impossible to achieve for the cell-edge user with a weak channel. To solve this issue, we introduce a multi-antenna FD relay in a NOMA system with two users, and a two-stage jamming scheme, full-duplex-jamming (FDJam), is proposed to guarantee the secure transmission.

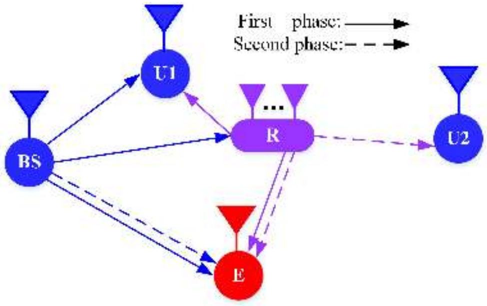

Fig. 1. Demonstration of the cooperative NOMA system assisted by multi-antenna FD relay for secure transmission.

- For the FDJam scheme, the transmission can be divided into two stages. In the first stage, the BS and FD relay transmit the confidential message and jamming signal to the cell-center user, relay and eavesdropper, respectively. The jamming signal is transmitted by the BS when the relay forwards the message to the cell-edge user in the second stage.
- To further improve the performance, beamforming is performed at the multi-antenna relay to cancel its self-interference and the jamming signal at the legitimate user. Accordingly, the analytical expressions of SOP are derived for both cell-center and cell-edge user, respectively. We also give the asymptotic SOP analysis to gain more insights when the transmit power is high.
- Two benchmark schemes, i.e., half-duplex-jamming (HDJam) and full-duplex-no-jamming (FDNoJam), are designed and analyzed to verify the effectiveness of the proposed FDJam scheme.

The rest of this paper is organized as follows. In Section II, the cooperative NOMA scheme with multi-antenna FD relay is proposed. In Section III, the theoretical expressions of SOP for NOMA users are derived, and the asymptotic SOP is also analyzed. Two benchmark schemes are designed in Section IV. In Section V, simulation results are presented, followed by conclusions in Section VI.

Notation: $\mathbf{I}_N$ is the $N \times N$ identity matrix. $\mathbf{0}_{M\times N}$ is an $M \times N$ zero matrix. $\mathbf{A}^\dagger$, $(\mathbf{A})^{-1}$ and $\|\mathbf{A}\|$ are the Hermitian transpose, inverse and Frobenius norm of matrix $\mathbf{A}$, respectively. $\|\mathbf{a}\|$ denotes the Euclidean norm of vector $\mathbf{a}$. $\mathbb{C}^{M\times N}$ represents the space of complex $M \times N$ matrices. The complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$ can be expressed as $\mathcal{CN}(\mathbf{a}, \mathbf{A})$. F_X and f_X denote the cumulative density function and probability density function of random variable X.

II. Cooperative NOMA Scheme With Multi-Antenna FD Relay

In this section, the system model of the proposed cooperative NOMA scheme with multi-antenna FD relay, FDJam, is presented, followed by the relay beamforming design.

Consider a downlink cooperative NOMA network, including one BS, two users, one malicious eavesdropper and one trustable relay, as shown in Fig. 1. The relay is equipped with multiple antennas, and all the other nodes are equipped with a single antenna. Assume that U_1 is near the BS while U_2 is far away from the BS. Thus, there is no direct link between the BS and U_2 due to the severe path loss and shadowing. The requirement and location information of U_2 can be obtained at the BS via the backhaul connected with the macro BS. A multi-antenna DF relay, which can serve as a FD transmission mode, is deployed to enhance the transmission reliability of U_2 and combat the eavesdropping simultaneously. Furthermore, to mitigate the self-interference at the FD relay, N_t antennas are adopted for transmission and the other N_r antennas are used for receiving. In the scheme, two stages are involved in each time slot as in Fig. 1, which will be presented as follows.

A. *First-Stage Transmission*

In the first stage, the superimposed signal at the BS is transmitted towards U_1, the relay, and the eavesdropper, respectively, i.e., $BS \to \{U_1, R, E\}$. Meanwhile, the FD relay transmits the precoded jamming signal to the eavesdropper, U_1 and itself, respectively, i.e., $R \to \{U_1, R, E\}$, while U_2 keeps silent. Note that the link $R \to R$ is denoted as self-interference caused by the FD operation.

According to the principle of NOMA, the transmitted signal of the BS can be expressed as

$$s = \sqrt{\alpha_1 P_s} s_1 + \sqrt{\alpha_2 P_s} s_2, \tag{1}$$

where P_s is the transmit power of the BS, α_1 and α_2 are the power allocation coefficients for the messages s_1 and s_2, respectively, which satisfy $\alpha_1 + \alpha_2 = 1$ and $\alpha_2 > \alpha_1$. Thus, the received signal at U_1 can be denoted as

$$y_{1,u_1} = h_{su_1} s + \sqrt{P_{jr}} \mathbf{h}_{ru_1} \mathbf{v}_j s_{jr} + n_{u_1}, \tag{2}$$

where $n_{u_1} \sim \mathcal{CN}(0, \sigma_1^2)$ is the additive white Gaussian noise (AWGN) at U_1, and P_{jr} denotes the jamming power transmitted by the FD relay. $\mathbf{v}_j \in \mathbb{C}^{N_t \times 1}$ is the precoding vector of the relay satisfying $\|\mathbf{v}_j\|^2 = 1$. The channel gain from the BS to U_1 is expressed as $h_{su_1} = \sqrt{\beta_0} d_{su_1}^{-\frac{\alpha}{2}} g_1$, where β_0 denotes the channel gain at reference distance $d = 1$, d_{su_1} is the distance between the BS and U_1, α is the path-loss exponent, and g_1 subjects to the Rayleigh fading. Similarly, $\mathbf{h}_{ru_1} = \sqrt{\beta_0} d_{ru_1}^{-\frac{\alpha}{2}} \mathbf{g}_{ru_1} \in \mathbb{C}^{1 \times N_t}$ represents the channel gains from the relay to U_1, in which d_{ru_1} is the distance between the relay and U_1, and $\mathbf{g}_{ru_1}$ denotes a $1 \times N_t$ vector whose elements are independent and identically distributed (i.i.d) and follow $\mathcal{CN}(0, 1)$. In addition, s_{jr} is the jamming symbol transmitted by the relay with $|s_{jr}|^2 = 1$.

Then, the received signal at the FD relay can be denoted as

$$y_{1,r} = \mathbf{u}_r^\dagger \mathbf{h}_{sr} s + \sqrt{P_{jr}} \mathbf{u}_r^\dagger \mathbf{H}_{rr} \mathbf{v}_j s_{jr} + \mathbf{u}_r^\dagger \mathbf{n}_r, \tag{3}$$

where $\mathbf{u}_r \in \mathbb{C}^{N_r \times 1}$ is the decoding vector at the relay for receiving and satisfies $\|\mathbf{u}_r\|^2 = 1$. The $N_r \times 1$ vector $\mathbf{h}_{sr}$ denotes the channel gains between the BS and relay, i.e., $\mathbf{h}_{sr} = \sqrt{\beta_0} d_{sr}^{-\frac{\alpha}{2}} \mathbf{g}_{sr}$. $\mathbf{n}_r \in \mathbb{C}^{N_r \times 1}$ is the AWGN vector at the relay, following $\mathcal{CN}(\mathbf{0}, \sigma_r^2 \mathbf{I}_{N_r})$. $\mathbf{H}_{rr} \in \mathbb{C}^{N_r \times N_t}$ represents the fading self-interference channel at the FD relay, and we assume that the perfect channel state information (CSI) on $\mathbf{H}_{rr}$ can be available at the relay[1] [39], [40]. The signal intercepted by the eavesdropper can be denoted as

$$y_{1,e} = h_{se} s + \sqrt{P_{jr}} \mathbf{h}_{re} \mathbf{v}_j s_{jr} + n_e, \tag{4}$$

where $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ is the AWGN at the eavesdropper. h_{se} denotes the channel gain with path loss from the BS to eavesdropper, i.e., $h_{se} = \sqrt{\beta_0} d_{se}^{-\frac{\alpha}{2}} g_{se}$. In addition, $\mathbf{h}_{re} = \sqrt{\beta_0} d_{re}^{-\frac{\alpha}{2}} \mathbf{g}_{re}$ is the channel coefficient vector with N_t dimensions from the FD relay to eavesdropper.

In this stage, we intend to degrade the eavesdropping channel using the jamming signal transmitted by the FD relay, without impacting on the legitimate transmission of U_1. Furthermore, the self-interference at the FD relay is expected to be eliminated for better performance. To achieve the above goals, the following conditions should be satisfied.

$$\mathbf{h}_{ru_1} \mathbf{v}_j = 0, \tag{5}$$

$$\mathbf{u}_r^\dagger \mathbf{H}_{rr} \mathbf{v}_j = 0. \tag{6}$$

When (5) is met, the jamming signal will be zero-forced at U_1, which means that it only disrupts the eavesdropping channel. In addition, the self-interference at the FD relay will be cancelled with (6) satisfied. Before solving (5) and (6), the feasibility conditions are first introduced as Lemma 1.

Lemma 1: The feasibility conditions for (5) and (6) can be derived as

$$N_t + N_r \geq 4, N_t \geq 2, N_r \geq 2. \tag{7}$$

Proof: Note that (5) and (6) denote a homogeneous linear equations, which can be solved only when the number of equations is not larger than that of variables. The total number of equations in (5) and (6) can be expressed as

$$\mathcal{N}_\varepsilon = 2. \tag{8}$$

Then, the total number of variables can be calculated as

$$\mathcal{N}_\nu = N_t - 1 + N_r - 1 = N_t + N_r - 2. \tag{9}$$

From algebra, when (5) and (6) are solvable, we have

$$\mathcal{N}_\varepsilon \leq \mathcal{N}_\nu \Rightarrow 2 \leq N_t + N_r - 2 \Rightarrow N_t + N_r \geq 4. \tag{10}$$

Furthermore, for (5), the relationship between the number of equations and variables can be denoted as

$$\mathcal{N}_\varepsilon^{(5)} \leq \mathcal{N}_\nu^{(5)} \Rightarrow 1 \leq N_t - 1 \Rightarrow N_t \geq 2. \tag{11}$$

Similarly, we can obtain $N_r \geq 2$ to make (6) solvable. ■

Based on the idea of NOMA, SIC is performed at each receiver to retrieve information in terms of the channel difference between them. Specifically, U_1 has to decode the message of U_2 before recovering its own message. Hence, the received signal-to-interference-plus-noise ratio (SINR) of U_2 at U_1 can be written as follows with feasibility conditions in (7) satisfied,

$$\gamma_{1,u_1}^{[2]} = |h_{su_1}|^2 \alpha_2 P_s / \left(|h_{su_1}|^2 \alpha_1 P_s + \sigma_1^2 \right). \tag{12}$$

[1] When the estimation error of the CSI on $\mathbf{H}_{rr}$ cannot be ignored, or the number of antennas at the relay is not enough to perform the beamforming, more practical model for the residual self-interference channel has to be considered, which will be investigated in our future work.

Subtracting the signal of U_2 perfectly, the received SINR for U_1 can be expressed as

$$\gamma_{1,u_1}^{[1]} = \left|h_{su_1}\right|^2 \alpha_1 P_s / \sigma_1^2. \tag{13}$$

Then, the SINR for decoding the message of U_2 at the relay can be denoted as

$$\gamma_{1,r}^{[2]} = \left|\mathbf{u}_r^{\dagger}\mathbf{h}_{sr}\right|^2 \alpha_2 P_s / \left(\left|\mathbf{u}_r^{\dagger}\mathbf{h}_{sr}\right|^2 \alpha_1 P_s + \sigma_r^2\right). \tag{14}$$

To further enhance the transmission reliability of U_2 at the relay, the decoding vector $\mathbf{u}_r$ can be optimized according to the following problem.

$$\begin{aligned} &\max_{\mathbf{u}_r} \ \gamma_{1,r}^{[2]} \\ &s.t. \ \mathbf{u}_r^{\dagger}\mathbf{H}_{rr}\mathbf{v}_j = 0, \ \left\|\mathbf{u}_r\right\|^2 = 1. \end{aligned} \tag{15}$$

According to the proof of Proposition 1 in [41], the optimal solution to (15) can be calculated as

$$\mathbf{u}_r = \mathbf{T}\mathbf{h}_{sr} / \sqrt{\mathbf{h}_{sr}^{\dagger}\mathbf{T}\mathbf{h}_{sr}}, \tag{16}$$

where $\mathbf{T} = \mathbf{I}_{N_r} - \mathbf{B}\left(\mathbf{B}^{\dagger}\mathbf{B}\right)^{-1}\mathbf{B}^{\dagger}$ and $\mathbf{B} = \mathbf{H}_{rr}\mathbf{v}_j$.

We assume that the eavesdropper has strong multi-user detection capability and consider the worst-case security[2] [35]. Thus, the upper bound of intercepted SINR of U_1 at E can be expressed as

$$\gamma_{1,e}^{[1]} = \left|h_{se}\right|^2 \alpha_1 P_s / \left(\left|\mathbf{h}_{re}\mathbf{v}_j\right|^2 P_{rj} + \sigma_e^2\right). \tag{17}$$

Similarly, the SINR of U_2 at E can be denoted as

$$\gamma_{1,e}^{[2]} = \left|h_{se}\right|^2 \alpha_2 P_s / \left(\left|\mathbf{h}_{re}\mathbf{v}_j\right|^2 P_{rj} + \sigma_e^2\right). \tag{18}$$

B. Second-Stage Transmission

In the second stage, the relay turns off its receiving antennas and switches to the HD mode. Thus, only its decoded information s_2 is transmitted to U_2, and U_1 keeps silent. Meanwhile, to further improve the security of U_2, the BS transmits the jamming signal to deteriorate the eavesdropping channel simultaneously without affecting the legitimate transmission.

First, the received signal at U_2 can be denoted as

$$y_{2,u_2} = \sqrt{P_r}\mathbf{h}_{ru_2}\mathbf{w}s_2 + n_{u_2}, \tag{19}$$

where $\mathbf{h}_{ru_2} = \sqrt{\beta_0}d_{ru_2}^{-\frac{\alpha}{2}}\mathbf{g}_{ru_2}$ denotes the channel gains vector between the relay and U_2 with size $1 \times N_t$. P_r is the transmit power of relay in the second stage. $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ denotes the precoding vector at the relay, which is designed to enhance the effective channel gain of U_2 in terms of maximal ratio transmission (MRT), i.e., $\mathbf{w} = \mathbf{h}_{ru_2}^{\dagger} / \left\|\mathbf{h}_{ru_2}\right\|$. $n_{u_2} \sim \mathcal{CN}(0, \sigma_2^2)$ is the AWGN at U_2. The received signal at the eavesdropper can be expressed as

$$y_{2,e} = \sqrt{P_r}\mathbf{h}_{re}\mathbf{w}s_2 + \sqrt{P_{js}}h_{se}s_{js} + n_e, \tag{20}$$

where P_{js} is the transmit power of jamming signal from the BS to eavesdropper. Thus, the received SINR at U_2 and eavesdropper can be written as follows, respectively.

$$\gamma_{2,u_2}^{[2]} = P_r\left|\mathbf{h}_{ru_2}\mathbf{w}\right|^2 / \sigma_2^2, \tag{21}$$

$$\gamma_{2,e}^{[2]} = P_r\left|\mathbf{h}_{re}\mathbf{w}\right|^2 / \left(P_{js}\left|h_{se}\right|^2 + \sigma_e^2\right). \tag{22}$$

Based on (13) and (17), the secrecy capacity for U_1 can be defined as

$$C_{s1} = \frac{1}{2}\left[\log_2\left(1+\gamma_{1,u_1}^{[1]}\right) - \log_2\left(1+\gamma_{1,e}^{[1]}\right)\right]^+, \tag{23}$$

where $[x]^+ \triangleq \max(x, 0)$. Moreover, according to the end-end transmission, the secrecy capacity for U_2 can be presented as

$$C_{s2} = \frac{1}{2}\left[\log_2\left(1+\min\left\{\gamma_{1,u_1}^{[2]}, \gamma_{1,r}^{[2]}, \gamma_{2,u_2}^{[2]}\right\}\right) - \log_2\left(1+\gamma_{1,e}^{[2]}+\gamma_{2,e}^{[2]}\right)\right]^+. \tag{24}$$

III. Secrecy Analysis for the Proposed Scheme

In this section, we analyze and derive the SOP for U_1 and U_2 in the proposed FDJam scheme, respectively, and the corresponding asymptotic SOP analysis is given as well at high transmit power. For simplicity, we assume that $\sigma_1^2 = \sigma_2^2 = \sigma_r^2 = \sigma_e^2 = \sigma^2$, $P_s = P_r = P$ and $P_{jr} = P_{js} = \eta P$, where $\eta > 0$ is a scaling factor.

A. SOP for U_1

Similar to [33], considering the worst case of imperfect SIC assumption, the secrecy outage probability for U_1 can be mathematically expressed as

$$\begin{aligned} P_{sop1} = &\underbrace{\Pr\left(C_{s1} < R_{s1} | \gamma_{1,u_1}^{[2]} \geq \gamma_2\right)\Pr\left(\gamma_{1,u_1}^{[2]} \geq \gamma_2\right)}_{A_1} \\ &+ \underbrace{\Pr\left(C_{s1} < R_{s1} | \gamma_{1,u_1}^{[2]} < \gamma_2\right)\Pr\left(\gamma_{1,u_1}^{[2]} < \gamma_2\right)}_{A_2}, \end{aligned} \tag{25}$$

where the items A_1 and A_2 denote the probabilities that the secrecy capacity is smaller than the given threshold R_{s1} under the condition that whether the message s_2 can be retrieved or not. Particularly, when the signal of U_2 fails to be decoded at U_1, i.e., $\gamma_{1,u_1}^{[2]} < \gamma_2$, the secrecy capacity will be zero, which means $\Pr\left(C_{s1} < R_{s1} | \gamma_{1,u_1}^{[2]} < \gamma_2\right) = 1$. Thus, the item A_2 can be simplified as

$$\Pr\left(\gamma_{1,u_1}^{[2]} < \gamma_2\right) = \Pr\left(\left|h_{su_1}\right|^2 < \frac{\gamma_2\sigma^2}{(\alpha_2 - \alpha_1\gamma_2)P}\right) = \Pr(X < \xi), \tag{26}$$

where $\xi = \frac{\gamma_2\sigma^2}{(\alpha_2-\alpha_1\gamma_2)P}$ should be larger than zero, i.e., $\alpha_2 - \alpha_1\gamma_2 > 0$, otherwise, $P_{sop1} = 1$ will be always held. In addition, $X = \left|h_{su1}\right|^2$ follows an exponential distribution with the parameter $\lambda_0 = 1/(\beta_0 d_{su1}^{-\alpha})$. Hence, its cumulative density function (CDF) can be calculated as

$$F_X(x) = 1 - e^{-\lambda_0 x}. \tag{27}$$

Then, the item A_2 can be rewritten as

$$F_X(\xi) = \Pr(X < \xi) = 1 - e^{-\lambda_0 \xi}. \tag{28}$$

Using (23) and (26), the term A_1 can be transformed as

$$A_1 = \Pr\left(\xi < X < \varphi\left(\gamma_{1,e}^{[1]}\right)\right), \tag{29}$$

[2] The work in this paper is easy to be extended to the case where other possible decoding strategies are adopted at the eavesdropper, details of which are not included due to space limitation.

where $\varphi\left(\gamma_{1,e}^{[1]}\right)=\frac{\left(2^{2R_{s1}}\left(1+\gamma_{1,e}^{[1]}\right)-1\right)\sigma^2}{\alpha_1 P}$. Note that the probability in (29) exists only when the inequality $\varphi\left(\gamma_{1,e}^{[1]}\right)>\xi$ can be satisfied, namely, $\gamma_{1,e}^{[1]}>\nu=\frac{\alpha_2 2^{-2R_{s1}}}{\alpha_2-\alpha_1\gamma_2}-1$. Based on the above analysis, we can rewrite (25) as

$$P_{sop1}=\Pr\left(\xi<X<\varphi\left(\gamma_{1,e}^{[1]}\right)\right)+\Pr\left(X<\xi\right). \tag{30}$$

To calculate the probability in (30), we first introduce Lemma 2 as follows.

Lemma 2: Assume that random variables (RVs) Y_1 and Y_2 are both subjected to exponential distribution, i.e., $Y_1\sim E(\lambda_1)$ and $Y_2\sim E(\lambda_2)$, where λ_1 and λ_2 are the parameters for Y_1 and Y_2, respectively. Define the RV $Z=\frac{Y_1}{Y_2+c}$, and its probability density function (PDF) can be derived as

$$f_Z(z)=\lambda e^{-\lambda_1 zc}\left(\frac{c}{\lambda_1 z+\lambda_2}+\frac{1}{(\lambda_1 z+\lambda_2)^2}\right). \tag{31}$$

Proof: Due to the independence between Y_1 and Y_2, their joint PDF can be expressed as

$$f(y_1,y_2)=f(y_1)f(y_2)=\lambda e^{-(\lambda_1 y_1+\lambda_2 y_2)}, \tag{32}$$

where $\lambda=\lambda_1\lambda_2$. According to probability theory, the PDF of Z can be denoted as $f_Z(z)=\int_0^\infty f(y_1(y_2,z),y_2)\left|\partial_z y_1\right|dy_2=\lambda e^{-\lambda_1 zc}\left(\frac{c}{\lambda_1 z+\lambda_2}+\frac{1}{(\lambda_1 z+\lambda_2)^2}\right)$. ■

Define $Z=\gamma_{1,e}^{[1]}$, we can obtain its PDF as follows according to Lemma 2.

$$f_Z(z)=\lambda e^{-\lambda_1 z\sigma^2}\left(\frac{\sigma^2}{\lambda_1 z+\lambda_2}+\frac{1}{(\lambda_1 z+\lambda_2)^2}\right), \tag{33}$$

where $\lambda_1=1/\left(\beta_0 d_{se}^{-\alpha}\alpha_1 P\right)$ and $\lambda_2=1/\left(\beta_0 d_{re}^{-\alpha}\eta P\right)$. Therefore, according to (28) and (33), the SOP for U_1 can be derived in the following proposition.

Proposition 1: The SOP for U_1 is derived as (34) at the top of the next page with two cases $\nu>0$ and $\nu\le 0$ considered, where μ can be found in Appendix A. $Ei(c)=\int_{-\infty}^{c}e^x/xdx$ denotes the exponential integral function.

Proof: See Appendix A. ■

B. SOP for U_2

When the secrecy capacity is smaller than its predefined threshold, the transmission of confidential message for U_2 will be interrupted. Thus, the SOP for U_2 can be denoted as

$$P_{sop2}=\Pr\left(C_{s2}<R_{s2}\right), \tag{35}$$

where R_{s2} is the given secrecy threshold of U_2. Replacing C_{s2} with (24), the probability (35) can be rewritten as

$$P_{sop2}=\Pr\left(Q<2^{2R_{s2}}V\right)=\int_1^\infty F_Q\left(2^{2R_{s2}}v\right)f_V(v)dv \tag{36}$$

where $Q=1+\min\left\{\gamma_{1,u_1}^{[2]},\gamma_{1,r}^{[2]},\gamma_{2,u_2}^{[2]}\right\}$ and $V=1+\gamma_{1,e}^{[2]}+\gamma_{2,e}^{[2]}$. The CDF of Q and the PDF of V can be given by the following Lemma 3.1 and 3.2, respectively.

Lemma 3.1: The CDF of Q can be obtained as

$$F_Q(q)=\begin{cases}0 & q<1,\\ 1-g_1(q)g_2(q)g_3(q) & 1<q<\frac{1}{\alpha_1},\\ 1 & q>\frac{1}{\alpha_1}.\end{cases} \tag{37}$$

where $g_1(q)$, $g_2(q)$ and $g_3(q)$ can be found in Appendix B.

Proof: See Appendix B. ■

Lemma 3.2: The PDF of V can be derived as

$$\begin{aligned}f_V(v)=&\frac{\pi}{L}\frac{v-1}{2}\sum\nolimits_{l=1}^{L}\sqrt{1-x_l^2}\\ &f_{V_1}\!\left(\frac{v-1}{2}x_l+\frac{v+1}{2}\right)f_{V_2}\!\left(v-\left(\frac{v-1}{2}x_l+\frac{v+1}{2}\right)\right),\end{aligned} \tag{38}$$

where $x_l=\cos\left(\frac{2l-1}{2L}\pi\right)$, and L denotes the number of nodes set in the Chebyshev-Guass approximation. Besides, $f_{V_1}(v)$ and $f_{V_2}(v)$ can be referred to Appendix C.

Proof: See Appendix C. ■

In terms of Lemma 3.1 and 3.2, the SOP for U_2 can be rewritten as

$$P_{sop2}=\int_1^b F_Q\left(v2^{2R_{s2}}\right)f_V(v)dv+\int_b^\infty f_V(v)dv, \tag{39}$$

where $b=2^{-2R_{s2}}/\alpha_1$. Note that $P_{sop2}=1$ when $b<1$. To solve (39), we utilize the Chebyshev-Guass quadrature to get an approximation for it. Specifically, based on (37), the formula (39) can be simplified as

$$P_{sop2}=1-\int_1^b g_1\!\left(v2^{2R_{s2}}\right)g_2\!\left(v2^{2R_{s2}}\right)g_3\!\left(v2^{2R_{s2}}\right)f_V(v)dv \tag{40}$$

Then, using the Chebyshev-Guass quadrature, the SOP for U_2 can be derived as

$$P_{sop2}=1-\frac{\pi}{L}\frac{b-1}{2}\sum_{j=1}^{L}\sqrt{1-x_j^2}g_1(\varpi)\,g_2(\varpi)g_3(\varpi)f_V\!\left(\frac{\varpi}{2^{2R_{s2}}}\right), \tag{41}$$

where $\varpi=2^{2R_{s2}}(\frac{b-1}{2}x_j+\frac{b+1}{2})$ and $x_j=\cos\left(\frac{2j-1}{2L}\pi\right)$.

C. Asymptotic SOP Analysis

To gain more insights about the proposed FDJam scheme, we analyze the asymptotic SOP for U_1 and U_2 with high transmit power considered, i.e., $P\to\infty$.

First, from (34), we can obtain

$$P_{sop1}^{\infty}=0, \tag{42}$$

for both the cases of $\nu>0$ and $\nu\le 0$, when $P\to\infty$. This means that U_1 can always achieve secure transmission with the secrecy rate R_{s1} at high transmit power.

On the other hand, for U_2 with sufficiently high transmit power, its asymptotic SOP can be given by the following Proposition 2.

Proposition 2: The asymptotic SOP for U_2 can be derived as

$$P_{sop2}^{\infty}=1-\frac{\pi}{L}\frac{b-1}{2}\sum\nolimits_{j=1}^{L}\sqrt{1-x_j^2}f_V\left(\frac{b-1}{2}\left(x_j+1\right)\right), \tag{43}$$

where $f_V(v)$ can be seen in the proof.

Proof: When $P\to\infty$, (35) can be approximated as

$$\begin{aligned}P_{sop2}^{\infty}=&\Pr\left(\frac{1+\frac{\alpha_2}{\alpha_1}}{1+V_1+V_2}<2^{2R_{s2}}\right)\\ =&1-\Pr\left(V_1+V_2<\frac{2^{-2R_{s2}}}{\alpha_1}-1\right)=1-F_V(b-1),\end{aligned} \tag{44}$$

$$P_{sop1} = \begin{cases} 1-\lambda_2 \exp\left(-\lambda_1 \left(\frac{d_{su1}}{d_{se}}\right)^{\alpha} \sigma^2 \left(2^{2R_{s1}}-1\right)\right)\left(\frac{1}{\lambda_2}+\left(\frac{d_{su1}}{d_{se}}\right)^{\alpha} 2^{2R_{s1}}\sigma^2 \exp\left(\lambda_2\mu\right) Ei(-\lambda_2\mu)\right), & \nu \le 0, \\ \left(1-F_X(\xi)\right)\lambda_2 \frac{\exp\left(-\lambda_1\nu\sigma^2\right)}{\lambda_1\nu+\lambda_2} + F_X(\xi) - \lambda_2 \exp\left(-\lambda_1\left(\frac{d_{su1}}{d_{se}}\right)^{\alpha}\sigma^2\left(2^{2R_{s1}}-1\right)\right) \times & \\ \left(\left(\frac{d_{su1}}{d_{se}}\right)^{\alpha} 2^{2R_{s1}}\sigma^2 \exp(\lambda_2\mu) Ei(-(\lambda_1\nu+\lambda_2)\mu) + \frac{\exp(-\lambda_1\nu\mu)}{\lambda_1\nu+\lambda_2}\right), & \nu > 0. \end{cases} \tag{34}$$

where $V = V_1 + V_2$, $V_1 = \alpha_2|h_{se}|^2/(\eta|\mathbf{h}_{re}\mathbf{v}_j|^2)$, $V_2 = |\mathbf{h}_{re}\mathbf{w}|^2/(\eta|h_{se}|^2)$. F_V denotes the CDF of V.

According to Lemma 3.2, we can obtain

$$f_V(v)=\int_0^v f_{V_1}(v-v_2)f_{V_2}(v_2)dv_2 = pp_0\int_0^v \mathcal{H}\left(v_2\right)dv_2 \tag{45}$$

where the parameters p, p_0, p_1, p_2, p_3 and p_4 are the same as those in Lemma 3.2. $\mathcal{H}(v_2)$ denotes

$$\mathcal{H}(v_2) = \frac{1}{\left((p_1v_2-(p_1v+p_2))^2(p_3v_2+p_4)\right)^2}.$$

To our best knowledge, it is difficult to obtain the closed-form solution to the integral in (45). Thus, the Chebyshev-Guass approximation is utilized to solve it as

$$f_V(v) = pp_0\frac{\pi}{L}\frac{v}{2}\sum\nolimits_{l=1}^{L}\sqrt{1-x_l^2}\mathcal{H}\left(\frac{v}{2}\left(x_l+1\right)\right). \tag{46}$$

Furthermore, we can obtain

$$F_V(b-1)=\frac{\pi}{L}\frac{b-1}{2}\sum\nolimits_{j=1}^{L}\sqrt{1-x_j^2}f_V\left(\frac{b-1}{2}\left(x_j+1\right)\right), \tag{47}$$

Substituting (47) into (44), the asymptotic SOP for U_2 can be expressed as $P_{sop2}^{\infty}=1-\frac{\pi}{L}\frac{b-1}{2}\sum\limits_{j=1}^{L}\sqrt{1-x_j^2}f_V\left(\frac{b-1}{2}\left(x_j+1\right)\right)$. ■

From (43), we can observe that when $P \to \infty$, the SOP of U_2 is varying with the change of parameters η, α_1, d_{re} and d_{se}, and will not be impacted by d_{sr} and d_{ru2}. This indicates that the power allocation between the legitimate signal and the jamming signal and the power allocation between U_1 and U_2 are both important for the secrecy performance of U_2, and the relative locations between the nodes BS, R and E are vital as well. In addition, the increasing number of antennas at the relay will not change the SOP of U_2 with $P \to \infty$. This is because when the transmit power is high, the statistical distribution of the transmission and eavesdropping rate in (44) are independent of the number of antennas.

IV. Two Benchmark Schemes

In this section, other two schemes, HDJam and FDNoJam, are proposed to compare the performance of the proposed FDJam scheme as benchmarks, with their SOP also derived.

A. HDJam Scheme

1) System Model: In the scheme, we consider $N = N_t + N_r$ antennas equipped at the relay are utilized to transmit or recover information. In the first stage of $BS \to \{U_1, R, E\}$, the relay cannot send the jamming signal to the eavesdropper due to the half-duplex mode. For fairness, we assume that the BS can send messages with transmit power P_T, where $P_T = P_s + P_{jr}$. Thus, the signal transmitted by the BS can be modified as

$$s = \sqrt{\alpha_1 P_T}s_1 + \sqrt{\alpha_2 P_T}s_2, \tag{48}$$

Accordingly, the received signal at the relay and U_1 can be denoted as follows, respectively.

$$y_{1,r} = \mathbf{u}_r^{\dagger}\mathbf{h}_{sr}s + \mathbf{u}_r^{\dagger}\mathbf{n}_r. \tag{49}$$

$$y_{1,u1} = h_{su_1}s + n_{u_1}, \tag{50}$$

In terms of the principle of maximum ratio combining (MRC), $\mathbf{u}_r$ is designed as $\mathbf{u}_r = \mathbf{h}_{sr}/\|\mathbf{h}_{sr}\|$. Then, the received SINR at the relay for U_2 can be expressed as

$$\gamma_{1,r}^{[2]} = \|\mathbf{h}_{sr}\|^2\alpha_2 P_T/\left(\|\mathbf{h}_{sr}\|^2\alpha_1 P_T + \sigma_r^2\right). \tag{51}$$

In addition, replacing P_s with P_T in (12) and (13), the received SINR for U_2 and U_1 at U_1 can be derived similarly as

$$\gamma_{1,u_1}^{[2]} = |h_{su_1}|^2\alpha_2 P_T/\left(|h_{su_1}|^2\alpha_1 P_T + \sigma_1^2\right), \tag{52}$$

$$\gamma_{1,u_1}^{[1]} = |h_{su_1}|^2\alpha_1 P_T/\sigma_1^2. \tag{53}$$

The intercepted signal at eavesdropper can be denoted as

$$y_{1,e} = h_{se}s + n_e, \tag{54}$$

and we have

$$\gamma_{1,e}^{[1]} = |h_{se}|^2\alpha_1 P_T/\sigma_e^2, \tag{55}$$

$$\gamma_{1,e}^{[2]} = |h_{se}|^2\alpha_2 P_T/\sigma_e^2. \tag{56}$$

On the other hand, the transmission of the second stage is the same as that in the FDJam scheme, i.e., the BS transmits the jamming signal, while the relay forwards its decoded message to U_2. Thus, in this scheme, the expressions of secrecy capacity for U_1 and U_2 are same as (23) and (24).

2) SOP Analysis: Following the same method adopted in the FDJam scheme, the SOP for U_1 can be derived as (57) at the top of the next page, where $\lambda_0 = d_{su1}^{\alpha}/\beta_0$ and $\lambda = \sigma^2/(\alpha_1 P_T\beta_0 d_{se}^{-\alpha})$.

As for U_2, its SOP can be derived as

$$P_{sop2}=1-\frac{\pi}{L}\frac{b-1}{2}\sum_{j=1}^{L}\sqrt{1-x_j^2}g_1(\varpi)\,g_2(\varpi)g_3(\varpi)f_V\left(\frac{\varpi}{2^{2R_{s2}}}\right). \tag{58}$$

$g_1(q)$, $g_2(q)$ and $f_V(v)$ in (58) are different from those in (41). Specifically, in this scheme, Q_1 and Q_2 subject to Gamma distribution with the shape parameter N and the scale

$$P_{sop1}=\begin{cases}1-\frac{\lambda\alpha_1 P_T}{\lambda_0 2^{2R_{s1}}\sigma^2+\lambda\alpha_1 P_T}\exp\left(-\frac{\lambda_0(2^{2R_{s1}}-1)\sigma^2}{\alpha_1 P_T}\right), \nu\le 0,\\ 1-\exp(-\lambda_0\xi)\left(1-\exp\left(\lambda\nu\right)\right)-\frac{\lambda\alpha_1 P_T}{\lambda_0 2^{2R_{s1}}\sigma^2+\lambda\alpha_1 P_T}\exp\left(-\left(\frac{\lambda\alpha_1 P_T}{\lambda_0 2^{2R_{s1}}\sigma^2+\lambda\alpha_1 P_T}\nu\right)+\frac{\lambda_0(2^{2R_{s1}}-1)\sigma^2}{\alpha_1 P_T}\right), \nu>0.\end{cases} \tag{57}$$

$$f_V(v)=pp_1 e^{-p_1(v-1)}\left(\frac{p_1}{p_3^2}e^{\mu\iota}\left(Ei(-\mu(v+\iota))-Ei(-\mu\iota)\right)+\frac{1}{p_3^2\iota}-\frac{e^{-\mu v}}{p_3^2(v+\iota)}\right). \tag{60}$$

parameters θ_1 and θ_2, respectively, i.e., $Q_1\sim\Gamma(N,\theta_1)$ and $Q_2\sim\Gamma(N,\theta_2)$. Thus, $g_1(q)$ and $g_2(q)$ should be modified as

$$\begin{aligned} g_1(q)&=e^{-\frac{\zeta(q)}{P_T\theta_1}}\sum_{i=0}^{N-1}\frac{1}{i!}\left(\frac{\zeta(q)}{P_T\theta_1}\right)^i,\\ g_2(q)&=e^{-\frac{q-1}{\theta_2}}\sum_{i=0}^{N-1}\frac{1}{i!}\left(\frac{q-1}{\theta_2}\right)^i,\end{aligned} \tag{59}$$

Moreover, in terms of Lemma 2 and 3.1, the PDF of V can be calculated as (60) at the top of next page, where $\mu=p_3\sigma^2-p_1$ and $\iota=p_4/p_3$. $p_1=\sigma^2/(\alpha_2 P_T\beta_0 d_{se}^{-\alpha})$, and parameters p, p_3 and p_4 are same as those in Appendix C.

3) Asymptotic SOP Analysis: When $P_T\to\infty$, the asymptotic SOP of U_1 can be denoted as

$$P_{sop1}^{\infty}=1-\frac{1}{1+2^{2R_{s1}}d_{se}^{-\alpha}d_{su1}^{\alpha}}. \tag{61}$$

From (61), we can see that P_{sop1}^{∞} is proportional to d_{su1} and inversely proportional to d_{se}, which is consistent with the practical analysis. In addition, the asymptotic SOP of U_2 can be expressed as

$$P_{sop2}^{\infty}=1–\Pr\left(\gamma_{1,e}^{[2]}+|\mathbf{h}_{re}\mathbf{w}|^2/(\eta|h_{se}|^2)<2^{-2R_{s2}}/\alpha_1-1\right). \tag{62}$$

From (56), we can know that $\gamma_{1,e}^{[2]}\to\infty$ with $P_T\to\infty$, and thus, $P_{sop2}^{\infty}=1$.

B. FDNoJam

1) System Model: In the scheme, we consider that the relay works at FD mode and no jamming signal is generated to degrade the eavesdropping channel, i.e., the relay receives information from the BS, and simultaneously transmits the already decoded signal to U_2. For fairness, we assume that both the transmit power of BS and relay is set as P_T. Thus, at the time slot t, the transmitted signal at the BS and relay can be expressed as

$$s(t)=\sqrt{\alpha_1 P_T}s_1(t)+\sqrt{\alpha_2 P_T}s_2(t), \tag{63}$$

$$\mathbf{s}_r(t)=\sqrt{P_T}\mathbf{w}s_2(t-\tau). \tag{64}$$

Then, the received signal at U_1 and relay can be denoted as

$$y_{u1}(t)=h_{su1}s(t)+\sqrt{P_T}\mathbf{h}_{ru1}\mathbf{w}s_2(t-\tau)+n_{u1}(t), \tag{65}$$

$$y_r(t)=\mathbf{u}_r^{\dagger}\mathbf{h}_{sr}s(t)+\sqrt{P_T}\mathbf{u}_r^{\dagger}\mathbf{H}_{rr}\mathbf{w}s_2(t-\tau)+\mathbf{u}_r^{\dagger}\mathbf{n}_r, \tag{66}$$

where $\tau\ge 1$ represents the processing delay at the relay. According to [42], we can observe that the second item in (65) can be removed via interference cancellation due to the fact that the side information of $s_2(t-\tau)$ can be obtained with SIC performed at U_1. Thus, the received SINR of U_1 and U_2 at U_1, i.e., $\gamma_{u1}^{[2]}$ and $\gamma_{u1}^{[1]}$, can be derived the same as (52) and (53), respectively. For (66), the same beamforming design as that in the FDJam scheme can be utilized to cancel the self-interference at the relay. Hence, $\gamma_r^{[2]}$ can be expressed the same as $\gamma_{1,r}^{[2]}$ in (14), replacing P_s with P_T.

Furthermore, the received signal at U_2 can be given as

$$y_{u2}(t)=\sqrt{P_T}\mathbf{h}_{ru2}\mathbf{w}s_2(t-\tau)+n_{u2}(t). \tag{67}$$

Accordingly, its received SINR can be written as

$$\gamma_{u2}^{[2]}=P_T\left|\mathbf{h}_{ru2}\mathbf{w}\right|^2/\sigma_2^2. \tag{68}$$

For the eavesdropper, its overheard signal can be denoted as

$$y_e(t)=h_{se}s(t)+\sqrt{P_T}\mathbf{h}_{re}\mathbf{w}s_2(t-\tau)+n_e(t). \tag{69}$$

Similar to the other two schemes, we consider the lower bound of secrecy capacity, and thus the intercepted SINR of U_1 at the eavesdropper can be denoted as

$$\gamma_e^{[1]}=\alpha_1 P_T\left|h_{se}\right|^2/\sigma_e^2, \tag{70}$$

and the received SINR of U_2 at the eavesdropper can be expressed as [28]

$$\gamma_e^{[2]}=\alpha_2 P_T\left|h_{se}\right|^2/\sigma_e^2+P_T\left|\mathbf{h}_{re}\mathbf{w}\right|^2/\sigma_e^2. \tag{71}$$

Due to the FD mode, the transmission of the cooperative NOMA system can be established during the entire time slot, which means there is no $\frac{1}{2}$ factor included in the definitions of users' secrecy capacity. Thus, in this scheme, the secrecy capacity of U_1 and U_2 can be denoted as

$$C_{s1}=\left[\log_2\left(1+\gamma_{u_1}^{[2]}\right)-\log_2\left(1+\gamma_e^{[1]}\right)\right]^+, \tag{72}$$

$$C_{s2}=\left[\log_2\left(1+\min\left\{\gamma_{u1}^{[2]},\gamma_r^{[2]},\gamma_{u2}^{[2]}\right\}\right)-\log_2\left(1+\gamma_e^{[2]}\right)\right]^+. \tag{73}$$

2) SOP Analysis: In terms of (25), we can calculate the SOP of U_1 with same method in Section III as follows.

$$P_{sop1}=\begin{cases}1-\frac{\lambda}{a_1}e^{-a_2}, & \nu\le 0,\\ 1-e^{-\lambda_0\xi}(1-e^{\lambda\nu})-\frac{\lambda}{a_1}e^{-(a_2+a_1\nu)}, & \nu>0,\end{cases} \tag{74}$$

where $a_1=\frac{\lambda_0 2^{R_{s1}}\sigma^2}{\alpha_1 P_T}+\lambda$ and $a_2=\frac{\lambda_0(2^{R_{s1}}-1)\sigma^2}{\alpha_1 P_T}$. λ and λ_0 are same as those in (57).

Similarly, the SOP of U_2 can be derived as

$$P_{sop2}=\Pr\left(Q<2^{R_{s2}}V\right)=\int_1^{\infty}F_Q\left(2^{R_{s2}}v\right)f_V(v)dv. \tag{75}$$

Note that the CDF of Q can be derived the same as (37), yet the PDF of V needs to be re-calculated according to Lemma 3.2 as

$$f_V(v)=\frac{p}{p_4-p_3}\left(e^{-p_3(v-1)}-e^{-p_4(v-1)}\right), \tag{76}$$

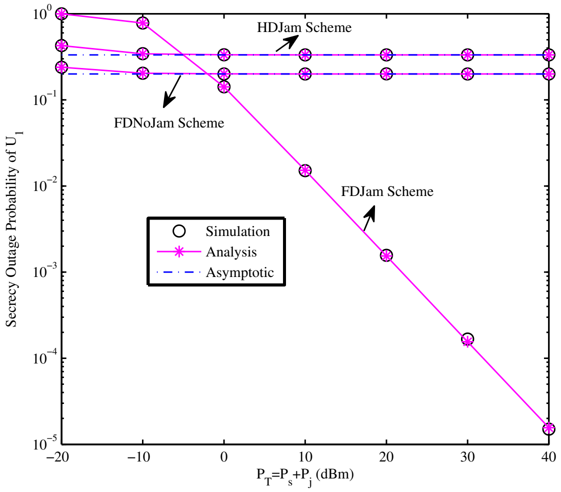

Fig. 2. Comparison of secrecy outage probability of U_1 for three schemes with different P_T.

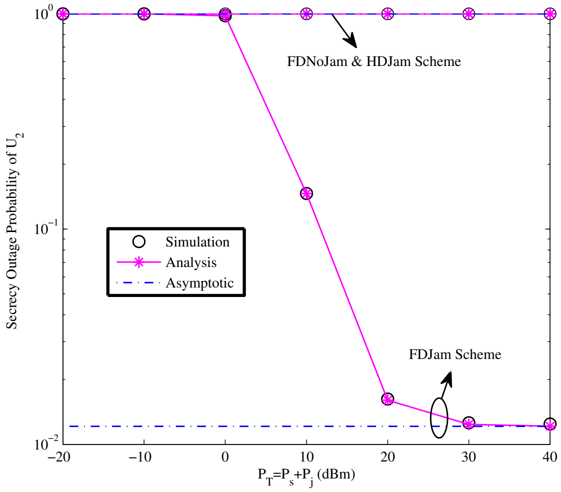

Fig. 3. Comparison of secrecy outage probability of U_2 for three schemes with different P_T.

where $p_3 = \sigma^2/(\alpha_2 P_T \beta_0 d_{se}^{-\alpha})$, $p_4 = \sigma^2/(P_T \beta_0 d_{re}^{-\alpha})$, and $p = p_3 p_4$. Substituting (76) and (37) into (75), we can get the SOP of U_2 as

$$P_{sop2}=1-\frac{\pi}{L}\frac{c-1}{2}\sum_{j=1}^{L}\sqrt{1-x_j^2}g_1(\omega)\,g_2(\omega)g_3(\omega)f_V\Big(\frac{\omega}{2^{R_{s2}}}\Big), \quad (77)$$

where $\omega = 2^{R_{s2}}\left(\frac{c-1}{2}x_j + \frac{c+1}{2}\right)$ and $c = 2^{-R_{s2}}/\alpha_1$.

3) Asymptotic SOP Analysis: Similar to the HDJam scheme, the asymptotic SOP of U_1 can be denoted as

$$P_{sop1}^{\infty} = 1 - \frac{1}{1 + 2^{R_{s1}} d_{se}^{-\alpha} d_{su1}^{\alpha}}. \quad (78)$$

We can express the SOP of U_2 as follows when $P_T \to \infty$.

$$P_{sop2}^{\infty} = 1 - \Pr\left(\gamma_e^{[2]} < 2^{-R_{s2}}/\alpha_1 - 1\right). \quad (79)$$

In this case, it is obvious that $\gamma_e^{[2]} \to \infty$, and thus $P_{sop2}^{\infty} = 1$.

V. Simulation Results and Discussion

In this section, simulation results are presented to validate the effectiveness of the proposed FDJam scheme. We assume that all the channels suffer from Rayleigh block fading, and that the path-loss exponent $\alpha = 3$. The SINR threshold for decoding the message of U_2 at U_1 is set as $\gamma_2 = 0.5$. The target secrecy rate over unit bandwidth for U_1 and U_2 is set as $R_{s1} = 1$ bit/s/Hz and $R_{s2} = 0.5$ bit/s/Hz, respectively. The distances are set as $d_{su1} = 10, d_{sr} = d_{se} = d_{ru1} = d_{re} = 20$ and $d_{ru2} = 80$ in meters. We also set $\alpha_1 = 0.2, \beta_0 = -40$ dB and $\sigma^2 = -110$ dBm.

First, we compare the SOP of both U_1 and U_2 for the three schemes with different P_T in Fig. 2 and Fig. 3, respectively. We set $L = 100$ in the Chebyshev-Guass approximation and $\eta = 99$. From the results, we can see that results obtained by Monte Carlo simulations match well with the analytical results for these three schemes. In Fig. 2, the SOP of U_1 decreases with P_T for the three schemes. Specifically, at lower P_T, the SOP of U_1 in the FDNoJam scheme is lower than both the HDJam and FDJam schemes. This is because the HDJam scheme has $1/2$ factor in its definition of secrecy capacity, and part of the transmit power P_T in the FDJam scheme is exploited to generate jamming signal. Nevertheless, the SOP of U_1 in the FDJam scheme is the lowest and close to 0 when P_T increases, while the SOP of U_1 in the other two schemes tends to be a constant. This is due to the fact that the jamming signal transmitted by the FD relay can degrade the eavesdropping channel significantly without affecting the legitimate channels, which is consistent with the asymptotic SOP analysis in Section III-C. In addition, the asymptotic SOP of U_1 in the FDJam scheme cannot be found in Fig. 2, due to the fact that it is 0 according to (42). From Fig. 3, we can observe that the SOP of U_2 in both FDNoJam and HDJam schemes is always approximated to 1 within the entire range of P_T, due to the worst-case assumption of the strong detection capability and MRC technique considered at the eavesdropper, which is also consistent with the asymptotic SOP analysis in Section IV. For the FDJam scheme, the SOP of U_2 becomes smaller with P_T and tends to be a constant when P_T is high, which is perfectly matched with the asymptotic result in (43).

Then, we evaluate the SOP of U_1 and U_2 for the FDJam and HDJam schemes under different P_s, when $\eta = 1$, $\eta = 10$, $\eta = 100$, as shown in Fig. 4 and Fig. 5. From the results, we can see that both users' SOP in the FDJam scheme decreases with η and P_s, especially for the cell-edge user U_2, which indicates that increasing the transmit power of jamming signal can effectively disrupt the eavesdropping and guarantee the secure transmission of NOMA users. For the HDJam scheme, the SOP of U_1 becomes smaller and approximates to a constant when η increases in Fig. 4, due to the increasing transmit power P_T, which is the same as the results in Fig. 2. Nevertheless, the SOP of U_2 in the HDJam scheme is nearly unchanged with η, and tends to be 1, which means that the jamming signal generated in the second stage has nearly no impact on the SOP of U_2. This is because there is no jamming signal to disturb the eavesdropping in the first stage and MRC is adopted at the eavesdropper.

In Fig. 6, the influence of the number of antennas at the

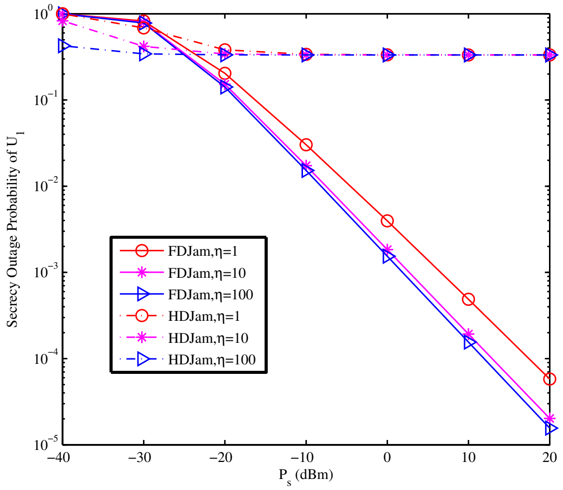

Fig. 4. Comparison of secrecy outage probability of U_1 for the FDJam and HDJam schemes under different P_s, with three cases of $\eta = 1$, $\eta = 10$ and $\eta = 100$ considered.

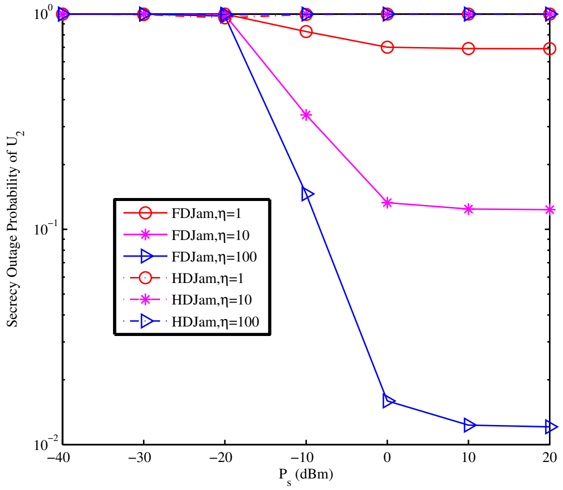

Fig. 5. Comparison of secrecy outage probability of U_2 for the FDJam and HDJam schemes under different P_s, with three cases of $\eta = 1$, $\eta = 10$ and $\eta = 100$ considered.

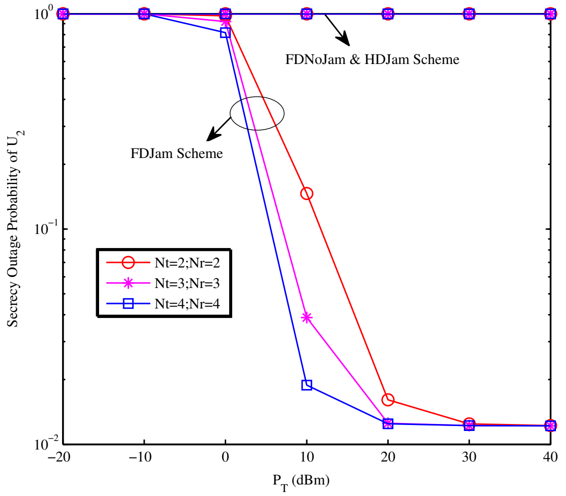

Fig. 6. Comparison of secrecy outage probability of U_2 for the three schemes under different P_T, with three cases of $N_t = N_r = 2$, $N_t = N_r = 3$ and $N_t = N_r = 4$ considered.

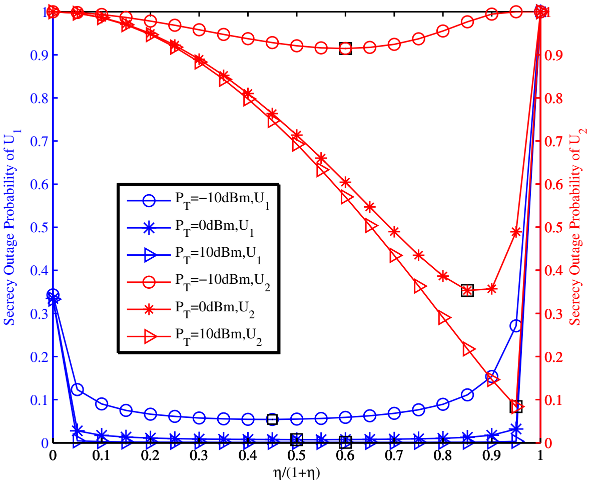

Fig. 7. Comparison of secrecy outage probability of U_1 and U_2 in the FDJam scheme with different power allocation between confidential and jamming signals. Three cases of $P_T = -10$dBm, $P_T = 0$dBm and $P_T = 10$dBm are considered.

relay on the SOP of U_2 is compared for the three schemes. Three cases of $N_t = N_r = 2$, $N_t = N_r = 3$ and $N_t = N_r = 4$ are considered. $\eta = 99$. Similarly to the results in Fig. 3, the SOP of U_2 for the FDNoJam and HDJam schemes in Fig. 6 is almost unchanged with the number of antennas. However, the secrecy performance of U_2 in the FDJam scheme can be improved with larger number of antennas. Furthermore, it is worth noticing that the number of antennas at the relay has no impact on the SOP of U_2 when the transmit power is high enough, which is consistent with the asymptotic analysis in Section III-C. Thus, when the transmit power is adequate, we can equip only minimum required antennas at the relay to achieve reliable performance, i.e., $N_t = N_r = 2$.

In Fig. 7, the secrecy performance of U_1 and U_2 in the proposed FDJam scheme are compared with different power allocation between confidential and jamming signals. Three cases of $P_T = -10$dBm, $P_T = 0$dBm and $P_T = 10$dBm are considered. From the results, we can observe that the SOP of U_1 decreases first, and then increases as $\frac{\eta}{1+\eta}$ varys. This reveals that there exists a power tradeoff between the confidential and jamming signals for U_1, i.e., a tradeoff should be made between the transmission reliability and security when P_T is limited, and η should be carefully chosen to achieve better security for U_1. On the other hand, we can see that there is also a tradeoff for the secrecy performance of U_2 with η. Thus, more transmit power should be allocated for the jamming signal to achieve optimal performance of security, with increasing P_T.

Then, the impact of the locations of U_1 and eavesdropper on the SOP of U_1 is studied for the three schemes in Fig. 8. $\eta = 99$. From the results, we can find that the SOP of U_1 becomes better with smaller d_{su1} and larger d_{se}. Moreover, when $d_{se} < d_{su1}$, the SOP of U_1 in both HDJam and FDNoJam schemes increases severely, while in the proposed FDJam scheme, the performance deteriorates only a little

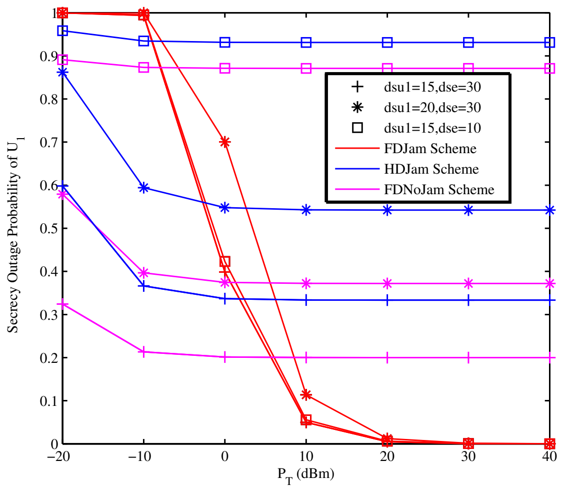

Fig. 8. Comparison of secrecy outage probability of U_1 for the three schemes under varying P_T, with different locations of U_1 and eavesdropper.

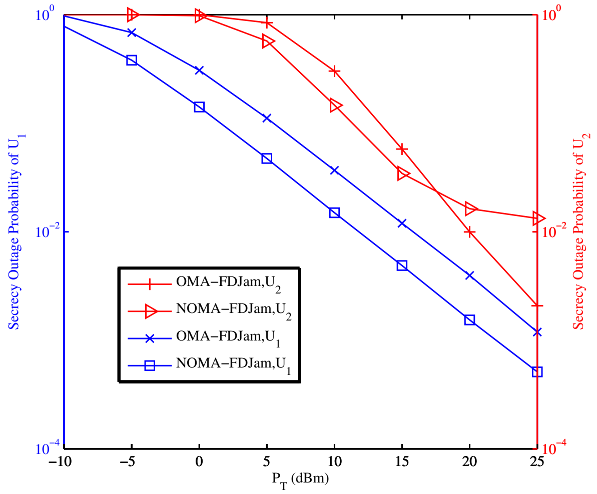

Fig. 10. Comparison of secrecy outage probability of U_1 and U_2 for the OMA-FDJam and NOMA-FDJam scheme with varying P_T.

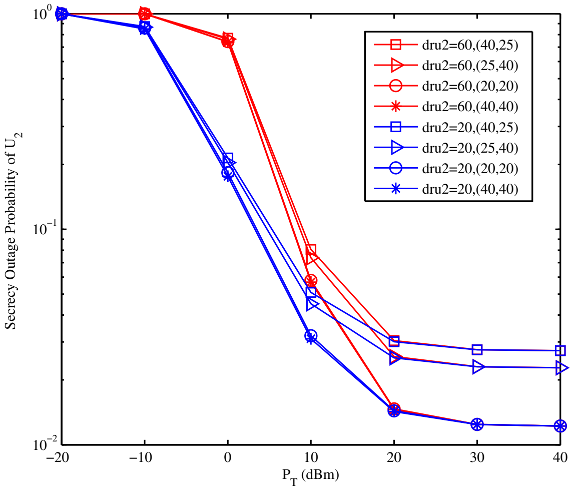

Fig. 9. Comparison of secrecy outage probability of U_2 for the FDJam scheme with different locations of U_2, BS and eavesdropper, under varying P_T.

due to the generated jamming signal at the FD relay. Thus, compared with the other two schemes, the FDJam scheme has a better performance to disrupt the closer eavesdropping. We can also see that the SOP of U_1 in the FDJam scheme is always approximated to zero at high transmit power, with different locations of U_1 and eavesdropper. However, for the other two schemes, their asymptotic SOP will be reduced to a positive constant at high transmit power, which will also decrease as d_{su1} decreases and d_{se} increases. All these results are perfectly consistent with the asymptotic analysis in Sections III and IV.

In Fig. 9, the SOP of U_2 in the FDJam scheme is compared for different locations of the U_2, BS and eavesdropper, under varying P_T. Two cases of $d_{ru2} = 20$m and $d_{ru2} = 60$m are considered. $\eta = 99$. Four groups of (d_{se}, d_{re}) are involved, i.e., (20,20), (40,40), (40,25) and (25,40). From the results, we can see that as P_T increases, the SOP of U_2 is declined, which is consistent with the results in Fig. 3 and Fig. 6. Also, when the transmit power is relatively high, the SOP of U_2 tends to be the same constant with different d_{ru2}, while the distances d_{se} and d_{re} can actually affect the secrecy performance. These results are in accord with the asymptotic analysis in Section III. Interestingly, when the BS and the relay are both away from or close to the eavesdropper, the SOP performance is almost the same, as shown in Fig. 9, due to the fact that the strength of jamming and confidential signal will become smaller or larger simultaneously, under the conditions of $(20, 20)$ and $(40, 40)$, respectively.

Finally, we also design a FDJam scheme based on orthogonal multiple access (OMA), i.e., the OMA-FDJam scheme, as a benchmark, and compare its secrecy performance with the proposed NOMA-FDJam scheme. For the OMA-FDJam scheme, the transmission process during each time slot is divided into three stages in average. In the first and second stage, the BS transmits the message $s1$ and s_2 to U_1 and the relay, respectively, and the relay sends jamming signal to disturb the eavesdropping. In the third stage, the relay forwards the message s_2 to U_2 and the BS transmits the jamming signal to protect its security. From the results in Fig. 10, we can observe that the SOP of U_1 in the OMA-FDJam scheme is lower than that in the NOMA-FDJam scheme due to the fact that less wireless resource can be allocated for the transmission of U_1 in the former scheme. As for U_2, its secrecy performance in the NOMA-FDJam scheme is superior to that in the OMA-FDJam scheme when the transmit power is low, whereas becomes worse when the transmit power is high. This is because more wireless resource can be available at U_2 in the NOMA-FDJam scheme, while the error floor will occur with $P \to \infty$ due to the inter-user interference existing in the transmission rate of U_2, which can be demonstrated in (44). In addition, it is worth noting that three transmission stages are involved to perform the security transmission for both NOMA users in the OMA-FDJam scheme, which will make the system design more intractable. Furthermore, we assume fixed power allocation, i.e., η, α_1 and α_2 are unchanged according to P_T, due to the fact that the power allocation is out of the scope of this paper. Nevertheless, if we can change the values of η, α_1 and α_2 according to the varying of P_T, the error floor of U_2

in our proposed scheme can be further reduced significantly.

VI. Conclusions

In this paper, we have considered the downlink NOMA system assisted by a multi-antenna FD relay and investigated its secrecy performance with the presentence of an eavesdropper. To guarantee the secure transmission, a two-stage jamming scheme, the FDJam scheme, was proposed, and the beamforming of relay was designed to cancel the self-interference and the jamming signal at the relay and legitimate node, respectively. The close-form expressions of SOP were derived for the NOMA users to evaluate the secrecy capability of the proposed scheme, and the asymptotic SOP analysis was provided as well. In addition, two benchmark schemes of HDJam and FDNoJam were also designed and analyzed to validate the effectiveness of the FDJam scheme. Simulation results were presented to show that the analytical results of SOP were perfectly consistent with the Monte Carlo results, and the proposed FDJam scheme can significantly improve the secrecy performance via multi-antenna FD relay and jamming.

Appendix A
Proof of Proposition 1

The SOP for U_1 in (30) can be equivalent to

$$P_{sop1} = \underbrace{\int_{\nu}^{\infty} F_X(\varphi(z)) f_Z(z) dz}_{I_1} - \underbrace{\int_{\nu}^{\infty} F_X(\xi) f_Z(z) dz}_{I_2} + F_X(\xi), \tag{80}$$

which is discussed in the following two cases.

Case 1: When $\nu \leq 0$, the probability of $\Pr(\xi < X < \varphi(z))$ does not exist with $\nu < z < 0$, which means $z \in (0, \infty)$. Thus, the part I_2 in (80) can be rewritten as

$$\begin{aligned} I_2 &= \int_0^{\infty} F_X(\xi) f_Z(z) dz = F_X(\xi) \int_0^{\infty} f_Z(z) dz \\ &= F_X(\xi) \lambda \int_0^{\infty} e^{-\lambda_1 z \sigma^2} \left(\frac{\sigma^2}{\lambda_1 z + \lambda_2} + \frac{1}{(\lambda_1 z + \lambda_2)^2} \right) dz \\ &= F_X(\xi) I_{21}. \end{aligned} \tag{81}$$

According to the results in [43], I_{21} can be calculated as

$$I_{21} = \lambda_2 \sigma^2 \left(-e^{\lambda_2 \sigma^2} Ei\left(-\lambda_2 \sigma^2\right) + e^{\lambda_2 \sigma^2} Ei\left(-\lambda_2 \sigma^2\right) + \frac{1}{\lambda_2 \sigma^2} \right). \tag{82}$$

Apparently, $I_{21} = 1$, and we can obtain $I_2 = F_X(\xi)$.

Subsequently, I_1 can be expressed as

$$I_1 = \int_0^{\infty} F_X(\varphi(z)) f_Z(z) dz = I_{21} + I_{11}, \tag{83}$$

where I_{11} should be organized as

$$\begin{aligned} I_{11} = &-\lambda \exp\left(-\lambda_1 \left(d_{su1}/d_{se}\right)^{\alpha} \sigma^2 \left(2^{2R_{s1}} - 1\right)\right) \\ &\int_0^{\infty} \exp(-\lambda_1 z \mu) \left(\frac{\sigma^2}{\lambda_1 z + \lambda_2} + \frac{1}{(\lambda_1 z + \lambda_2)^2} \right) dz, \end{aligned} \tag{84}$$

where $\mu = \sigma^2 \left(\left(\frac{d_{su1}}{d_{se}} \right)^{\alpha} 2^{2R_{s1}} + 1 \right)$. Similarly, with the results in [43] adopted, we can calculate the integral I_{11} as

$$\begin{aligned} I_{11} = &-\lambda_2 \exp\left(-\lambda_1 \left(d_{su1}/d_{se}\right)^{\alpha} \sigma^2 \left(2^{2R_{s1}} - 1\right)\right) \times \\ &\left(1/\lambda_2 + \left(d_{su1}/d_{se}\right)^{\alpha} 2^{2R_{s1}} \sigma^2 \exp(\lambda_2 \mu) Ei(-\lambda_2 \mu)\right). \end{aligned} \tag{85}$$

With all above, the SOP for U_1 can be obtained as

$$P_{sop1} = I_1 - I_2 + F_X(\xi) = 1 + I_{11}. \tag{86}$$

Case 2: When $\nu > 0$, the integral I_{21} can be changed as

$$I_{21} = \lambda_2 \exp\left(-\lambda_1 \nu \sigma^2\right) / \left(\lambda_1 \nu + \lambda_2\right), \tag{87}$$

Furthermore, the result of I_{11} should be replaced with

$$\begin{aligned} I_{11} = &-\lambda_2 \exp\left(-\lambda_1 \left(d_{su1}/d_{se}\right)^{\alpha} \sigma^2 \left(2^{2R_{s1}} - 1\right)\right) \times \\ &\left(\left(d_{su1}/d_{se}\right)^{\alpha} 2^{2R_{s1}} \sigma^2 \exp(\lambda_2 \mu) Ei(-(\lambda_1 \nu + \lambda_2) \mu) + \zeta \right), \end{aligned} \tag{88}$$

where $\zeta = \exp(-\lambda_1 \nu \mu)/(\lambda_1 \nu + \lambda_2)$. Thus, with $\nu > 0$, we can calculate the SOP for U_1 as

$$P_{sop1} = \left(1 - F_X(\xi)\right) I_{21} + I_{11} + F_X(\xi). \tag{89}$$

Combining (86) and (89), (34) can be achieved.

Appendix B
Proof of Lemma 3.1

Define RVs $Q_1 = 1 + \gamma_{1,r}^{[2]}$, $Q_2 = 1 + \gamma_{2,u_2}^{[2]}$ and $Q_3 = 1 + \gamma_{1,u_1}^{[2]}$. The CDF for the RV Q can be calculated as

$$\begin{aligned} F_Q(q) = &\Pr\left(\min\left\{Q_1, Q_2, Q_3\right\} < q\right) \\ = &1 - (1 - F_{Q_1}(q))(1 - F_{Q_2}(q))(1 - F_{Q_3}(q)), \end{aligned} \tag{90}$$

where $F_{Q_1}(q)$, $F_{Q_2}(q)$ and $F_{Q_3}(q)$ denote the CDF of Q_1, Q_2 and Q_3, respectively. For Q_1, due to the fact that $\left|\mathbf{u}_r^{\dagger} \mathbf{h}_{sr}\right|^2$ follows the Gamma distribution with $(N_r - 1, \beta_0 d_{sr}^{-\alpha})$, where $(N_r - 1)$ and $\theta_1 = \beta_0 d_{sr}^{-\alpha}$ are the shape and scale parameters, respectively, the CDF for Q_1 can be obtained as

$$F_{Q_1}(q) = 1 - e^{-\frac{\zeta(q)}{P\theta_1}} \sum_{i=0}^{N_r - 2} \frac{1}{i!} \left(\frac{\zeta(q)}{P\theta_1} \right)^i = 1 - g_1(q), \tag{91}$$

where $\zeta(q) = \frac{(q-1)\sigma^2}{\alpha_2 - (q-1)\alpha_1}$. When $\zeta(q) > 0$, i.e., $1 < q < 1/\alpha_1$, (91) is held. Thus,

$$F_{Q_1}(q) = \begin{cases} 0 & q < 1, \\ 1 - g_1(q) & 1 < q < \frac{1}{\alpha_1}, \\ 1 & q > \frac{1}{\alpha_1}, \end{cases} \tag{92}$$

For Q_2, it can be known that $\left|\mathbf{h}_{ru_2} \mathbf{w}\right|^2$ subjects to a Gamma distribution with (N_t, θ_2), where $\theta_2 = \frac{P\beta_0 d_{ru_2}^{-\alpha}}{\sigma^2}$. Hence, the CDF of Q_2 can be expressed as

$$F_{Q_2}(q) = 1 - e^{-\frac{q-1}{\theta_2}} \sum_{i=0}^{N_t - 1} \frac{1}{i!} \left(\frac{q-1}{\theta_2} \right)^i = 1 - g_2(q). \tag{93}$$

Note that (93) is satisfied with $q > 1$, otherwise, $F_{Q_2}(q) = 0$.

Besides, based on (27), the CDF of Q_3 can be denoted as

$$F_{Q_3}(q) = 1 - e^{-\lambda_0 \frac{\zeta(q)}{P}} = 1 - g_3(q), \tag{94}$$

where $\zeta(q)$ is the same as that in (91). Substituting (92), (93) and (94) into (90), we can obtain

$$F_Q(q) = \begin{cases} 0 & q < 1, \\ 1 - g_1(q) g_2(q) g_3(q) & 1 < q < \frac{1}{\alpha_1}, \\ 1 & q > \frac{1}{\alpha_1}. \end{cases}$$

Appendix C
Proof of Lemma 3.2

Assume that $V_1 = 1 + \gamma_{1,e}^{[2]}$ and $V_2 = \gamma_{2,e}^{[2]}$. According to Lemma 2, the PDF of V_1 can be denoted as

$$f_{V_1}(v_1) = p_0 e^{-p_1(v_1-1)\sigma^2}\left(\frac{\sigma^2}{p_1(v_1-1)+p_2}+\frac{1}{(p_1(v_1-1)+p_2)^2}\right), \quad (95)$$

where $p_1 = 1/(\beta_0 d_{se}^{-\alpha}\alpha_2 P)$, $p_2 = 1/(\beta_0 d_{re}^{-\alpha}\eta P)$ and $p_0 = p_1 p_2$. Similarly, the PDF of V_2 can be derived as

$$f_{V_2}(v_2) = p e^{-p_3 v_2 \sigma^2}\left(\frac{\sigma^2}{p_3 v_2 + p_4}+\frac{1}{(p_3 v_2 + p_4)^2}\right), \quad (96)$$

where $p_3 = 1/(\beta_0 d_{re}^{-\alpha} P)$, $p_4 = 1/(\beta_0 d_{se}^{-\alpha}\eta P)$ and $p = p_3 p_4$.

Combining (95) and (96), we can obtain the PDF of V as

$$f_V(v) = \int_1^v f_{V_1}(v_1) f_{V_2}(v - v_1) dv_1. \quad (97)$$

The accurate solution for (97) is difficult to calculate. Thus, the Chebyshev-Guass quadrature is performed to find its approximation, and (97) can be derived as $f_V(v) = \frac{\pi}{L}\frac{v-1}{2}\sum_{l=1}^{L}\sqrt{1-x_l^2} f_{V_1}\left(\frac{v-1}{2}x_l + \frac{v+1}{2}\right) f_{V_2}\left(v - \left(\frac{v-1}{2}x_l + \frac{v+1}{2}\right)\right)$, where $x_l = \cos\left(\frac{2l-1}{2L}\pi\right)$, and L denotes the number of nodes set in the Chebyshev-Guass approximation.

References

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C.-L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[2] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[3] Z. Ding, P. Fan, G. K. Karagiannidis, R. Schober, and H. V. Poor, "NOMA assisted wireless caching: Strategies and performance analysis," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4854–4876, Oct. 2018.

[4] L. Dai, B. Wang, Y. Yuan, S. Han, C.-L. I, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sept. 2015.

[5] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart. 2017.

[6] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7244–7257, Nov. 2016.

[7] Z. Chen, Z. Ding, X. Dai, and R. Zhang, "An optimization perspective of the superiority of NOMA compared to conventional OMA," *IEEE Trans. Signal Process.*, vol. 65, no. 19, pp. 5191–5202, Oct. 2017.

[8] N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, and M. Alouini, "Joint trajectory and precoding optimization for UAV-assisted NOMA networks," *IEEE Trans. Commun.*, to be published. DOI: 10.1109/T-COMM.2019.2895831.

[9] N. T. Do, D. B. da Costa, T. Q. Duong, and B. An, "A BNBF user selection scheme for NOMA-based cooperative relaying systems with SWIPT," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 664–667, Mar. 2017.

[10] T. N. Do, D. B. da Costa, T. Q. Duong, and B. An, "Improving the performance of cell-edge users in NOMA systems using cooperative relaying," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 1883–1901, May 2018.

[11] L. Zhang, J. Liu, M. Xiao, G. Wu, Y. Liang, and S. Li, "Performance analysis and optimization in downlink NOMA systems with cooperative full-duplex relaying," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2398–2412, Oct. 2017.

[12] Z. Ding, H. Dai, and H. V. Poor, "Relay selection for cooperative NOMA," *IEEE Wireless Commun. Lett.*, vol. 5, pp. 416–419, Aug. 2016.

[13] C. Zhong and Z. Zhang, "Non-orthogonal multiple access with cooperative full-duplex relaying," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2478–2481, Dec. 2016.

[14] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Exploiting full/half-duplex user relaying in NOMA systems," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 560–575, Feb. 2018.

[15] W. Duan, X. Jiang, M. Wen, J. Wang, and G. Zhang, "Two-stage superposed transmission for cooperative NOMA systems," *IEEE Access*, vol. 6, pp. 3920–3931, 2018.

[16] J. Zhao, Z. Ding, P. Fan, Z. Yang, and G. K. Karagiannidis, "Dual relay selection for cooperative NOMA with distributed space time coding," *IEEE Access*, vol. 6, pp. 20440–20450, 2018.

[17] B. Chen, Y. Chen, Y. Chen, Y. Cao, N. Zhao, and Z. Ding, "A novel spectrum sharing scheme assisted by secondary NOMA relay," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 732–735, Oct. 2018.

[18] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE.*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[19] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.

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

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

[22] T. Lv, H. Gao, R. Cao, and J. Zhou, "Co-ordinated secure beamforming in K-user interference channel with multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 212–215, Apr. 2016.

[23] 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.

[24] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[25] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, J. Tang, and V. C. M. Leung, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[26] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[27] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[28] 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, pp. 574–583, Mar. 2015.

[29] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Apr. 2017.

[30] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, Aug. 2017.

[31] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[32] Y. Liu, Z. Qin, M. Elkashlan, and Y. Gao, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[33] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[34] N. Zhao, W. Wang, J. Wang, Y. Chen, Y. Lin, Z. Ding, and N. C. Beaulieu, "Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2294–2305, Mar. 2019.

[35] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[36] B. Zheng, M. Wen, C. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[37] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, “Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems,” *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4119–4137, Sept. 2018.

[38] K. Yang, J. Yang, J. Wu, C. Xing, and Y. Zhou, “Performance analysis of DF cooperative diversity system with OSTBC over spatially correlated Nakagami-m fading channels,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1270–1281, Mar. 2014.

[39] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, “Physical-layer security for full duplex communications with self-interference mitigation,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[40] T. Riihonen, S. Werner, and R. Wichman, “Mitigation of loopback self-interference in full-duplex MIMO relays,” *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[41] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communications,” *IEEE J. Sel. Areas Commun.*, vol. 30, pp. 359–368, Feb. 2012.

[42] J. Kim and I. Lee, “Non-orthogonal multiple access in coordinated direct and relay transmission,” *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 2037–2040, Nov. 2015.

[43] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*. New York: Academic Press, 7th ed., 2007.

Yang Cao is currently pursuing Ph.D. degree in the School of Information and Communication Engineering at Dalian University of Technology, China. She received the B.S. degree from HeFei University of Technology, China.

Her current research interests include non-orthogonal multiple access, interference alignment, physical layer security, wireless energy harvesting, and resource allocation.

Nan Zhao (S’08-M’11-SM’16) is currently an Associate Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China.

Dr. Zhao is serving or served on the editorial boards of 7 SCI-indexed journals, including IEEE Transactions on Green Communications and Networking. He won the best paper awards in IEEE VTC 2017 Spring, MLICOM 2017, ICNC 2018, WCSP 2018 and CSPS 2018. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.

Gaofeng Pan (M’12) received his B.Sc 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 Sept. 2009 to April 2011 as a joint-trained PhD student under the supervision of Prof. Eylem Ekici. From May 2012 to April 2019, he was with Southwest University, Chongqing, China, and he was also with School of Computing and Communications, Lancaster University, Lancaster, U.K., from Jan. 2016 to Jan. 2018, where he was a postdoc under the supervision of Prof. Zhiguo Ding. Since April 2019, he has been with School of Information and Electronics, Beijing Institute of Technology, P. R. China, as a professor.

Yunfei Chen (S’02-M’06-SM’10) received his B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, P.R.China, in 1998 and 2001, respectively. He received his Ph.D. degree from the University of Alberta in 2006. He is currently working as an Associate Professor at the University of Warwick, U.K. His research interests include wireless communications, cognitive radios, wireless relaying and energy harvesting.

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinacom 2014.

Minglu Jin (M’96) received the B.S degree from University of Science and Technology in 1982, M.S. and Ph. D degrees from Beijing University of Aeronautics and Astronautics in 1984 and 1995, respectively. He was a Visiting scholar in the Arimoto Lab. at Osaka University, Osaka, Japan, from 1987 to 1988. He was a Research Fellow in Radio & Broadcasting Research Lab at Electronics Telecommunications Research Institute (ETRI), Korea from 2001 to 2004. He is currently a professor at Dalian University of Technology. His research interests include wireless communication, wireless sensor networks, signal processing for wireless communication system.

Mohamed-Slim Alouini (S’94-M’98-SM’03-F’09) was born in Tunis, Tunisia. He received the Ph.D. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.