MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

NOMA Based Coordinated Direct and Relay Transmission: Secure Design and Performance Analysis

Pei, X.; Wen, M.; Kim, K.J.; Zheng, B.; Yu, H.

TR2019-155 December 09, 2019

Abstract

In this paper, we propose a coordinated direct and relay transmission scheme based on non-orthogonal multiple access (NOMA), where the relay and cell-center user operate in full-duplex mode to help enhance the quality of service of the cell-edge user as well as ensure the secure transmission. In the proposed system, the base station directly serves the cellcenter user and relay while communicating with the cell-edge user through the relay and cell-center user. Taking advantage of NOMA, the cell-center user and relay are able to cancel the mutual interference between themselves. Moreover, they can also cooperatively apply the artificial noise scheme to interfere any potential eavesdropper without impairing the legitimate cell-edge user. Exact and closed-form expressions for the outage probability, achievable rate, and achievable secure rate are derived. Numerical results prove that the proposed system outperforms the existing counterpart in the low signal-to-noise ratio region, and ensures secure communications with appropriate power allocation.

IEEE Global Communications Conference (GLOBECOM)

NOMA Based Coordinated Direct and Relay Transmission: Secure Design and Performance Analysis

Xinyue Pei†, Miaowen Wen†, Kyeong Jin Kim§, Beixiong Zheng†, and Hua Yu†
†School of Electronic and Information Engineering
South China University of Technology, Guangzhou 510640, China
Email: {eexypei, zheng.bx}@mail.scut.edu.cn, {eemwwen, yuhua}@scut.edu.cn
§Mitsubishi Electric Research Laboratories
Cambridge, MA 02139 USA
Email: kyeong.j.kim@hotmail.com

***Abstract*—In this paper, we propose a coordinated direct and relay transmission scheme based on non-orthogonal multiple access (NOMA), where the relay and cell-center user operate in full-duplex mode to help enhance the quality of service of the cell-edge user as well as ensure the secure transmission. In the proposed system, the base station directly serves the cell-center user and relay while communicating with the cell-edge user through the relay and cell-center user. Taking advantage of NOMA, the cell-center user and relay are able to cancel the mutual interference between themselves. Moreover, they can also cooperatively apply the artificial noise scheme to interfere any potential eavesdropper without impairing the legitimate cell-edge user. Exact and closed-form expressions for the outage probability, achievable rate, and achievable secure rate are derived. Numerical results prove that the proposed system outperforms the existing counterpart in the low signal-to-noise ratio region, and ensures secure communications with appropriate power allocation.**

***Index Terms*—physical layer security, NOMA, full-duplex, outage probability, secure rate.**

I. Introduction

One of the most important applications of non-orthogonal multiple access (NOMA) is cooperative NOMA, where users or dedicated relays cooperate to improve the transmission efficiency of the system. The NOMA-based coordinated direct and relay transmission (CDRT) was introduced in [1]. It was shown therein that NOMA-based CDRT performs better than the non-coordinated direct and relay transmission counterpart. The study of [1] employs the half-duplex (HD) technique. However, systems equipped with HD technique need an extra phase for cooperation, which suffer from a loss of spectral efficiency. Attentive to this, the authors of [2] replaced the HD relay in [1] with the full-duplex (FD) relay to enhance the spectral efficiency. In both [1] and [2], the near user only uses the data symbol of the far user to process interference cancellation. Different from [1] and [2], in our work, the near user is working in FD mode to use the decoded data symbol to assist the far user while receiving new data symbols, which shows to further enhance the spectral efficiency.

Transmitting an additional copy by the near user, however, renders the CDRT system more vulnerable to eavesdropping. Therefore, how to protect the legitimate far user from being wiretapped is crucial. There have been many studies in the literature concerning the secure communications problem. Assuming the channel state information (CSI) of the eavesdropper available at the legitimate transmitter, the secrecy capacities were analyzed in [3]–[5]. Although this assumption facilitates the analysis, it can be impractical when the eavesdropper works in a passive way. Without any knowledge of the eavesdropper's channel, [6] proposed a solution called artificial noise scheme to ensure secure communications. For its effectiveness, the artificial scheme was employed to solve the security problem under different scenarios, e.g., multi-input multi-output [7]–[10], cooperative relaying systems (CRS) [11]–[13], and two-way relay networks [14]. We find that the artificial noise scheme can also be applied to the NOMA-based CDRT system since the near user can cooperate with the relay in favor of the FD mode.

In this paper, we consider a NOMA-based CDRT system with one base station, two users, one relay, and one eavesdropper, where the cell-edge user cannot communicate with the base station directly and both the cell-center user and relay operate in FD mode to assist the cell-edge user in our system. The main contributions of this work are summarized as follows. We analyze the performance of the proposed NOMA-based CDRT system over Rayleigh fading channels. Specifically, exact closed-form expressions for instantaneous and ergodic rates of cell-center and cell-edge users are derived. Moreover, the outage probability of each data symbol is derived. We take advantage of both FD nodes and incorporate the artificial noise scheme. This sophisticated strategy makes eavesdropper hard to wiretap the information of the cell-edge user. The expressions for the instantaneous and ergodic secure rates under the scenario of a single eavesdropper are derived. Both numerical and Monte Carlo simulation results are presented. Results show that the proposed NOMA-based CDRT system has superior performance at low transmit signal-to-noise ratio (SNR) in terms of the ergodic sum rate, and outage probability. Moreover, under the scenario of a single eavesdropper, our system performs much better than the existing system by

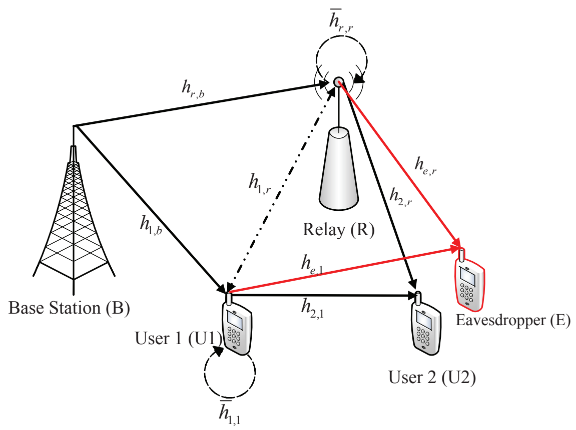

Fig. 1. System model, where dash dotted line represents interference between two nodes.

applying appropriate power allocation.

Notation: $E[X]$ stands for the expectation of random variable X. $f_X(\cdot)$, $F_X(\cdot)$ and $\bar{F}_X(\cdot)$ denote the probability density function (PDF), cumulative distribution function (CDF) and complementary CDF (CCDF) of random variable X, respectively. $\mathbb{C}^{a_1\times b_1}$ and $\mathbf{0}^{a_1\times b_1}$ denote a matrix and all-zero matrix with a_1 rows and b_1 columns, respectively, where a_1 and b_1 are arbitrary non-zero positive integers. $\mathbf{I}_n$ denotes a square matrix of order n, whose elements are all one. $[x]^+$ denotes $\max\{x, 0\}$. $\mathcal{N}_c(\mu, \sigma_0^2)$ denotes complex Gaussion distribution with mean μ and variance σ_0^2. $Ei(x) = \int_{-\infty}^{x} e^t/tdt$, $x < 0$.

II. System Model

Consider a cooperative communication scenario shown in Fig. 1, which consists of a base station (denoted by B), a relay (denoted by R), user 1 (denoted by $U1$), user 2 (denoted by $U2$), and one potential eavesdropper (denoted by E). All the nodes are assumed to be synchronous. User 1 is the cell-center user, and user 2 is the cell-edge user. We assume that the base station operates in HD mode, while user 1 and the relay in FD mode. Considering that user 2 may move to the cell-center, it is also equipped with a FD antenna. The channels $B-R$, $B-U1$, $R-U1$, $R-U2$, $U1-U2$, $U1-E$, and $R-E$ are respectively denoted by $h_{r,b}$, $h_{1,b}$, $h_{1,r}$, $h_{2,r}$, $h_{2,1}$, $h_{e,1}$, and $h_{e,r}$, which are assumed to follow independent zero-mean complex Gaussian distributions with variances $\beta_{r,b}$, $\beta_{1,b}$, $\beta_{1,r}$, $\beta_{2,r}$, $\beta_{2,1}$, $\beta_{e,1}$, and $\beta_{e,r}$, respectively. User 1 is assumed to be closer to the B than R. Due to the strong shadowing or long distance between the base station and user 2, it is assumed that there is no direct link between them. User 2 communicates with the base station with the assistance of user 1 and the relay. There are two phases involved in the whole transmission, namely, initial phase (denoted by t_0) and stable phase (denoted by t). We denote τ as the length of a time duration.

A. Communication Procedure

During time duration t, the base station transmits a new superimposed signal $x_b(t)$ to relay and user 1, which is given in the form of

$$x_b(t) = \sqrt{P_b a_1} x_1(t) + \sqrt{P_b a_2} x_2(t), \tag{1}$$

where $E[|x_1(t)|^2] = E[|x_2(t)|^2] = 1$. The relay and user 1 transmit the decoded symbol $x_2(t-\tau)$ to user 2 while receiving $x_b(t)$ with transmission power P_r and P_1, respectively. Since both the relay and base station are working in FD mode, there exist echo channels between the transmit and receive antennas. Let $\bar{h}_{r,r}$ and $\bar{h}_{1,1}$ denote the echo channels of the relay and user 1, respectively.

In the proposed system, the relay and user 1 cooperatively apply the beamforming technique to transmit data symbol $x_2(t-\tau)$ to user 2. Specifically, user 1 and relay can be seen as two independent antennas of a hypothetical node, which transmits the data symbol vector $[x_2(t-\tau),\, x_2(t-\tau)]^T$ to user 2 directly. In this way, the channel vector is given by $\mathbf{h} = [h_{2,r},\, h_{2,1}]^T \in \mathbb{C}^{2\times 1}$, and the transmit power matrix by $\mathbf{P} = [\sqrt{P_r},\, 0; 0,\, \sqrt{P_1}]$. Let $\mathbf{k} = \mathbf{Ph} = [h_{2,r}\sqrt{P_r},\, h_{2,1}\sqrt{P_1}]^T$. The range space of $\mathbf{k}^T$ can be readily derived as $\mathbf{v}_U = [v_1,\, v_2]^T$,[1] where $v_1 = \frac{h_{2,r}^*\sqrt{P_r}}{\sqrt{|h_{2,r}|^2 P_r + |h_{2,1}|^2 P_1}}$, and $v_2 = \frac{h_{2,1}^*\sqrt{P_1}}{\sqrt{|h_{2,r}|^2 P_r + |h_{2,1}|^2 P_1}}$, which are the beamforming coefficients employed by the relay and user 1, respectively. Therefore, the received signals at user 1 and relay can be expressed respectively as

$$\begin{aligned} y_1(t) =& h_{1,b} x_b(t) + h_{1,r}\sqrt{P_r} v_1 x_2(t-\tau) \\ &+ \sqrt{P_1}\bar{h}_{1,1} v_2 x_2(t-\tau) + n_1(t), \end{aligned} \tag{2}$$

and

$$\begin{aligned} y_r(t) =& h_{r,b} x_b(t) + h_{1,r}\sqrt{P_1} v_2 x_2(t-\tau) \\ &+ \sqrt{P_r}\bar{h}_{r,r} v_1 x_2(t-\tau) + n_r(t), \end{aligned} \tag{3}$$

where $n_1(t)$, $n_r(t) \sim \mathcal{N}_c(0, \sigma^2)$, respectively.

In the previous phase, as user 1 has already decoded $x_2(t-\tau)$ based on successive interference cancellation (SIC), it can cancel out the interference of $h_{1,r}\sqrt{P_r} v_2 x_2(t-\tau)$, and so can the relay. After removing the effect of $x_2(t-\tau)$ and modeling the residual self-interference as additive white Gaussian noise (AWGN), we can rewrite Eqs. (2) and (3) as

$$y_1(t) = h_{1,b} x_b(t) + \hat{n}_1(t), \tag{4}$$

and

$$y_r(t) = h_{r,b} x_b(t) + \hat{n}_r(t), \tag{5}$$

respectively, where $\hat{n}_1(t)$ and $\hat{n}_r(t)$ are equivalent AWGNs with variances $(P_1\gamma_{1,1}+1)\bar{\sigma}^2$ and $(P_r\gamma_{r,r}+1)\bar{\sigma}^2$, respectively, using the same model given in [15]–[17], and $\gamma_{1,1}$ and $\gamma_{r,r}$ represent the normalized gains of residual interference due to imperfect mitigation of self-interference.

Accordingly, the transmitted signal by the hypothetical node to user 2 is designed in the form of

$$\mathbf{x} = \mathbf{v}_U \sqrt{\phi} x_2(t-\tau), \tag{6}$$

[1]Through sending pilot signal, user 1 and the relay can obatin $h_{2,1}$ and $h_{2,r}$ respectively from feedback.

where ϕ denotes the power allocation ratio between the signal power and the total transmit power. In this scenario, ϕ is equal to one.

The signal received by user 2 is given by

$$\begin{aligned} y_2(t) =& \mathbf{k}^T \mathbf{x} + n_2(t) \\ =& (h_{2,r}\sqrt{P_r}v_1 + h_{2,1}\sqrt{P_1}v_2)\sqrt{\phi}x_2(t-\tau) + n_2(t), \end{aligned} \tag{7}$$

where $n_2(t) \sim \mathcal{N}_c(0, \sigma^2)$.

B. Presence of An Eavesdropper

We consider the presence of an eavesdropper in Fig. 1. When user 1 and the relay retransmit data symbol to user 2, the eavesdropper receives the signal from the relay and user 1 silently at the same time. Suppose that the eavesdropper knows the instantaneous CSIs of all the links, while the legitimate users only know the CSIs of adjacent legitimate links. It is easy to find that user 2 will suffer from security problem without protections. To solve this problem, we use the artificial noise scheme, whose idea is to confuse the potential eavesdropper without interfering the legitimate users.

By applying the null space of the legitimate channels, i.e., $\mathbf{v}_E = [v_3,\ v_4]^T$, where $v_3 = \frac{-h_{2,1}\sqrt{P_1}}{\sqrt{|h_{2,r}|^2 P_r + |h_{2,1}|^2 P_1}}$, and $v_4 = \frac{h_{2,r}\sqrt{P_r}}{\sqrt{|h_{2,r}|^2 P_r + |h_{2,1}|^2 P_1}}$, the mixed signal is designed in the form of

$$\mathbf{x} = \mathbf{v}_U\sqrt{\phi}x_2(t-\tau) + \mathbf{v}_E\sqrt{1-\phi}n_v(t), \tag{8}$$

where $n_v(t) \sim \mathcal{N}_c(0,1)$ is the artificial noise and $\phi \in [0,1]$. The signal received at the eavesdropper is given by

$$\begin{aligned} y_e =& \mathbf{k}_E^T\mathbf{x} + n_e \\ =& \mathbf{k}_E^T\mathbf{v}_U\sqrt{\phi}x_2(t-\tau) + \mathbf{k}_E^T\mathbf{v}_E\sqrt{(1-\phi)}n_v + n_e(t) \\ & + (h_{e,r}\sqrt{P_r}v_3 + h_{e,1}\sqrt{P_1}v_4)\sqrt{1-\phi}n_v + n_e(t), \end{aligned} \tag{9}$$

where $\mathbf{k}_E = \mathbf{P}\mathbf{h}_E = [h_{e,r}\sqrt{P_r} \quad h_{e,1}\sqrt{P_1}]^T$, $\mathbf{h}_E = [h_{e,r} \quad h_{e,1}]^T$, and $n_e(t) \sim \mathcal{N}_c(0, \sigma_E^2)$.

III. Performance Analysis

In this section, the instantaneous rate, outage performance, ergodic sum rate, outage probability, throughput, and EE of the proposed system are investigated sequentially.

A. Instantaneous Rate

Let $\rho_b = \frac{P_b}{\sigma^2}$, $\rho_r = \frac{P_r}{\sigma^2}$, $\rho_1 = \frac{P_1}{\sigma^2}$, $|h_{1,b}|^2 = \lambda_{1,b}$, $|h_{r,b}|^2 = \lambda_{r,b}$, $|h_{1,r}|^2 = \lambda_{1,r}$, $|h_{2,1}|^2 = \lambda_{2,1}$, and $|h_{2,r}|^2 = \lambda_{2,r}$. For simple computation, we set $\gamma_{1,1} = \gamma_{r,r} = \gamma$.

User 1 first decodes the data symbol of user 2 and then decodes its own data symbol based on the SIC. In light of Eq. (4), the SINR of user 2 observed at user 1 is given by $\gamma_0 = \frac{a_2\lambda_{1,b}\rho_b}{a_1\lambda_{1,b}\rho_b + P_1\gamma + 1}$, while the SINR of user 1 is $\gamma_1 = \frac{a_1\lambda_{1,b}\rho_b}{1+P_1\gamma}$. In addition, the SINR of the relay is $\gamma_r = \frac{a_2\lambda_{r,b}\rho_b}{\lambda_{r,b}\rho_b a_1 + P_r\gamma + 1}$. On the basis of Eq. (7), the SNR of user 2 is $\gamma_2 = |h_{2,r}\sqrt{\rho_r}v_1 + h_{2,1}\sqrt{\rho_1}v_2|^2\phi$.

From the above definitions, we can obtain the achievable rate at user 1 measured in bps/Hz as $C_1 = \log_2(1+\gamma_1)$.

Since the data symbol of user 2 must be decoded first at user 1 for SIC as well as at the relay, the achievable rate at user 2 is dominated by the lowest SINR, which can be expressed as $C_2 = \log_2(1 + \min\{\gamma_0, \gamma_r, \gamma_2\})$.

B. Ergodic Sum Rate

The ergodic sum rate of the proposed system is given by $\bar{C}_{sum} \triangleq E[C_1] + E[C_2] = \bar{C}_1 + \bar{C}_2$. Since the CDF of λ_δ ($\delta \in \{\{1,b\},\{r,b\},\{1,r\},\{2,r\},\{2,1\}\}$) is $F_{\lambda_\delta} = 1 - e^{-\frac{x}{\beta_\delta}}$, and $\int_0^\infty \log_2(1+x)f_X(x)dx = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_X(x)}{1+x}dx$ from [18, Eq. (3.352.4)], $\bar{C}_1$ can be derived as

$$\bar{C}_1 = -\frac{e^{\frac{P_1\gamma+1}{a_1\rho_b\beta_{1,b}}}}{\ln 2}Ei\left(-\frac{P_1\gamma+1}{a_1\rho_b\beta_{1,b}}\right). \tag{10}$$

Let $Y = \min\{\gamma_0, \gamma_r, \gamma_2\}$. Therefore, $\bar{C}_2 = \int_0^\infty \log_2(1+Y)f_Y(y)dy$, and $F_Y(y) = 1 - \bar{F}_{\gamma_0}(y)\bar{F}_{\gamma_r}(y)\bar{F}_{\gamma_2}(y)$. The CCDF of γ_2 is shown as

$$\begin{aligned} \bar{F}_{\gamma_2}(z) =& \frac{\beta_{2,r}\rho_r}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}e^{-\frac{z}{\phi\rho_r}\frac{1}{\beta_{2,r}}} \\ & - \frac{\beta_{2,1}\rho_1}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}e^{-\frac{z}{\phi\rho_1}\frac{1}{\beta_{2,1}}}. \end{aligned} \tag{11}$$

See Appendix A for the proof of Eq. (11).

Letting $d_1 = \frac{\beta_{2,r}\rho_r}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}$ and $d_2 = \frac{\beta_{2,1}\rho_1}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}$, $\bar{C}_2$ can be derived as

$$\begin{aligned} \bar{C}_2 =& \frac{1}{\ln 2}\int_0^{\frac{a_2}{a_1}} e^{-\frac{x}{(a_2-a_1x)\rho_b}\left(\frac{P_1\gamma+1}{\beta_{1,b}} + \frac{P_r\gamma+1}{\beta_{r,b}}\right)} \\ & \times \left(d_1 e^{-\frac{x}{\phi\rho_r}\frac{1}{\beta_{2,r}}} - d_2 e^{-\frac{x}{\phi\rho_1}\frac{1}{\beta_{2,1}}}\right)/(1+x)dx. \end{aligned} \tag{12}$$

Unfortunately, to the best of our knowledge, no exact closed-form solution of Eq. (12) exists.

When $P_b = mP_1 = mP_r$, ρ_b, ρ_r, and $\rho_1 \to \infty$, the approximation of $\bar{C}_1$ can be derived as

$$\bar{C}_1^{app} = -\frac{e^{\frac{\gamma\sigma^2}{ma_1\beta_{1,b}}}}{\ln 2}Ei\left(-\frac{\gamma\sigma^2}{ma_1\beta_{1,b}}\right). \tag{13}$$

Similarly, the approximation of $\bar{C}_2$ can be derived as

$$\begin{aligned} \bar{C}_2^{app} =& \frac{1}{\ln 2}\int_0^{\frac{a_2}{a_1}} e^{-\frac{Ax}{(a_2-a_1x)}}/(1+x)dx \\ \overset{(a)}{=}& \frac{d_1-d_2}{\ln 2}\int_0^\infty \frac{a_2e^{-At}}{[(a_1+a_2)t+1](a_1t+1)}dt \\ \overset{(b)}{=}& \frac{d_1-d_2}{\ln 2}\left[e^{\frac{A}{a_1}}Ei\left(-\frac{A}{a_1}\right) - e^{\frac{A}{a_1+a_2}}Ei\left(-\frac{A}{a_1+a_2}\right)\right], \end{aligned} \tag{14}$$

where $A = \left(\frac{\sigma^2\gamma}{m\beta_{1,b}} + \frac{\sigma^2\gamma}{m\beta_{r,b}}\right)$, (a) follows from a change of variable $t = \frac{x}{a_2-a_1x}$, and (b) follows from [18, Eq. (3.352.4)].

C. Outage Probability

Assume R_1 and R_2 are the target data rates associated with the data symbols of user 1 and user 2, respectively. In our proposed system, the three nodes, namely the relay, user 1, and user 2, need to decode messages, and it is assumed that the base station will always transmit a new data symbol no matter whether the previous one is decoded successfully or not. On the other hand, if user 1 fails to decode $x_2(t-\tau)$, it is impossible for user 1 to eliminate the interference from the relay as indicated by Eq. (2). If user 1 fails to decode $x_1(t)$, the process will also break. Consequently, the outage probability of $x_1(t)$ is given by

$$P_{out,1}^{t} = 1 - P(\gamma_0 > u_2, \gamma_1 > u_1) = \begin{cases} 1 - e^{-\frac{q_1}{\rho_b \beta_{1,b}}}, & u_2 < \frac{a_2}{a_1} \\ 1, & u_2 > \frac{a_2}{a_1} \end{cases}, \quad (15)$$

where $q_1 = \max\left\{\frac{(1+P_1\gamma)u_2}{a_2 - u_2 a_1}, \frac{(1+P_1\gamma)u_1}{a_1}\right\}$, $u_1 = 2^{R_1 - 1}$, and $u_2 = 2^{R_2 - 1}$.

Since both user 1 and the relay send messages to user 2, $x_2(t-\tau)$ is blocked when both interruptions occur in user 1 and the relay or interruption occurs in user 2. Therefore, the outage probability of $x_2(t-\tau)$ can be derived as

$$\begin{aligned} P_{out,2}^{t-\tau} &= 1 - P(\gamma_0 > u_2, \gamma_r > u_2, \gamma_2 > u_2) \\ &= 1 - \bar{F}_{\gamma_0}(u_2)\bar{F}_{\gamma_r}(u_2)\bar{F}_{\gamma_2}(u_2) \\ &= \begin{cases} 1 - \left(i_1 e^{-\frac{u_2}{\phi\rho_r}\frac{1}{\beta_{2,r}}} - i_2 e^{-\frac{u_2}{\phi\rho_1}\frac{1}{\beta_{2,1}}}\right), & u_2 < \frac{a_2}{a_1} \\ 1, & u_2 > \frac{a_2}{a_1} \end{cases}, \end{aligned} \quad (16)$$

where

$$i_1 = e^{-\frac{u_2}{a_2 - u_2 a_1}\frac{1}{\rho_b}\left(\frac{(1+P_1\gamma)}{\beta_{1,b}} + \frac{(1+P_r\gamma)}{\beta_{r,b}}\right)} \frac{\beta_{2,r}\rho_r}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}, \quad (17)$$

and

$$i_2 = e^{-\frac{u_2}{a_2 - u_2 a_1}\frac{1}{\rho_b}\left(\frac{(1+P_1\gamma)}{\beta_{1,b}} + \frac{(1+P_r\gamma)}{\beta_{r,b}}\right)} \frac{\beta_{2,1}\rho_1}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1}. \quad (18)$$

D. Secure Instantaneous Rate

Using Eq. (9), the receive SINR of the eavesdropper is given by

$$\gamma_e = \frac{|h_{e,r}\sqrt{P_r}v_1 + h_{e,1}\sqrt{P_1}v_2|^2\phi}{|h_{e,r}\sqrt{P_r}v_3 + h_{e,1}\sqrt{P_1}v_4|^2(1-\phi) + \sigma_E^2}. \quad (19)$$

The instantaneous rate of data symbol $x_2(t-\tau)$ for the wiretap channel is $C_e = \log_2(1+\gamma_e)$.

E. Ergodic Secure Rate

The ergodic secure rate of data symbol $x_2(t-\tau)$ is given by [20]

$$\bar{C}_2^{sec} = [\bar{C}_2 - \bar{C}_e]^+, \quad (20)$$

where $\bar{C}_e$ is the ergodic rate of data symbol $x_2(t-\tau)$, whose closed-form expression is given by Eq. (B.2) in Appendix B.

IV. Numerical Results

In this section, we evaluate the performance of our proposed CRS-NOMA system. For comparison, we choose the system in [2] and the OMA system. The study of [2] proposed a system, where user 1 operating in HD mode directly communicates with the base station, while user 2 needs the help of the relay that is equipped with FD technique and decode-and-forward (DF) protocol. Notably, the nodes in the OMA system have the same antenna configuration as those in our system. The only difference with our system is that there is no link between user 1 and user 2.

It is assumed that user 1 and the relay have identical transmit power, i.e., $P_r = P_1$, while the power of the base station is $P_b = 5P_r = 5P_1$. To simplify performance analysis, we also assume that the normalized gain of residual interference introduced by the FD mode is identical at all nodes, i.e., $\gamma_{1,1} = \gamma_{r,r} = \gamma$ with $\gamma \in [0,1]$. Besides, the noise variance is assumed to be the same at all nodes, i.e., $\sigma^2 = \sigma_E^2 = \bar{\sigma}^2 = 1$. Moreover, we can set $\beta_{1,b} = \beta_{2,1} = 10$ and $\beta_{1,r} = \beta_{r,b} = \beta_{2,r} = 1$. The power allocation factors are set as $a_2 = 1-\alpha$, and $a_1 = \alpha$. $|\hat{f}_1|^2$, which is defined in [2], is set as 0 in the simulations. Let $R_1 = R_2 = R_0$. Unless indicated, $R_0 = 1$. Except Fig. 4, all figures disregard the impact of eavesdropping. Therefore, the power allocation ratio of the signal power to the total transmit power ϕ is set as 1 in these figures. To examine the impact of γ on the performance, we consider two different system setups: $\gamma = 0$ and $\gamma = 0.1$, which are referred to as Case 1 and Case 2, respectively, in all figures.

Fig. 2 shows the ergodic sum rates of our system, the OMA system and the counterpart in [2] with respect to the normalized gain of self-interference γ and SNR. We can observe that the analytic results, i.e., Eqs. (10) and (12), agree with the simulation ones perfectly. Besides, at high SNR, when $\gamma \neq 0$, the analytical results given by Eqs. (13) and (14) agree with the simulation results. In Case 1, the proposed system performs much better than the one in [2] and the OMA one. This is because the effect of γ is not taken into account in this case, and user 1 also coordinates the transmission of $x_2(t-\tau)$ for user 2. When γ increases, the ergodic sum rate of our system decreases as γ has negative effects on the ergodic rates of $x_1(t)$ and $x_2(t-\tau)$. In Case 2, compared with the counterpart in [2], the proposed system performs better in the low SNR region, while in the high SNR region, it does worse due to the strong self-interference. This phenomenon is caused by the fact that user 1 is equipped with FD technique in our system but not in the previous one. Equipped with FD technique, user 1 is more sensitive to the self-interference. Although user 1 in the OMA system works in FD mode, it is not interfered by the relay and there is no self-interference. Therefore, our system is inferior to the OMA system at high SNR when $\gamma \neq 0$.

Fig. 3 shows that the theoretical analysis of outage propbabilities in Eqs. (15) and (16) agrees with the simulation results perfectly. When $R_0 = 5$, no matter how large γ is,

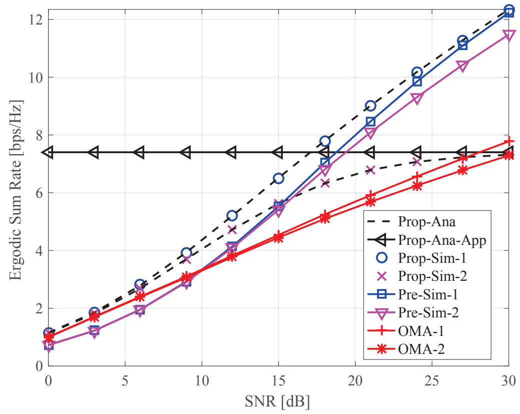

Fig. 2. Comparison of ergodic rates of the proposal and the one in [2] versus the transmit SNR with $\alpha = 0.05$.

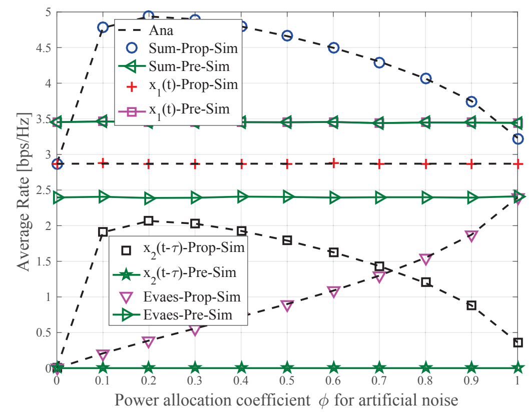

Fig. 4. Ergodic secure rate and the one in [2] versus power allocation coefficient ϕ for the artificial noise scheme with $\rho_b = 15$dB, $\alpha = 0.05$ and $\gamma = 0.1$.

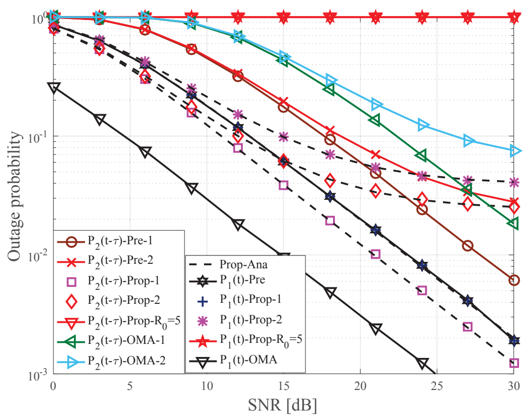

Fig. 3. Outage probability in different cases, the one in [2], and in OMA versus the transmit SNR with $\alpha = 0.05$.

the outage probability is always one, due to the fact that the system stops working when $R_0 > \frac{u_2}{u_1}$. As seen from Fig. 3, $P_1(t)$ of the previous system performs better than $P_1(t)$ of the proposal. This can be explained by the fact that Eq. (15) is affected by the self-interference while [2, Eq. (12)] is not. Moreover, if $\gamma \neq 0$, the curves of $P_1(t)$ and $P_2(t-\tau)$ will approach constant in the high SNR region due to the negative effect of self-interference. Notably, $P_1(t)$ of the OMA system shows the best performance among these three systems. This is because user 1 in the OMA system is not affected by the self-interference and the interference between the relay and user 1. Comparing curves of Cases 1 and 2, we can easily find that the system with smaller self-interference performs better. In Case 1 with $\gamma = 0$, our system demonstrates superior performance to the one in [2]. It is easy to find that $P_2(t-\tau)$ is much lower than that of the previous system and the OMA system in the low SNR region, while it performs worse than $P_2(t-\tau)$ of [2] in the high SNR region.

As observed in Fig. 4, only the ergodic rate of $x_2(t-\tau)$ is affected by ϕ, while the ergodic rates of the other data symbols remain unchanged, which reflects the fact that the eavesdropper only wiretaps $x_2(t-\tau)$ all the time. With increasing power allocation coefficient ϕ, the ergodic rate of the eavesdropper increases. From Eq. (19), we know that the larger ϕ is, the higher received SINR at the eavesdropper is. We can also find that there exists an optimal value of ϕ to maximize the ergodic secure rate of $x_2(t-\tau)$ at the legitimate user. Compared with the ergodic secure rate of [2], the ergodic secure rate of the proposed system performs much better in a very large range of ϕ. This comes from the fact that the previous system does not use any protection. Notably, if $\phi = 0$, user 1 and the relay only transmit artificial noise; if $\phi = 1$, user 1 and the relay transmit data symbol without secure protection strategy, which makes $x_2(t-\tau)$ vulnerable to potential eavesdropping. Obviously, we can obtain a relatively high ergodic secure rate with an appropriate power allocation coefficient ϕ.

V. Conclusions

In this paper, we have proposed a NOMA-based CDRT system. We have analyzed the performance of the proposed system and derived closed-form expressions for the instantaneous rate, outage probability. Besides, we have also derived the approximate expressions for the ergodic sum rate. Our proposed system has been proven to achieve better ergodic sum rate in the low SNR region than the previous one and the OMA system. Moreover, we have extended our system to a secure scenario where one eavesdropper exists. By using the artificial noise scheme, we have enhanced the ability of user 1 and the relay to puzzle the eavesdropper without affecting the legitimate user. We have derived the expression for the ergodic secure rate. The analytical results have been shown to match the simulation ones perfectly.

Appendix A
Proof of $F_{\gamma_2}(z)$

Since $|h_{2,r}|^2$ is independent of $|h_{2,1}|^2$, we have $f_{XY}(x,y) = \frac{1}{\beta_{2,1}\beta_{2,r}} e^{-\frac{x}{\beta_{2,1}}} e^{-\frac{y}{\beta_{2,r}}}$ with $|h_{2,1}|^2 = X$ and

$|h_{2,r}|^2 = Y$. Letting $Z = \gamma_2 = \rho_r(X+Y)$, we have

$$\begin{aligned} F_Z(Z<z) =& F_Z(\rho_1 X + \rho_r Y < z) \\ =& \iint\limits_{\rho_1 X + \rho_r Y < z} f_{XY}(x,y) dx dy \\ =& \int_0^{\frac{z}{\phi\rho_1}} dx \int_0^{\frac{z}{\phi\rho_r} - \frac{\rho_1}{\rho_r}x} f_{XY}(x,y) dy \\ =& 1 - \frac{\beta_{2,r}}{\beta_{2,r}\rho_r - \beta_{2,1}\rho_1} \\ & \times \left(\rho_r e^{-\frac{z}{\phi\rho_r}\frac{1}{\beta_{2,r}}} - \rho_1 e^{-\frac{z}{\phi\rho_1}\frac{1}{\beta_{2,1}}} \right). \end{aligned} \tag{A.1}$$

Appendix B
Proof of $\bar{C}_e$

Note that $h_{e,r}$ and $h_{e,1}$ are independent complex Gaussian random variables. Let $x = |h_{e,r}\sqrt{P_r}v_1 + h_{e,1}\sqrt{P_1}v_2|$, $y = |h_{e,r}\sqrt{P_r}v_3 + h_{e,1}\sqrt{P_1}v_4|$, $L_1 = x^2$, and $L_2 = y^2$. Although v_1 and v_2 are correlative with $h_{2,1}$ and $h_{2,r}$, they are irrelevant to $h_{e,1}$ and $h_{e,r}$. Using the Gaussian distribution characteristics, it is obvious that $L_1 \sim \mathcal{N}_c(0, \beta_{e,r}\sqrt{P_r}|v_1|^2 + \beta_{e,1}\sqrt{P_1}|v_2|^2)$, and $L_2 \sim \mathcal{N}_c(0, \beta_{e,r}\sqrt{P_r}|v_1|^2 + \beta_{e,1}\sqrt{P_1}|v_2|^2)$. Besides, we have $|v_1|^2 + |v_2|^2 = 1$ and $|v_3|^2 + |v_4|^2 = 1$. By denoting $\beta_{e,1} = \beta_{e,r} = \beta$, $b_1 = \beta_{e,r}\sqrt{P_r}|v_1|^2 + \beta_{e,1}\sqrt{P_1}|v_2|^2$, and $b_2 = \beta_{e,r}\sqrt{P_r}|v_3|^2 + \beta_{e,1}\sqrt{P_1}|v_4|^2$, $L_1 \sim \exp(b_1\beta)$ and $L_1 \sim \exp(b_2\beta)$ can be obtained. The CCDF of γ_e is

$$\begin{aligned} \bar{F}_{\gamma_e}(x) =& \Pr\left\{ \frac{L_1\phi}{L_2(1-\phi)+\sigma_E^2} > x \right\} \\ \overset{(a)}{=}& E_{L_2}\left[e^{-(\frac{L_2 m_0}{b_1\beta} + \frac{\sigma_E^2}{\phi b_1 \beta})x} \right] \\ \overset{(b)}{=}& \int_0^\infty e^{-(\frac{L_2 m_0}{b_1\beta} + \frac{\sigma_E^2}{\phi b_1 \beta})x} \frac{1}{b_2\beta} e^{-\frac{L_2}{b_2\beta}} dL_2 \\ \overset{(c)}{=}& e^{-\frac{\sigma_E^2 x}{\phi b_1 \beta}} \frac{b_1}{m_0 b_2 x + b_1}, \end{aligned} \tag{B.1}$$

where $m_0 = \frac{1-\phi}{\phi}$. Note that, in Eq. (B.1), (a) comes from the fact that L_2 is also a variable, (a) and (b) use the definition of the expectation, and (c) follows from [18, Eq. (3.310)]. After substituting Eq. (B.1) into $\frac{1}{\ln 2}\int_0^\infty \frac{1-F_X(x)}{1+x}dx$, the ergodic rate of the eavesdropper can be derived as

$$\begin{aligned} \bar{C}_e =& \frac{1}{\ln 2}\int_0^\infty \frac{e^{-\frac{\sigma_E^2 x}{\phi b_1\beta}}}{(1+x)(m_0\frac{b_2}{b_1}x+1)} dx \\ \overset{(a)}{=}& m_1 \int_0^\infty e^{-\frac{x}{\phi b_1 \beta}} \left(\frac{m_0\frac{b_2}{b_1}}{m_0\frac{b_2}{b_1}x+1} - \frac{1}{x+1} \right) dx \\ =& m_1 \left[e^{\frac{1}{\phi b_1\beta}} Ei\left(-\frac{1}{\phi b_1 \beta}\right) - e^{\frac{1}{\phi b_2 m_0 \beta}} Ei\left(-\frac{b_2}{\phi\rho_r\beta m_0 b_1}\right) \right], \end{aligned} \tag{B.2}$$

where $m_1 = \frac{1}{\ln 2}\frac{b_1}{m_0 b_2 - b_1}$. Besides, in Eq. (B.2), (a) must conform to $\phi \neq 0.5$. When $\phi = 0.5$, $m_0 = 1$, we can clearly find that m_1 does not have a definite value. If $\phi = 0.5$, we have

$$\begin{aligned} \bar{C}_e =& \frac{1}{\ln 2}\int_0^\infty \frac{e^{-\frac{\sigma_E^2 x}{\phi b_1\beta}}}{(1+x)^2} dx \\ =& \frac{1}{\ln 2}\left[1 + \frac{\sigma_E^2 x}{\phi b_1 \beta} e^{-\frac{\sigma_E^2 x}{\phi b_1 \beta}} Ei\left(-\frac{\sigma_E^2 x}{\phi b_1 \beta} \right) \right]. \end{aligned} \tag{B.3}$$

References

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

[2] 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.

[3] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. 2007 IEEE International Symp. on Inf. Theory*, Nice, French, Jun. 2007, pp. 2466–2470.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] T. X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[8] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[9] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[10] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[11] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[12] C. Wang, H.-M. Wang, D. W. K. Ng, X.-G. Xia, and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

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

[14] B. Zheng, M. Wen, C. X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay systems using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, to be published

[15] G. Liu, X. Chen, Z. Ding, Z. Ma, and F. R. Yu, "Hybrid half-duplex/full-duplex cooperative non-orthogonal multiple access with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 506–519, Jan. 2018.

[16] H. Cui, M. Ma, L. Song, and B. Jiao, "Relay selection for two-way full duplex relay systems with amplify-and-forward protocol," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3768–3777, Jul. 2014.

[17] B. Zheng, X. Wang, M. Wen, and F. Chen, "NOMA-based multi-pair two-way relay systems with rate splitting and group decoding," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2328–2341, Oct. 2017.

[18] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Academic press, 2014.

[19] Y. Zhang, Z. Yang, Y. Feng and S. Yan, "Performance analysis of cooperative relaying systems with power-domain non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 39839–39848, Jul. 2018.

[20] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.