Non-orthogonal Multiple Access and Artificial-Noise Aided Secure Transmission in FD Relay Networks

Youhong Feng†*, Zhen Yang†, and Shihao Yan‡
†Key Laboratory of Ministry of Education in Broadband Wireless Communication and Sensor Network Technology
Nanjing University of Posts and Telecommunications, China
*College of Physics and Electronic Information Engineering, Anhui Normal University, China
‡Research School of Engineering, The Australian National University, Canberra, ACT 0200, Australia
Emails: 2013010213@njupt.edu.cn, yangz@njupt.edu.cn, shihao.yan@anu.edu.au

***Abstract*—In this paper, we investigate an artificial-noise (AN) aided secure transmission for non-orthogonal multiple access (NOMA) full-duplex (FD) relay network. We propose a novel joint NOMA and AN-aided full-duplex relay (NOMA-ANFDR) scheme to enhance the physical security. In this scheme, the optimal power allocation between the information and the AN signal is determined such that the capacity of the two end-to-end (i.e., two source-relay-destination pairs) channel are maximized to ensure the highest quality of cooperative transmission. To fully examine the benefits of the NOMA-ANFDR scheme, we derive a new closed-form expression for the secrecy outage probability. We show that the NOMA-ANFDR scheme significantly outperforms the joint NOMA and AN in half-duplex relay (NOMA-ANHDR) scheme as well as the NOMA-HDR scheme in terms of minimum secrecy outage probability and effect secrecy throughout. This result indicates that adopting the joint of FD and AN technique at relays can effectively enhance the physical layer secrecy performance in the NOMA cooperative network.**

I. Introduction

Recently, non-orthogonal multiple access (NOMA) has received enormous interests since it can significantly boost the system spectral efficiency [1]. Different from the conventional orthogonal multiple access methods such as frequency division multiple access, time division orthogonal multiple access, and code division multiple access, NOMA allows multiple users to share the same resource block (i.e., time/frequency/code), in which successive interference cancellation (SIC) has to be performed at one receiver to suppress the interference caused by other users' information.

In [2], cooperative NOMA with maximum ratio combining was studied to enhance the spatial diversity. In [3], different relay selection strategies were proposed and analyzed in cooperative NOMA systems. In [4], outage probability and ergodic sum capacity were investigated in a NOMA system with coordinated direct and relay transmission. In [5], two source-destination user pairs sharing a common half-duplex relay was investigated in NOMA cooperative system. It is noted that cooperative NOMA introduced in [2–5] all adopt half-duplex cooperative relay mode. Meanwhile, the security of wireless communication is a pivotal issue that needs to be addressed in wireless networks. As a complimentary approach to the traditional cryptographic techniques, physical layer security has been recognized as a key solution to safeguard wireless data transmissions and thus attracted numerous research interests [6]. In the context of physical layer security, many technologies, such as artificial-noise (AN)-aided transmission, full-duplex techniques, and cooperative relay transmission, have been proposed to enhance the secrecy performance of wireless communications [7–13]. Specially, Generating AN at the legitimate transmitter is proposed to be an effective technique to confound the eavesdropper [8–12]. Cooperative full-duplex relay has also been proved as an effective way to improve the system security [9]. In [7], a physical layer security based on AN-aided strategy was first considered in relay networks, which can largely improve the physical-layer security. Motivated by the benefits of relay and AN assistance, many researchers have investigated various secure transmission strategies, such as cooperative beamforming (CB) [8] and cooperative jamming (CJ) [9].

Although physical layer security has been well studied in many scenarios, the design of secrecy transmission for NOMA cooperative is still not clear. The aim of this work is to examine the secure performance of NOMA protocol in cooperative networks. To answer this important question, we focus on a similar scenario considered in [5]. However, the authors did not consider the existence of eavesdropping users. Furthermore, in order to improve the security of the systems, AN-aided and full-duplex methods are applied in this communication scenario.

In this work, we exploit the use of AN-aided and full-duplex (FD) strategies at relay node to enhance the secrecy in NOMA cooperative networks. Specifically, we propose a novel joint NOMA and AN-aided full-duplex relay (NOMA-ANFDR) scheme. In this scheme, the optimal power allocation between the information and the AN signal is determined such that the capacity of the two end-to-end (i.e., two source-relay-destination pairs) channel are maximized to ensure the highest quality of cooperative transmission. To disclose the benefits of the NOMA-ANFDR scheme relative to the joint NOMA and AN-aided half-duplex relay scheme (NOMA-

978-1-5386-3920-7/17/$31.00 ©2017 IEEE

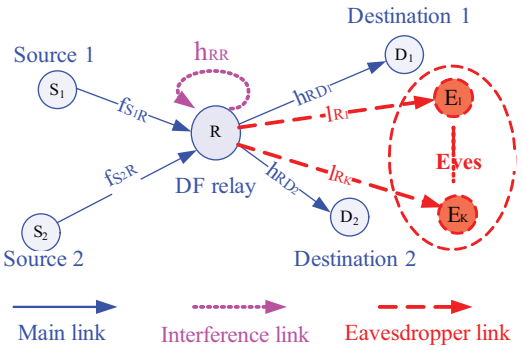

Fig. 1. System model

ANFDR), we derive a new closed-form expression for the secrecy outage probability of the NOMA-ANFDR scheme. We also derive the secrecy outage probability of the NOMA-ANHDR scheme as a benchmark. Our analysis demonstrates that the NOMA-ANFDR scheme significantly outperforms the NOMA-ANHDR scheme by achieving a lower secrecy outage probability and a higher effect secrecy throughout when the self-interference at the FD relay can be reasonably suppressed. Furthermore,we also compare the AN-aided schemes (i.e., the NOMA-ANFDR and NOMA-ANFDR schemes) with joint NOMA and half-duplex relay scheme (NOMA-FDR) , Our analysis demonstrates that the AN-aided schemes perform significantly than the NOMA-HDR scheme.

II. Proposed NOMA-ANFDR Scheme in a Common Full-duplex-DF-Relay Network

We consider a secure cooperative relay network, as illustrated in Fig. 1, in which two source-destination pairs S_1-D_1 and S_2-D_2 share a common FD decode-and-forward (DF) relay R. All nodes in networks are equipped with a single antenna and operative in the full-duplex DF mode. We assume that K eavesdroppers (E) exists in this network and overhears the transmission from the relay. Similar to [5], we also assume that the direct links from S to D and E are not available due to the strong path-loss and attenuation between them. In this case, both S_1 and S_2 only rely on R to communicate simultaneously with their corresponding receivers D_1 and D_2, respectively. This assumption can be justified in case of urban areas where nodes are placed far apart, and is also in line with previous researches such as [3, 5].

In this work, we assume that all channels experience block Rayleigh fading such that the channels remain constant over one block but vary independently from one block to another [9], and we denote $f_{S_1,R} \sim \mathcal{CN}(0, d_{1R}^{-v})$, $f_{S_2,R} \sim \mathcal{CN}(0, d_{2R}^{-v})$, $h_{R,D_1} \sim \mathcal{CN}(0, d_{RD_1}^{-v})$, $h_{R,D_2} \sim \mathcal{CN}(0, d_{RD_2}^{-v})$, and $l_{R,E_k} \sim \mathcal{CN}(0, d_{RE_k}^{-v})$ as the channel coefficients of the S_1-R, S_2-R, $R-D_1$, $R-D_2$, and $R-E_k$ links, respectively. We denote P_S and P_R as the transmit power at S and R, respectively. We then denote that $n_{\mathrm{R}} \sim \mathcal{CN}(0, \sigma_{\mathrm{R}}^2)$, $n_{\mathrm{D}} \sim \mathcal{CN}(0, \sigma_{\mathrm{D}}^2)$, and $n_{\mathrm{E}} \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2)$ as the complex additive white Gaussian noise components at R, D, and E, respectively. where v is the path loss exponent and d represents the distance in meters. In our considered network, it is anticipated that $|f_{S_1,R}| > |f_{S_2,R}|$ and $|d_{RD_2}| > |d_{RD_1}|$ because it is assumed that $d_{1R} < d_{2R}$ and $d_{RD_2} < d_{RD_1}$.

A. Information Received and Decoded on Relay

We assumed that, at the $n-$th time slot, both S_1 and S_2 simultaneously transmit symbols $x_1[n]$ and $x_2[n]$ with powers $\alpha_1 P_S$ and $\alpha_2 P_S$ to the relay, respectively, where P_S is the total transmit power constraint, α_1 and α_2 denote power allocation coefficients, such that $\alpha_1+\alpha_2 = 1$ and $\alpha_1 > \alpha_2$. It is assumed that S_1 and S_2 have some sort of cooperation and based on that, power is distributed between them to meet the total transmission power requirement. Note that the total transmit power requirement is essential for many practical scenarios [5, 15]. Similar to [5, 15], uplink NOMA method is used, the relay first decodes the better source symbol $x_1[n]$ by treating the symbol $x_2[n]$ of worse source as noise. We consider a FD relay in this communication scenario, and also assume that the relay transmit symbols $x_1[n]$ and $x_2[n]$ with powers $\alpha_3 P_R$ and $\alpha_4 P_R$ to D_1 and D_2, respectively, where P_R is the total transmit power at relay. Then, the relay performs SIC to obtain symbol $x_2[n]$. Thus, the received signal-to-interference-plus-noise ratio (SINR) for symbol $x_1[n]$ and signal-to-plus-noise (SNR) for symbol $x_2[n]$ at the relay are given by

$$\begin{aligned}\gamma_{x_1}^{u} &= \frac{\alpha_1 P_S |f_{S_1,R}|^2}{\alpha_2 P_S |f_{S_2,R}|^2 + P_R |h_{R,R}|^2 + \sigma_R^2} \\ &= \frac{\alpha_1 \rho_S |f_{S_1,R}|^2}{\alpha_2 \rho_S |f_{S_2,R}|^2 + \rho_R |h_{R,R}|^2 + 1},\end{aligned} \tag{1}$$

and

$$\gamma_{x_2}^{u} = \frac{\alpha_2 P_S |f_{S_2,R}|^2}{P_R |h_{R,R}|^2 + \sigma_R^2} = \frac{\alpha_2 \rho_S |f_{S_2,R}|^2}{\rho_{RR} |h_{R,R}|^2 + 1}, \tag{2}$$

respectively, where $\rho_S = \frac{P_S}{\sigma_R^2}$ and $\rho_{RR} = \frac{P_R}{\sigma_R^2}$, $h_{R,R} \sim \mathcal{CN}(0, \lambda_{RR})$ denotes channel coefficient for the relay self-interference channel. It is noted that the self-interference can be significantly suppressed so that $h_{R,R}$ can be regarded as an independent Rayleigh distributed variable [9].

B. Information Received and Decoded on Destinations

Recalling to the downlink NOMA in [5, 14], in which a superimposed composite signal are regenerated and transmitted. In our considered network, in order to improve the security of information transmission, similar to [8, 12], we proposed the use of so-called artificial noise aided secure transmission in the relay. As such, by adopting the superposition code, the transmitted signal at the relay is given by

$$S[n] = \sqrt{\alpha_3 P_R} x_1[n] + \sqrt{\alpha_4 P_R} x_2[n] + \sqrt{\alpha_5 P_R} x_a, \tag{3}$$

where $x_1[n]$ and $x_2[n]$ are the regenerated data symbols at during $n-$th time slot, x_a is an an artificial noise used to defend against eavesdropping, and α_5 denote power allocation coefficient for artificial noise, such that $\alpha_3+\alpha_4+\alpha_5 = 1$ and $\alpha_3 > \alpha_4$. In this paper, we assume that the artificial noise transmitted by the relay is generated from a pseudo random sequence, which is known to the legitimate receivers (i.e., R,

D_1, and D_2) and remains unknown to the eavesdroppers [8, 12]. Furthermore, according to NOMA protocol, D_1 decodes own symbol $x_1[n]$ by treating $x_2[n]$ as noise. Therefore, the received SINR at D_1 for symbols $x_1[n]$ is given as

$$\gamma_{x_1}^d = \frac{\alpha_3 P_R |h_{R,D_1}|^2}{\alpha_4 P_R |h_{R,D_1}|^2 + \sigma_D^2} = \frac{\alpha_3 \rho_R |h_{R,D_1}|^2}{\alpha_4 \rho_R |h_{R,D_1}|^2 + 1}, \quad (4)$$

where $\rho_R = \frac{P_R}{\sigma_D^2}$. On the other hand, according to NOMA protocol, the destination node with the stronger channel condition (i.e., D_2) needs to firstly detect its partner's information (i.e.,D_1) and then to obtain own information x_2 using SIC. Thus, the received SINR for x_1 and SNR for x_2 at D_2 are respectively given by

$$\gamma_{x_1 \to x_2}^d = \frac{\alpha_3 P_R |h_{R,D_2}|^2}{\alpha_4 P_R |h_{R,D_2}|^2 + \sigma_D^2} = \frac{\alpha_3 \rho_R |h_{R,D_2}|^2}{\alpha_4 \rho_R |h_{R,D_2}|^2 + 1}, \quad (5)$$

and

$$\gamma_{x_2}^d = \frac{\alpha_4 P_R |h_{R,D_2}|^2}{\sigma_D^2} = \alpha_4 \rho_R |h_{R,D_2}|^2, \quad (6)$$

where $x_1 \to x_2$ denotes the SINR required at D_2 to decode symbol x_1.

On the other hand, for eavesdroppers, following the similar assumption, we consider the worst-case scenario of large-scale networks in which eavesdroppers are assumed to have strong detection abilities and distinguished legal data stream from the relay [14]. Therefore, the instantaneous SINR for detecting the legal information of $x_1[n]$ and $x_2[n]$ at the most detrimental eavesdropper can be expressed as follows:

$$\begin{aligned} \gamma_{E_\iota} &= \max_{k=1,\cdots,K} \frac{\alpha_\iota P_R |l_{R,E_k}|^2}{\alpha_5 P_R |l_{R,E_k}|^2 + \sigma_E^2} \\ &= \max_{k=1,\cdots,K} \frac{\alpha_\iota \rho_E |l_{R,E_k}|^2}{\alpha_5 \rho_E |l_{R,E_k}|^2 + 1}, \end{aligned} \quad (7)$$

where $\iota \in \{3, 4\}$, $\rho_E = \frac{P_R}{\sigma_E^2}$ is the transmit SNR, σ_E^2 is the variance of AWGN at eavesdroppers.

III. New Channel Statistics

In this section, we derive several new channel statistics for destinations and eavesdroppers, which will be used to derive the secrecy outage probability in the next section.

Theorem 1: Conditioned on the two source-destination pairs $S_1 - D_1$ and $S_2 - D_2$ share a common DF relay in considered NOMA networks and the relay using the AN to confuse eavesdroppers, the PDF of the most detrimental eavesdropper γ_{E_ι} is given by (8)

$$f_{\gamma_{E_\iota}}(x) = \begin{cases} K \sum_{k=0}^{K-1} \binom{K-1}{k} \frac{(-1)^k \alpha_\iota e^{-\frac{(k+1)x}{\pi_{RE}(\alpha_\iota - \alpha_5 x)}}}{\pi_{RE}(\alpha_\iota - \alpha_5 x)^2}, & x \le \frac{\alpha_\iota}{\alpha_5}, \\ 0, & x > \frac{\alpha_\iota}{\alpha_5}, \end{cases} \quad (8)$$

where $\pi_{RE} = \rho_R d_{RE}^{-v}$.

Proof: From (7), and let $X_k = \frac{\alpha_\iota \rho_E |l_{R,E_k}|^2}{\alpha_5 \rho_E |l_{R,E_2}|^2 + 1} = \frac{\alpha_\iota X}{\alpha_5 X + 1}$, we can obtain the CDF of X_k as

$$\begin{aligned} F_{X_k}(x) &= \Pr\left(\frac{\alpha_\iota X}{\alpha_5 X + 1} < x\right) = \Pr\left(X < \frac{x}{\alpha_\iota - \alpha_5 x}\right) \\ &= \begin{cases} 1 - e^{-\left(\frac{x}{\pi_{RE}(\alpha_\iota - \alpha_5 x)}\right)}, & x \le \frac{\alpha_\iota}{\alpha_5}, \\ 1, & x > \frac{\alpha_\iota}{\alpha_5}, \end{cases} \end{aligned} \quad (9)$$

and we can obtain the PDF of X_k as

$$f_{X_k}(x) = \begin{cases} \frac{\alpha_\iota \pi_{RE} e^{-\frac{x}{\pi_{RE}(\alpha_\iota - \alpha_5 x)}}}{(\pi_{RE}(\alpha_\iota - \alpha_5 x))^2} & x \le \frac{\alpha_\iota}{\alpha_5}, \\ 0, & x > \frac{\alpha_\iota}{\alpha_5}. \end{cases} \quad (10)$$

We further obtain the CDF of γ_{E_ι} as follows

$$F_{\gamma_{E_\iota}}(x) = \Pr\{\gamma_{E_\iota} < x\} = \Pr\{\max_{k=1,\cdots,K} X_k < x\} = F_{X_k}(x)^K. \quad (11)$$

Based on (9), (10), (11), and performing some mathematical manipulations, we obtain (8), which completes the proof of Theorem 1. ■

Theorem 2: Conditioned on the two source-destination pairs $S_1 - D_1$ and $S_2 - D_2$ share a common DF relay in considered NOMA networks, the cumulative distribution function (CDF) of SINR (SNR) for symbol x_1 is given by (12)

$$F_X^{S_1 D_1}(x) = \begin{cases} 1 - \left(\frac{c_1}{\frac{1}{\pi_{RR}} + \frac{x}{\alpha_1 \pi_{S_1 R}}} + \frac{c_2}{\frac{1}{\alpha_2 \pi_{S_2 R}} + \frac{x}{\alpha_1 \pi_{S_1 R}}}\right) \\ \quad \times e^{-\left(\frac{\pi_{RD_1}^{-1} + \pi_{RD_2}^{-1}}{\alpha_3 - \alpha_4 x} + \frac{1}{\alpha_1 \pi_{S_1 R}}\right) x}, & x \le \frac{\alpha_3}{\alpha_4}, \\ 1, & x > \frac{\alpha_3}{\alpha_4}, \end{cases} \quad (12)$$

where $c_1 = \frac{1}{\pi_{RR}}(1 - \frac{\alpha_2 \pi_{S_2 R}}{\pi_{RR}})^{-1}$, $c_2 = \frac{1}{\alpha_2 \pi_{S_2 R}}(1 - \frac{\pi_{RR}}{\alpha_2 \pi_{S_2 R}})^{-1}$, $\pi_{S_1 R} = \rho_S d_{1R}^{-v}$, $\pi_{S_2 R} = \rho_S d_{2R}^{-v}$, $\pi_{RD_1} = \rho_R d_{RD_1}^{-v}$, $\pi_{RD_2} = \rho_R d_{RD_2}^{-v}$, and $\pi_{RR} = \rho_{RR} \lambda_{RR}$.

Proof: Bying using (1), (4), and (5), the achievable SINR(SNR) associated with symbol x_1 is given by

$$\rho_{S_1 D_1}(x_1) = \min\{\gamma_{x_1}^u, \gamma_{x_1}^d, \gamma_{x_1 \to x_2}^d\}. \quad (13)$$

Recall (1), and let $Y_1 = |f_{S_1,R}|^2$, $Y_2 = |f_{S_2,R}|^2$, and $Y_3 = |h_{R,R}|^2$, $\gamma_{x_1}^u$ can be reexpressed as $\gamma_{x_1}^u = \frac{\alpha_1 \rho_S Y_1}{\alpha_2 \rho_S Y_2 + \rho_R Y_3 + 1}$. We also assume $Y_4 = \alpha_2 \rho_S Y_2 + \rho_R Y_3$, and we can easily obtain the PDF of x_4 as follows:

$$f_{Y_4}(y) = c_1 e^{-\frac{y}{\pi_{RR}}} + c_2 e^{-\frac{y}{\alpha_2 \pi_{S_2 R}}}. \quad (14)$$

We further reexpress (1) as $X_1 = \frac{\alpha_1 \rho_S Y_1}{Y_4 + 1}$, and the CDF of X_1 can be computed by

$$\begin{aligned} F_{X_1}(x) &= \Pr\{X_1 < x\} = \Pr\left(\frac{\alpha_1 \rho_S Y_1}{Y_4 + 1} < x\right) \\ &= \int_0^\infty [1 - e^{-\frac{x(Y_4+1)}{\alpha_1 \pi_{S_1 R}}}] f_{Y_4}(y) dy. \end{aligned} \quad (15)$$

On the other hand, we let $X_2 = \gamma_{x_1}^d = \frac{\alpha_3 \rho_R |h_{R,D_1}|^2}{\alpha_4 \rho_R |h_{R,D_1}|^2 + 1}$ and $X_3 = \gamma_{x_1 \to x_2}^d = \frac{\alpha_3 \rho_R |h_{R,D_2}|^2}{\alpha_4 \rho_R |h_{R,D_2}|^2 + 1}$. Similar to the analysis in

Theorem 1, we can obtain the CDFs of Y_2 and Y_3 as follows:

$$F_{X_2}(x) = \begin{cases} 1 - e^{-(\frac{x}{\pi_{R,D_1}(\alpha_3-\alpha_4 x)})}, & x \le \frac{\alpha_3}{\alpha_4}, \\ 1, & x > \frac{\alpha_3}{\alpha_4}, \end{cases} \quad (16)$$

and

$$F_{X_3}(x) = \begin{cases} 1 - e^{-(\frac{x}{\pi_{R,D_2}(\alpha_3-\alpha_4 x)})}, & x \le \frac{\alpha_3}{\alpha_4}, \\ 1, & x > \frac{\alpha_3}{\alpha_4}, \end{cases} \quad (17)$$

According to (13)the CDF of $F_X^{S_1D_1}(x)$ can be expressed as

$$F_X^{S_1D_1}(x)=1-(1-F_{X_1}(x))(1-F_{X_2}(x))(1-F_{X_3}(x)). \quad (18)$$

Substituting (14), (15), (16), and (17) into (18), with some mathematical manipulations, we obtain (12), which completes the proof of Theorem 2. ∎

***Theorem** 3:* Conditioned on the two source-destination pairs $S_1 - D_1$ and $S_2 - D_2$ share a common DF relay in the NOMA networks, the CDF of SNR of $S_2 - D_2$ link is given by

$$F_X^{S_2D_2}(x) = 1 - \frac{\alpha_2\pi_{S_2R}e^{-(\frac{1}{\alpha_2\pi_{S_2R}}+\frac{1}{\alpha_4\pi_{RD_2}})x}}{\alpha_2\pi_{S_2R}+\pi_{RR}x}, \quad (19)$$

Proof: Bying using (2) and (6), the achievable SINR(SNR) associated with symbol x_2 is given by

$$\rho_{S_2D_2}(x_2) = \min\{\gamma_{x_2}^u, \gamma_{x_2}^d\}. \quad (20)$$

Following similar arguments as that of Theorem 2 for the CDF of (SNR) for symbol x_1, we obtain (19), which completes the proof of Theorem 3. ∎

IV. Secrecy Outage Probability and Effect Secrecy Throughout Analysis

In this paper, the secrecy outage probability (SOP) and effect secrecy throughout(EST) are used as a secrecy performance metric. Additionally, the secrecy capacity of the $S_1 - D_1$ and $S_2 - D_2$ can be expressed as

$$C_{S_1D_1} = \big(\log_2(1+\rho_{S_1D_1}) - \log_2(1+\gamma_{E_3})\big)^+, \quad (21)$$

and

$$C_{S_2D_2} = \big(\log_2(1+\rho_{S_2D_2}) - \log_2(1+\gamma_{E_4})\big)^+, \quad (22)$$

respectively, where $(x)^+ = \max\{x, 0\}$.

A. Exact Secrecy Outage Probability

Given the secrecy information rate R_1 and R_2 for the $S_1 - D_1$ and $S_2 - D_2$, a secrecy outage is declared when the instantaneous secrecy capacity drops below R_1 and R_2, respectively. Based on (21), the SOP for $S_1 - D_1$ is given by

$$\begin{aligned} P_{S_1D_1}(R_1) &= \Pr\{C_{S_1D_1} < R_1\} \\ &= \Pr\{\rho_{S_1D_1} < 2^{R_1}(1+\gamma_{E_3}) - 1\} \\ &= \int_0^\infty F_X^{S_1D_1}\left(2^{R_1}(1+x)-1\right) f_{\gamma_{E_3}}(x)dx. \end{aligned} \quad (23)$$

Based on (12) and (8), and using the assumption $\alpha_3 > \alpha_4$ in Section II, we obtain $P_{S_1D_1}(R_1)$ as (24), shown on the top of next page, where $\theta(x) = \frac{2^{R_1}x+2^{R_1}-1}{\alpha_1\pi_{S_1R}}$, and $\xi = \min((\frac{\alpha_3}{\alpha_4}+1)2^{-R_1}-1, (\frac{\alpha_3}{\alpha_5}+1)2^{-R_1}-1)$. Similarly, for the $S_2 - D_2$ user, based on (22), the SOP is given by

$$\begin{aligned} P_{S_2D_2}(R_2) &= \Pr\{C_{S_2D_2} < R_2\} \\ &= \Pr\{\rho_{S_2D_2} < 2^{R_2}(1+\gamma_{E_4}) - 1\} \\ &= \int_0^\infty F_X^{S_2D_2}\big(2^{R_2}(1+x)-1\big) f_{\gamma_{E_4}}(x)dx. \end{aligned} \quad (25)$$

Substituting (8) and (19) into (25), we can obtain the expression of SOP of the $S_2 - D_2$ user as (26) on the second top of next page. Though the analysis on information decoded for $S_1 - D_1$ and $S_2 - D_2$ user pairs in Section II, we find the secrecy outage occur of the $S_1 - D_1$ user and $S_2 - D_2$ user are independent. In other words, the SOP of the $S_1 - D_1$ user pair has no effect on that of $S_2 - D_2$ user pair and vice versa. As such, the SOP of the proposed NOMA-ANFDR scheme for the considered networks can be expressed as [14]

$$P_{out}^{NOMA-AFRS} = 1 - (1 - P_{S_1D_1})(1 - P_{S_2D_2}). \quad (27)$$

Following a similar procedure to derive the SOP of the proposed NOMA-ANFDR scheme, we can obtain SOP of the NOMA-ANHDR scheme, which is used as a baseline to compare with the proposed NOMA-ANFDR scheme. Specifically, the SOP of the NOMA-ANHDR scheme is given by

$$\begin{aligned} &P_{out}^{NOMA-AHRS} \\ &= 1 - K^2 \sum_{k_1=0}^{K-1}\sum_{k_2=0}^{K-1}(-1)^{k_1+k_2}\binom{K-1}{k_1}\binom{K-1}{k_2}\tau_1\frac{\alpha_3\alpha_4}{\pi_{RE}^2} \\ &\times \varpi(\xi)\int_0^{\frac{\alpha_4}{\alpha_5}} \frac{e^{-\frac{2^{2R_2}x}{\alpha_2\pi_{S_2R}}+\frac{2^{2R_2}x}{\alpha_4\pi_{RD_2}}+\frac{(k_2+1)x}{\pi_{RE}(\alpha_4-\alpha_5x)}}}{(\alpha_4-\alpha_5x)^2}dx, \end{aligned} \quad (28)$$

where

$$\begin{aligned} \varpi(\xi) &= \int_{\tilde{\xi}}^{\frac{\alpha_3}{\alpha_5}} \frac{e^{-\frac{(k_1+1)x}{\pi_{RE}(\alpha_3-\alpha_5x)}}}{(\alpha_3-\alpha_5x)^2}dx \\ &+\int_0^{\tilde{\xi}} \Phi(x)\frac{e^{-\frac{2^{2R_1}x}{\alpha_1\pi_{S_1R}}-\frac{\pi_{RD_1}^{-1}+\pi_{RD_2}^{-1}}{\alpha_3(2^{2R_1}(x+1)-1)^{-1}-\alpha_4}-\frac{\pi_{RE}^{-1}(k_1+1)x}{(\alpha_3-\alpha_5x)}}}{(\alpha_3-\alpha_5x)^2}dx, \end{aligned} \quad (29)$$

$$\tilde{\xi} = \min\{(\frac{\alpha_3}{\alpha_4}+1)2^{-2R_1}-1, (\frac{\alpha_3}{\alpha_5}+1)2^{-2R_1}-1\}, \quad (30)$$

$$\Phi(x) = \frac{1}{1+\frac{\alpha_2\pi_{S_2R}}{\alpha_1\pi_{S_1R}}(2^{2R_1}(1+x)-1)}e^{-\frac{2^{2R_1}-1}{\alpha_1\pi_{S1R}}}, \quad (31)$$

and

$$\tau_1 = e^{-(\frac{1}{\alpha_2\pi_{S2R}}+\frac{1}{\alpha_4\pi_{RD_2}})(2^{2R_2}-1)}, \quad (32)$$

respectively. We note that HD relaying is known to suffer from a spectral efficiency loss compared to FD relaying due to its time-orthogonal relay listening/forwarding suffering, so half-duplex suffer from 50% loss in data rate, there is 1/2 factor in both data transmission and eavesdropping capacities [9].

$$P_{S_1D_1} = 1 - K\sum_{k=0}^{K-1}(-1)^k\binom{K-1}{k}\frac{\alpha_3}{\pi_{RE}}\left[\int_{\xi}^{\frac{\alpha_3}{\alpha_5}}\frac{1}{(\alpha_3-\alpha_5 x)^2}e^{-\frac{(k+1)x}{\pi_{RE}(\alpha_3-\alpha_5 x)}}dx + e^{-\frac{2^{R_1}-1}{\alpha_1\pi_{S_1R}}}\int_0^{\xi}\left(\frac{c_1}{\frac{1}{\pi_{RR}}+\theta(x)}+\frac{c_2}{\frac{1}{\alpha_2\pi_{S_2R}}+\theta(x)}\right)\frac{e^{-\frac{2^{R_1}-1}{\alpha_1\pi_{S_1R}}-\frac{(\pi_{RD_1}^{-1}+\pi_{RD_2}^{-1})}{\alpha_3(2^{R_1}(x+1)-1)^{-1}-\alpha_4}-\frac{(k+1)x}{\pi_{RE}(\alpha_3-\alpha_5 x)}}}{(\alpha_3-\alpha_5 x)^2}dx\right], \quad (24)$$

$$P_{S_2D_2} = 1 - K\sum_{k=0}^{K-1}(-1)^k\binom{K-1}{k}\frac{e^{-(2^{R_2}-1)(\frac{1}{\alpha_2\pi_{S_2R}}+\frac{1}{\alpha_4\pi_{RD_2}})}}{\pi_{RE}}\int_0^{\frac{\alpha_4}{\alpha_5}}\frac{\alpha_4\alpha_2\pi_{S_2R}e^{-\frac{2^{R_2}x}{\alpha_2\pi_{S_2R}}+\frac{2^{R_2}x}{\alpha_4\pi_{RD_2}}+\frac{(k+1)x}{\pi_{RE}(\alpha_4-\alpha_5 x)}}}{(\alpha_2\pi_{S_2R}+(2^{R_2}(x+1)-1))(\alpha_4-\alpha_5 x)^2}dx. \quad (26)$$

B. Optimization of the Power Allocation Parameter α_5 and Effect Secrecy Throughout

The optimal value of power allocation parameter α_5 that minimizes the exact SOP given (27) can be obtained though

$$\alpha_5^* = \underset{0\le\alpha_5<1}{\operatorname{argmin}} P_{out}^{NOMA-ANFDR}. \quad (33)$$

We first analytically determine the first-order derivative of $P_{out}^{NOMA-ANFDR}$ with respect to a_5 for a given a_3 and a_4. We numerically find that $\partial P_{out}^{NOMA-ANFDR}/\partial a_5$ is first negative and then positive. We then analytically determine the second-order derivative of $P_{out}^{NOMA-ANFDR}$ with respect to a_5 for given a_3 and a_4. We numerically find that $\partial^2 P_{out}^{NOMA-ANFDR}/\partial^2 a_5$ is always positive when $0 < a_5 < 1$. Therefore, we conjecture that there is a unique value of a_5 within $0 < a_5 < 1$, referred to as a_5^* , which achieves the minimum $P_{out}^{NOMA-ANFDR}$. This conjecture will be supported by the numerical results in Section V. We denote $P_{out}^{*NOMA-ANFDR}$ as minimum exact SOP achieved by setting $\alpha_5 = \alpha_5^*$ in (27).

In this paper, the EST is defined as the product of the secrecy rate and the maximum secure transmission probability (i.e., the minimum SOP) , which is given by

$$T_{NOMA-AHRS} = (R_1 + R_2)(1 - P_{out}^{*NOMA-AFRS}), \quad (34)$$

where $(1 - P_{out}^{*NOMA-ANFDR})$ means the transmission from the source was successfully received by the destination for both $S_1 - D_1$ and $S_2 - D_2$ user pairs, but not at eavesdroppers.

V. Numerical Results

In this section, we provide numerical results to examine the secrecy performance of the proposed NOMA-ANFDR scheme. The NOMA-ANHDR scheme and NOMA in cooperative half-duplex-relay without considering security (NOMA-HDR-w/o-SE, without considering the presence of eavesdroppers [5]) is also shown as benchmarks in the figures. We assume that all nodes are assumed to be collinear with $d_{1R} = 0.2$, $d_{2R} = 0.5$, $d_{RD_1} = 0.8$, $d_{RD_2} = 0.6$, and $\nu = 4$. We also assume that employing fixed transmit power allocation for legal users in these NOMA schemes. We set $\alpha_1 = 0.9$, $\alpha_2 = 0.1$, $\alpha_3 = 9\alpha_4$, $R_1 = 0.5$, $R_2 = 1$, $P_S = P_R = 20$dB, and $P_E = 2$dB.

Fig. 2 plots the SOPs of the proposed NOMA-ANFDR scheme, NOMA-ANHDR scheme, and NOMA-HDR-w/o-SE

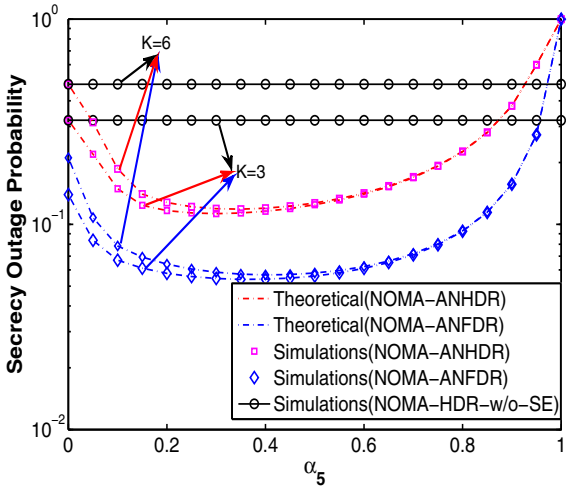

Fig. 2. SOP versus different values α_5 with $R_1 = 0.5$ and $R_2 = 1$.

with $K = 3$ and $K = 6$. We first see that the SOPs of the proposed NOMA-ANFDR and NOMA-ANHDR schemes first decrease and then increase as a_5 increases, which implies that there is a unique a_5 that minimizes the SOP, i.e., a_5^*. This supports our conjecture on a_5 in Section IV. Secondly, it is observed from Fig. 2 that the theoretic SOPs achieved by the proposed NOMA-ANFDR and NOMA-AHFDR schemes match their simulated SOPs. This confirms the correctness of the results present in (27) and (28). Thirdly, it is observed from Fig. 2 that, both the SOPs of the proposed NOMA-ANFDR and NOMA-ANHDR schemes perform better than NOMA-HDR-w/o-SE. This indicates that artificial-noise enhances the physical layer security against eavesdropping attack. It is also observed from Fig. 2 that the NOMA-ANFDR scheme significantly outperforms the NOMA-ANHDR scheme, illustrating the security benefits of exploiting the FD mode to prevent eavesdropping attacks.

Fig. 3 plots minimum SOPs versus P_R with $\pi_{RR} = 0$dB and $\pi_{RR} = 4$dB. We see that the minimum SOPs of the three schemes tend to decrease with P_R, but the proposed NOMA-ANFDR scheme achieves a best performance, and the NOMA-HDR-w/o-SE scheme has the worst secrecy performance as compared to other AN-aided schemes, showing that the securi-

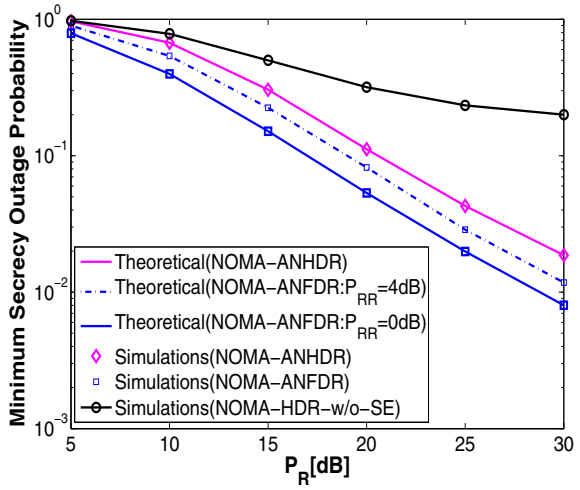

Fig. 3. Minimum secrecy outage probabilities versus P_R with $K = 3$, $R_1 = 0.5$, $R_2 = 1$, $\pi_{RE} = 2$dB, $\pi_{RR} = 0$dB, and $\pi_{RR} = 4$dB.

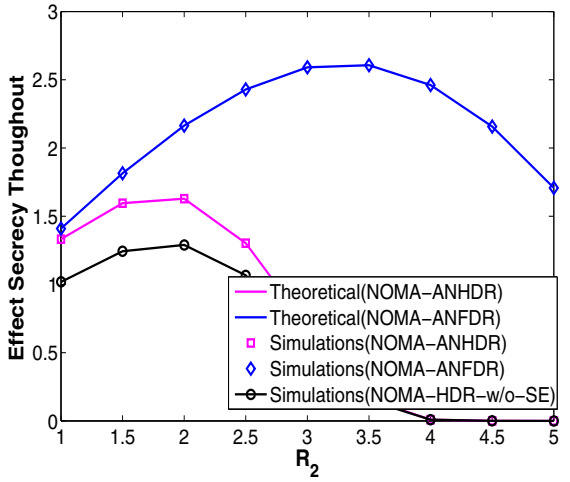

Fig. 4. EST versus R_2 with $K = 3$, $\pi_{RR} = 4$dB, and $\pi_{RE} = 2$dB.

ty benefits of the exploiting AN-aided and FD mode in relay in defending against eavesdropping. It is also from Fig. 3 that the secrecy performance of the NOMA-ANFDR scheme relative to NOMA-ANHDR scheme becomes more prominent as π_{RR} decreases, e.g., from $\pi_{RR} = 4$ dB to $\pi_{RR} = 0$ dB. This can be explained by the fact that the NOMA-ANFDR scheme has a better secrecy performance than the NOMA-ANHDR scheme when the self-interference is well suppressed.

Fig. 4 plots the EST versus R_2. One can observe that the NOMA-ANFDR scheme achieves the highest EST since it has the lowest minimum SOP among the three schemes. It is also from Fig. 4 that the proposed NOMA-ANFDR scheme can use a highest secure transmission rate for $S_2 - D_2$ user pair when the case of achieving the highest EST.

VI. Conclusions

In this paper, we proposed a new NOMA-ANFDR scheme in a cooperative relay network in the presence of K eavesdroppers. To analyze the benefits of the NOMA-ANFDR scheme, we derive its SOP in closed form. It was shown that the NOMA-ANFDR scheme significantly outperforms the NOMA-ANHDR and the NOMA-HDR-w/o-SE scheme by achieving a lowest SOP and a highest EST. This result indicates that adopting the joint of FD and AN techniques at relays can greatly improve the physical layer security in cooperative NOMA systems.

Acknowledgement

The authors would like to acknowledge that this work was partially supported by the National Natural Science Foundation of China (61671252, 61501251, 61571233, 61772287), the Key Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 14KJA510003, and the Australian Research Council Discovery Project (DP150103905).

References

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, 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, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[3] Z. Ding, H. Dai, and H. V. Poor, "Relay selection for cooperative NOMA," *IEEE Commun. Lett.*, vol. 5, no. 4, pp. 416C-419, Aug. 2016.

[4] J. B. Kim and I. H. Lee, "Capacity analysis of cooperative relaying systems using non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 1949–1952, Nov. 2015.

[5] M. Kader, M. Shahab, and S. Shin, "Exploiting non-orthogonal multiple access in cooperative relay sharing," *IEEE Commun. Lett.*, accepted to appear.

[6] 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, Sep. 2016.

[7] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory,* vol. 54, no. 9, Sep. 2008.

[8] Y. Feng, Z. Yang, W.-P. Zhu, Q. Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2354–2366, Mar. 2017.

[9] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system" *IEEE Trans. Inf. Forensics Security.*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

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

[11] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[12] Y. Zou, "Physical-Layer Security for Spectrum Sharing Systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319– 1329,Feb. 2017.

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

[14] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," *in Proc. Int. Commun. Conf. (ICC),* May 2016, pp. 1–6.

[15] 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.