



Heriot-Watt University
Research Gateway

Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex

Citation for published version:

Zheng, B, Wen, M, Wang, C-X, Wang, X, Chen, F, Tang, J & Ji, F 2018, 'Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex', *IEEE Journal on Selected Areas in Communications*. <https://doi.org/10.1109/JSAC.2018.2824624>

Digital Object Identifier (DOI):

[10.1109/JSAC.2018.2824624](https://doi.org/10.1109/JSAC.2018.2824624)

Link:

[Link to publication record in Heriot-Watt Research Portal](#)

Document Version:

Peer reviewed version

Published In:

IEEE Journal on Selected Areas in Communications

Publisher Rights Statement:

© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

General rights

Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex

Beixiong Zheng, Miaowen Wen, *Member, IEEE*, Cheng-Xiang Wang, *Fellow, IEEE*,
Xiaodong Wang, *Fellow, IEEE*, Fangjiong Chen, *Member, IEEE*,
Jie Tang, *Member, IEEE*, and Fei Ji, *Member, IEEE*

Abstract

In this paper, we develop a non-orthogonal multiple access (NOMA)-based two-way relay network with secrecy considerations, in which two users wish to exchange their NOMA signals via a trusted relay in the presence of single and multiple eavesdroppers. To ensure secure communications, the relay not only forwards confidential information to the legitimate users but also keeps emitting jamming signals all the time to degrade the performance of any potential eavesdropper. Moreover, we equip the relay and each user with the full-duplex technique in the multiple-access phase to combat the eavesdropping and improve the data transmission efficiency, respectively. We propose different decoding schemes based on the successive interference cancellation (SIC) for the legitimate users, relay, and eavesdroppers. Closed-form expressions for the achievable ergodic secrecy rates of all data symbols under both single- and multiple-eavesdropper cases are derived, validated by the excellent fitting to the computer simulation results for our proposed network.

Index Terms

Physical layer security, non-orthogonal multiple access (NOMA), two-way relay networks, full-duplex, artificial noise.

I. INTRODUCTION

Due to the continuous growth of mobile devices and rapid development of Internet of things (IoT), the fifth generation (5G) wireless communication networks impose an explosive demand

B. Zheng, M. Wen, F. Chen, J. Tang, and F. Ji are with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China (email: zheng.bx@mail.scut.edu.cn; {eemwwen, eefjchen, eejtang, eefeiji}@scut.edu.cn).

C.-X. Wang is with the Institute of Sensors, Signals and Systems, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, U.K. (e-mail: cheng-xiang.wang@hw.ac.uk).

X. Wang is with the Department of Electrical Engineering, Columbia University, New York, NY 10027, USA (e-mail: wangx@ee.columbia.edu).

on low latency and massive connectivity over limited radio resources. Non-orthogonal multiple access (NOMA), which has shown the potential to improve spectral efficiency, balance user fairness, enlarge connections, and reduce access latency, has been envisioned as a promising technology for 5G networks [1]–[3]. In contrast to the conventional orthogonal multiple access (OMA), NOMA simultaneously serves a multitude of users with the same radio resource via superposition coding, where different users are distinguished with different power levels and the successive interference cancellation (SIC) is applied to cancel the multi-user interference.

Owing to various advantages it promises, NOMA has received considerable interest in both industry and academia. The system-level performance of both uplink and downlink NOMA was studied in [4]–[6], showing better performance than conventional OMA. In [7], the performance of NOMA was studied in a cellular scenario with randomly roaming users. Under the statistical and instantaneous channel state information (CSI), the power allocation problem for NOMA to achieve the max-min fairness among users was solved in [8]. In addition, the combination of NOMA transmission with other techniques, e.g., multiple-input multiple-output (MIMO) [9]–[11], cognitive radio [12]–[14], and cooperative relaying [15]–[17], has also been investigated.

The support of massive connectivity makes the mobile user easy to access, which unfortunately also makes it easy to be wiretapped by eavesdroppers due to the broadcast nature of wireless medium. Moreover, with ever-increasing amount of sensitive data, security issues of wireless communications become more and more prominent and emergent. To ensure transmission security, the concept of physical layer (PHY) security, which was initially introduced by Wyner from the information-theoretical perspective [18], has attracted increasing attention in various wireless communication scenarios [19]–[37]. Particularly, multi-antenna techniques have extensively been studied as an efficient way to achieve security enhancements. When the eavesdropper's CSI is available at the transmitter, the secrecy capacities were investigated and analyzed under various antenna configurations and channel conditions [22]–[26]. However, in practical systems, an eavesdropper usually works in a passive way and its instantaneous CSI is unavailable to the transmitter, especially under fading channels. When the potential eavesdropper may have better channel condition and its CSI is completely unknown, one of the effective solutions called artificial noise scheme in [27] can be applied for secure transmissions, in which the information-bearing signals and the artificial noises were simultaneously transmitted to deteriorate the received signal of the potential eavesdroppers without impairing the legitimate users. After that, the design and

analysis of artificial-noise-aided transmissions were studied in various wiretap channels, e.g., MIMO channels [28]–[31], cooperative relay channels [32]–[34], and two-way relay channels [35]–[37].

Although NOMA shows to achieve higher spectral efficiency and better user fairness than conventional OMA, the technology itself does not prevent from the information leakage and is also vulnerable to the eavesdropping. Therefore, the design of secrecy transmission for NOMA protocol is an important research topic. Unfortunately, to the best of our knowledge, the secrecy issue of NOMA has rarely been reported in the literature, except for the very recent studies [38]–[44]. The secrecy performance of NOMA in large-scale networks was analyzed in [38] and [39], where randomly deployed users and eavesdroppers were assumed. In [40], the secure problem of preventing multicast receivers from intercepting unicasting messages was investigated. The optimization problem with different designable parameters was solved in [41] under the secrecy considerations for NOMA systems. The optimization problem in terms of the secrecy sum rate was solved for the single-input single-output (SISO), multi-input single-output (MISO), and MIMO NOMA systems in [42], [43], and [44], respectively.

In this paper, we focus on the NOMA-based two-way relaying communication scenario with one pair of user nodes, one relay node, and multiple passive eavesdroppers. Two user nodes wish to exchange information via the trusted relay node in two phases: the multiple-access phase and broadcast phase. It is worth pointing out that without any protection, such relay-aided transmissions can be more vulnerable to eavesdropping because the confidential information is broadcast twice, i.e., by the users and relay. **To increase the system throughput and reduce the information leakage, we propose a secure NOMA-based two-way relay network, in which the relay not only protects the network from eavesdropping but also improves the spectral efficiency by creating the heterogeneous channel condition for the NOMA users.** The main contributions of this work are summarized as follows.

- In the proposed secure NOMA-based two-way relay network, we equip the relay and each user with the full-duplex technique in the multiple-access phase to combat the eavesdropping and improve the data transmission efficiency, respectively. Specifically, without requiring any extra bandwidth resource, two legitimate users receive the NOMA signals from each other under the protection of the full-duplex relay to ensure secure information exchange.
- We design different decoding schemes based on the SIC for the legitimate users, relay, and

eavesdroppers, **which exploit channel gain differences to achieve better decoding performance with NOMA proposal.** Moreover, to consider a harsh secure scenario, we provide the eavesdroppers with a sophisticated strategy by jointly processing the signals received in the two phase to better wiretap the information.

- We analyze the performance of the secure NOMA-based two-way relay network in terms of instantaneous and ergodic secrecy rates for each data symbol. Under the assumption of independent Rayleigh fading channels, we first derive the closed-form expressions on the ergodic secrecy rates for the single-eavesdropper case. By extending the single-eavesdropper case to the multiple-eavesdropper case, we further derive the closed-form expressions on the ergodic secrecy rates under both non-colluding and colluding eavesdroppers. **These closed-form expressions are in perfect agreement with simulation results.**

The remainder of this paper is organized as follows. Section II describes the proposed secure NOMA-based two-way relay network and the decoding strategies. In Section III, we conduct the performance analysis of the network under the single-eavesdropper case. The secure performance of the network under multiple eavesdroppers is analyzed in Section IV. Section V presents numerical results. Finally, conclusions are drawn in Section VI.

II. NETWORK MODEL AND DECODING SCHEME

A. Network Model

Let us consider a wireless network as shown in Fig. 1, in which one pair of user nodes (denoted by A and B) wish to exchange information via a relay node (denoted by R), under the existence of eavesdroppers (denoted by E). The relay is equipped with N_R antennas **while all the other nodes only have one antenna each due to the size limitation.** The eavesdroppers are assumed to be passive all the time and attempt to intercept the information exchanged between the two legitimate users. We assume all the links are available and all the channels are flat fading and quasi-static. Without loss of generality, we first consider the case with only one eavesdropper in this section. The more general case with multiple eavesdroppers using different cooperative strategies to wiretap the information will be discussed and analyzed later in the following sections. As shown in Fig. 1, the channel gains of $A \rightarrow B$, $B \rightarrow A$, $A \rightarrow E$, and $B \rightarrow E$ are denoted by h_{AB} , h_{BA} , h_{AE} , and h_{BE} , respectively. With multiple antennas equipped at the relay, the channel gains of $A \rightarrow R$, $B \rightarrow R$, $R \rightarrow A$, $R \rightarrow B$, and $R \rightarrow E$ are denoted by

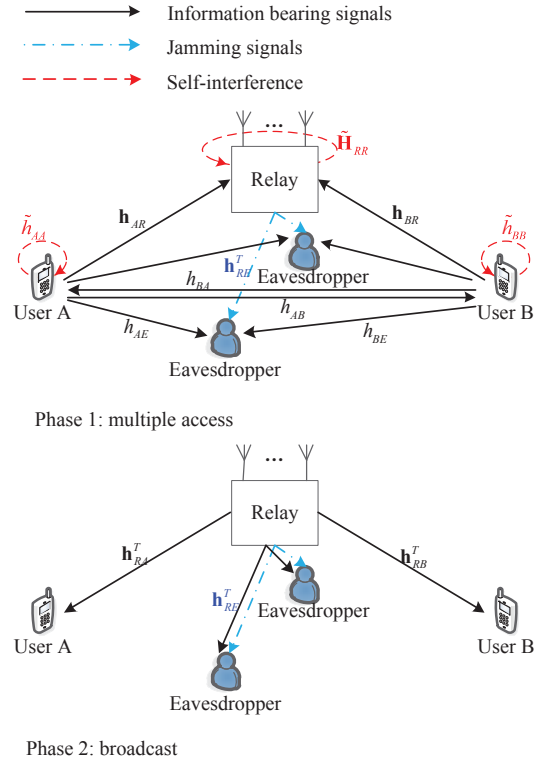


Fig. 1. An illustration of the secrecy NOMA-based TWR network.

\mathbf{h}_{AR} , \mathbf{h}_{BR} , \mathbf{h}_{RA}^T , \mathbf{h}_{RB}^T , and \mathbf{h}_{RE}^T , respectively. Moreover, it is assumed that the eavesdropper has full access to the global CSI; however, the legitimate users and relay only know that the CSI is not related to the eavesdroppers. The bidirectional communication consists of a multiple-access phase and a broadcast phase, in which the eavesdropper can overhear the signals from both phases.

1) *Multiple-Access Phase*: In the first phase, two legitimate users transmit their signals simultaneously to each other and the relay node while the eavesdropper receives the signals silently. For the implementation of NOMA, User A splits itself into two sub-users, say A1 and A2, with the power ratios α and $1 - \alpha$ respectively, and so does User B. Then each legitimate user transmits the signals of two sub-users by adopting the superposition code, which are given in the form of

$$x_A = \sqrt{\alpha P_A} s_{A1} + \sqrt{(1 - \alpha) P_A} s_{A2} \quad (1)$$

$$x_B = \sqrt{\alpha P_B} s_{B1} + \sqrt{(1 - \alpha) P_B} s_{B2} \quad (2)$$

for Users A and B , respectively, where s_δ denotes the independent data symbol of Sub-user δ with $\mathbb{E}[|s_\delta|^2] = 1$ for $\delta \in \{A1, A2, B1, B2\}$, and P_A and P_B stand for the transmit powers of Users A and B , respectively. According to the NOMA principle, s_{A1} and s_{B1} are allocated with more power and we have $\sqrt{\alpha} > \sqrt{1-\alpha}$, i.e., $0.5 < \alpha < 1$. By applying (1) and (2) at user nodes, we provide receivers with the freedom to decide which fraction of the interference to decode along with the desired signal and improve the spectral efficiency by exploiting channel gain differences between sub-users.

To protect the information in the first phase, we assume the relay operates in the full-duplex mode to receive signals from the legitimate users while radiating jamming signals simultaneously to degrade the quality of the potential eavesdroppers by using the artificial noise scheme. The key idea of generating artificial noises for secure communications is to confuse the potential eavesdroppers without interfering the legitimate users by exploiting the null space of the legitimate channels. Let the singular value decomposition [45] of $\mathbf{H}_{RU} = [\mathbf{h}_{RA} \ \mathbf{h}_{RB}]^T \in \mathbb{C}^{2 \times N_R}$ be expressed as

$$\mathbf{H}_{RU} = \mathbf{U} \begin{bmatrix} \mathbf{\Lambda} & \mathbf{0}_{2 \times (N_R - 2)} \end{bmatrix} [\mathbf{W}_U \ \mathbf{W}_E]^H \quad (3)$$

where $\mathbf{h}_{RA} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RA} \mathbf{I}_{N_R})$ and $\mathbf{h}_{RB} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RB} \mathbf{I}_{N_R})$ denote the channel vectors from the relay to the legitimate users, $\mathbf{W} = [\mathbf{W}_U \ \mathbf{W}_E]$ forms an orthonormal basis of $\mathbb{C}^{N_R \times N_R}$ with $\mathbf{W}_U \in \mathbb{C}^{N_R \times 2}$ and $\mathbf{W}_E \in \mathbb{C}^{N_R \times (N_R - 2)}$ standing for the range space and null space of \mathbf{H}_{RU} , respectively, and $\mathbf{\Lambda}$ is a diagonal matrix whose diagonal entries are two singular values. Using the artificial noise scheme, the jamming signal vector radiated at the relay in the first phase is designed in the form of

$$\mathbf{x}_R^{(1)} = \mathbf{W}_E \sqrt{\frac{P_R}{N_R - 2}} \mathbf{v}^{(1)} \quad (4)$$

where $\mathbf{v}^{(1)} \sim \mathcal{N}_c(\mathbf{0}_{(N_R - 2) \times 1}, \mathbf{I}_{N_R - 2})$ is the artificial noise vector and P_R denotes the transmit power of the relay that is equally allocated to the $N_R - 2$ entries of $\mathbf{v}^{(1)}$.

After suppressing the self-interference, the signal received at the relay node in the first phase can be written as

$$\mathbf{y}_R = \mathbf{h}_{AR}x_A + \mathbf{h}_{BR}x_B + \tilde{\mathbf{H}}_{RR}\mathbf{x}_R^{(1)} + \mathbf{n}_R = \mathbf{H}_{UR} \begin{bmatrix} x_A \\ x_B \end{bmatrix} + \tilde{\mathbf{n}}_R \quad (5)$$

where $\mathbf{H}_{UR} = [\mathbf{h}_{AR} \ \mathbf{h}_{BR}] \in \mathbb{C}^{N_R \times 2}$ represents the channel matrix from the legitimate users to the relay with $\mathbf{h}_{AR} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{AR} \mathbf{I}_{N_R})$ and $\mathbf{h}_{BR} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{BR} \mathbf{I}_{N_R})$, $\mathbf{n}_R \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \sigma_R^2 \mathbf{I}_{N_R})$ is an additive white Gaussian noise (AWGN) vector, $\tilde{\mathbf{H}}_{RR}$ denotes the residual self-interference channel due to the imperfect interference mitigation at the relay node whose entries are independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with variance β_{RR} , $\tilde{\mathbf{n}}_R = \tilde{\mathbf{H}}_{RR} \mathbf{x}_R^{(1)} + \mathbf{n}_R$ stands for the residual-interference-plus-noise vector, which is modeled by a zero-mean complex Gaussian random vector, i.e., $\tilde{\mathbf{n}}_R \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, (P_R \beta_{RR} + \sigma_R^2) \mathbf{I}_{N_R})$. After receiving the signals from the users as in (5), the relay first applies the zero-forcing (ZF) equalization to decompose the data streams from the two users, which can be expressed as

$$\mathbf{z}_R = \mathbf{C}_{ZF} \mathbf{y}_R = \begin{bmatrix} x_A \\ x_B \end{bmatrix} + \mathbf{C}_{ZF} \tilde{\mathbf{n}}_R = \begin{bmatrix} \sqrt{\alpha P_{AS} s_{A1}} + \sqrt{(1-\alpha) P_{AS} s_{A2}} \\ \sqrt{\alpha P_{BS} s_{B1}} + \sqrt{(1-\alpha) P_{BS} s_{B2}} \end{bmatrix} + \begin{bmatrix} \bar{n}_A \\ \bar{n}_B \end{bmatrix} \quad (6)$$

where $\mathbf{C}_{ZF} = (\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \mathbf{H}_{UR}^H$ denotes the equalization matrix, and \bar{n}_A and \bar{n}_B are the equalized noises corresponding to the data streams from Users A and B , respectively. In particular, the variances of \bar{n}_A and \bar{n}_B are given by

$$\bar{\sigma}_A^2 = (P_R \beta_{RR} + \sigma_R^2) \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{1,1}, \quad \bar{\sigma}_B^2 = (P_R \beta_{RR} + \sigma_R^2) \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{2,2} \quad (7)$$

where $[\cdot]_{i,i}$ denotes the i -th diagonal element of the square matrix. By denoting

$$\rho_A = \frac{1}{\beta_{AR} \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{1,1}}, \quad \rho_B = \frac{1}{\beta_{BR} \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{2,2}} \quad (8)$$

we have $\bar{\sigma}_A^2 = (P_R \beta_{RR} + \sigma_R^2) / (\beta_{AR} \rho_A)$ and $\bar{\sigma}_B^2 = (P_R \beta_{RR} + \sigma_R^2) / (\beta_{BR} \rho_B)$, where $\rho_\delta \sim \chi_{2(N_R-1)}^2$ with the complementary cumulative density function (CCDF) [46], [47] as

$$\bar{F}_{\rho_\delta}(x) = \exp(-x) \sum_{k=0}^{N_R-2} \frac{x^k}{k!}, \quad x \geq 0 \quad (9)$$

for $\delta \in \{A, B\}$.

Thanks to the recent advances in full-duplex mobile device [48]–[50], we also equip two legitimate user nodes with the full-duplex mode during the first phase so that they can receive the NOMA signals from each other to improve the network performance. As the artificial noise vector $\mathbf{v}^{(1)}$ is projected into the null space of \mathbf{H}_{RU} in (4), the signals received at the legitimate

user nodes A and B are respectively given by

$$y_A^{(1)} = h_{BA}x_B + \tilde{h}_{AA}x_A + n_A^{(1)} = h_{BA} \left(\sqrt{\alpha P_B} s_{B1} + \sqrt{(1-\alpha) P_B} s_{B2} \right) + \tilde{n}_A^{(1)} \quad (10)$$

$$y_B^{(1)} = h_{AB}x_A + \tilde{h}_{BB}x_B + n_B^{(1)} = h_{AB} \left(\sqrt{\alpha P_A} s_{A1} + \sqrt{(1-\alpha) P_A} s_{A2} \right) + \tilde{n}_B^{(1)} \quad (11)$$

which are not interfered by the jamming signal vector $\mathbf{x}_R^{(1)}$ with the leverage of the null space property $\mathbf{H}_{RU} \mathbf{W}_E = \mathbf{0}_{2 \times (N_R - 2)}$, where $h_{BA} \sim \mathcal{N}_c(0, \beta_{BA})$ and $h_{AB} \sim \mathcal{N}_c(0, \beta_{AB})$ are the direct links between the users, $n_A^{(1)} \sim \mathcal{N}_c(0, \sigma_A^2)$ and $n_B^{(1)} \sim \mathcal{N}_c(0, \sigma_B^2)$ are the complex AWGNs, \tilde{h}_{AA} and \tilde{h}_{BB} denote the residual self-interference channels with the normalized gains β_{AA} and β_{BB} , respectively, and $\tilde{n}_A^{(1)} = \tilde{h}_{AA}x_A + n_A^{(1)}$ and $\tilde{n}_B^{(1)} = \tilde{h}_{BB}x_B + n_B^{(1)}$ stand for the residual-interference-plus-noises, which are modeled by the zero-mean complex Gaussian random variables, i.e., $\tilde{n}_A^{(1)} \sim \mathcal{N}_c(0, P_A\beta_{AA} + \sigma_A^2)$ and $\tilde{n}_B^{(1)} \sim \mathcal{N}_c(0, P_B\beta_{BB} + \sigma_B^2)$ at Users A and B , respectively.

Concurrently, the signal received at the passive eavesdropper in the first phase is given by

$$y_E^{(1)} = h_{AE}x_A + h_{BE}x_B + \mathbf{h}_{RE}^T \mathbf{x}_R^{(1)} + n_E^{(1)} \quad (12)$$

$$\begin{aligned} &= h_{AE} \left(\sqrt{\alpha P_A} s_{A1} + \sqrt{(1-\alpha) P_A} s_{A2} \right) + h_{BE} \left(\sqrt{\alpha P_B} s_{B1} + \sqrt{(1-\alpha) P_B} s_{B2} \right) \\ &\quad + \mathbf{h}_{RE}^T \mathbf{W}_E \sqrt{\frac{P_R}{N_R - 2}} \mathbf{v}^{(1)} + n_E^{(1)} \end{aligned} \quad (13)$$

where $h_{AE} \sim \mathcal{N}_c(0, \beta_{AE})$, $h_{BE} \sim \mathcal{N}_c(0, \beta_{BE})$, $\mathbf{h}_{RE} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RE} \mathbf{I}_{N_R})$ are the channels related to the eavesdropper, and $n_E^{(1)} \sim \mathcal{N}_c(0, \sigma_E^2)$ is the complex AWGN.

2) *Broadcast Phase*: After decoupling the two data streams by ZF equalization, the relay decodes them separately according to (6). **Then, to confuse the potential eavesdropper and coordinate the transmission of two low-power sub-users ($A2$ and $B2$) simultaneously in the second phase, the relay mixes some artificial noises with two data symbols s_{A2} and s_{B2} , which is designed in the form of**

$$\mathbf{x}_R^{(2)} = \mathbf{W}_U \sqrt{\frac{\phi P_R}{2}} \begin{bmatrix} s_{B2} \\ s_{A2} \end{bmatrix} + \mathbf{W}_E \sqrt{\frac{(1-\phi) P_R}{N_R - 2}} \mathbf{v}^{(2)} \quad (14)$$

where ϕ denotes the power allocation ratio of the signal power to the total transmit power P_R for the artificial noise scheme and $\mathbf{v}^{(2)} \sim \mathcal{N}_c(\mathbf{0}_{(N_R-2) \times 1}, \mathbf{I}_{N_R-2})$ is the artificial noise vector generated in the second phase.

As the artificial noise vector $\mathbf{v}^{(2)}$ is projected into the null space of \mathbf{H}_{UR} in (14), the signals

received at the legitimate user nodes A and B are respectively given by

$$y_A^{(2)} = \mathbf{h}_{RA}^T \mathbf{x}_R^{(2)} + n_A^{(2)} = \mathbf{h}_{RA}^T \mathbf{W}_U \sqrt{\frac{\phi P_R}{2}} \begin{bmatrix} s_{B2} \\ s_{A2} \end{bmatrix} + n_A^{(2)} \quad (15)$$

$$y_B^{(2)} = \mathbf{h}_{RB}^T \mathbf{x}_R^{(2)} + n_B^{(2)} = \mathbf{h}_{RB}^T \mathbf{W}_U \sqrt{\frac{\phi P_R}{2}} \begin{bmatrix} s_{B2} \\ s_{A2} \end{bmatrix} + n_B^{(2)} \quad (16)$$

where $\mathbf{h}_{RA} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RA} \mathbf{I}_{N_R})$ and $\mathbf{h}_{RB} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RB} \mathbf{I}_{N_R})$ denote the channels from the relay to the users, and $n_A^{(2)} \sim \mathcal{N}_c(0, \sigma_A^2)$ and $n_B^{(2)} \sim \mathcal{N}_c(0, \sigma_B^2)$ are the complex AWGNs at Users A and B , respectively. Since signal s_{A2} is generated by User A , User A can perform the self-interference cancellation of s_{A2} before decoding its desired signal s_{B2} in (15), and so can User B in (16). By denoting $\mathbf{W}_U = [\mathbf{w}_A \ \mathbf{w}_B]$, we can rewrite the signal models in (15) and (16) after the self-interference cancellation as

$$y_A^{(2)} = \mathbf{h}_{RA}^T \mathbf{w}_A \sqrt{\frac{\phi P_R}{2}} s_{B2} + n_A^{(2)} \quad (17)$$

$$y_B^{(2)} = \mathbf{h}_{RB}^T \mathbf{w}_B \sqrt{\frac{\phi P_R}{2}} s_{A2} + n_B^{(2)}. \quad (18)$$

During the second phase, the signal received at the eavesdropper is given by

$$\begin{aligned} y_E^{(2)} &= \mathbf{h}_{RE}^T \mathbf{x}_R^{(2)} + n_E^{(2)} \\ &= \mathbf{h}_{RE}^T \mathbf{w}_B \sqrt{\frac{\phi P_R}{2}} s_{A2} + \mathbf{h}_{RE}^T \mathbf{w}_A \sqrt{\frac{\phi P_R}{2}} s_{B2} + \mathbf{h}_{RE}^T \mathbf{W}_E \sqrt{\frac{(1-\phi) P_R}{N_R - 2}} \mathbf{v}^{(2)} + n_E^{(2)} \end{aligned} \quad (19)$$

where $n_E^{(2)} \sim \mathcal{N}_c(0, \sigma_E^2)$ is the complex AWGN in the second phase.

Remark: To ensure the secure communication, the relay keeps emitting the jamming signals to degrade the performance of the potential eavesdroppers by employing the artificial noise scheme. In the first phase the relay only emits the pure jamming signals while in the second phase it transmits the mixture of the information-bearing signals and the jamming signals. **In that way, the relay plays two important roles in the secure NOMA-based two-way relay network: not only forwards the confidential information for two sub-users but also jams the potential eavesdroppers.**

B. Decoding Scheme Based on SIC

In (6), the relay decodes s_{A1} and s_{B1} by treating s_{A2} and s_{B2} as interference, respectively, where the signal-to-interference-plus-noise ratios (SINRs) for s_{A1} and s_{B1} are given by

$$\gamma_{A1}^R = \frac{\alpha P_A}{(1-\alpha)P_A + \bar{\sigma}_A^2} = \frac{\alpha P_A}{(1-\alpha)P_A + \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR\rho_A}}} \quad (20)$$

$$\gamma_{B1}^R = \frac{\alpha P_B}{(1-\alpha)P_B + \bar{\sigma}_B^2} = \frac{\alpha P_B}{(1-\alpha)P_B + \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{BR\rho_B}}}. \quad (21)$$

After using the SIC to remove the interference of s_{A1} and s_{B1} , the relay then decodes s_{A2} and s_{B2} with the SINRs given by

$$\gamma_{A2}^R = \frac{(1-\alpha)P_A}{\bar{\sigma}_A^2} = \frac{(1-\alpha)P_A}{\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR\rho_A}}} = \frac{(1-\alpha)P_A \beta_{AR\rho_A}}{P_R \beta_{RR} + \sigma_R^2} \quad (22)$$

$$\gamma_{B2}^R = \frac{(1-\alpha)P_B}{\bar{\sigma}_B^2} = \frac{(1-\alpha)P_B}{\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{BR\rho_B}}} = \frac{(1-\alpha)P_B \beta_{BR\rho_B}}{P_R \beta_{RR} + \sigma_R^2}. \quad (23)$$

During the first phase, by treating s_{B2} and s_{A2} as interference, Users B and A decode s_{A1} and s_{B1} according to (11) and (10) with the SINRs given by

$$\gamma_{A1}^B = \frac{|h_{AB}|^2 \alpha P_A}{|h_{AB}|^2 (1-\alpha)P_A + P_B \beta_{BB} + \sigma_B^2} \quad (24)$$

$$\gamma_{B1}^A = \frac{|h_{BA}|^2 \alpha P_B}{|h_{BA}|^2 (1-\alpha)P_B + P_A \beta_{AA} + \sigma_A^2}. \quad (25)$$

While in the second phase, Users B and A decode s_{A2} and s_{B2} directly in (18) and (17) after the self-interference cancellation, leading to the signal-to-noise ratios (SNRs) for s_{A2} and s_{B2} given by

$$\gamma_{A2}^B = \frac{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2 \phi P_R}{2\sigma_B^2} \quad (26)$$

$$\gamma_{B2}^A = \frac{|\mathbf{h}_{RA}^T \mathbf{w}_A|^2 \phi P_R}{2\sigma_A^2}. \quad (27)$$

From above, it can be observed that the decoding of different data symbols is associated with different channels, which exploits the channel gain differences to achieve better system performance with NOMA proposal.

In the proposed NOMA-based two-way relay network, the potential eavesdropper can overhear

the confidential information twice, namely, the information transmitted by the legitimate users in the first phase and the information broadcast by the relay in the second phase. In the first phase, the eavesdropper receives four data symbols s_{A1} , s_{A2} , s_{B1} , and s_{B2} simultaneously, which can be tough to decode by using the SIC scheme based on (13) only. While in the second phase, the eavesdropper only receives two data symbols s_{A2} and s_{B2} according to (19), which is more feasible by using the SIC scheme. Therefore, to better wiretap the information from the perspective of the eavesdropper, we provide it with a sophisticated strategy by first decoding s_{A2} and s_{B2} in (19), and then stripping them off before decoding s_{A1} and s_{B1} in (13). Specifically, based on (19), **the eavesdropper first decodes s_{A2} by treating s_{B2} as interference**, yielding the SINR of s_{A2} as

$$\gamma_{A2}^E = \frac{\frac{|\mathbf{h}_{RE}^T \mathbf{w}_B|^2 \phi P_R}{2}}{\frac{|\mathbf{h}_{RE}^T \mathbf{w}_A|^2 \phi P_R}{2} + \frac{(1-\phi)P_R \|\mathbf{h}_{RE}^T \mathbf{w}_E\|^2}{N_R-2} + \sigma_E^2}, \quad (28)$$

then decodes s_{B2} after subtracting s_{A2} , obtaining the SINR of s_{B2} as

$$\gamma_{B2}^E = \frac{\frac{|\mathbf{h}_{RE}^T \mathbf{w}_A|^2 \phi P_R}{2}}{\frac{(1-\phi)P_R \|\mathbf{h}_{RE}^T \mathbf{w}_E\|^2}{N_R-2} + \sigma_E^2}. \quad (29)$$

As the eavesdropper has decoded s_{A2} and s_{B2} , it can strip them off in (13), which yields

$$y_E^{(1)} = h_{AE} \sqrt{\alpha P_A} s_{A1} + h_{BE} \sqrt{\alpha P_B} s_{B1} + \mathbf{h}_{RE}^T \mathbf{w}_E \sqrt{\frac{P_R}{N_R-2}} \mathbf{v}^{(1)} + n_E^{(1)}. \quad (30)$$

Based on (30), **the eavesdropper first decodes s_{A1} by treating s_{B1} as interference**, which obtains the SINR of s_{A1} as

$$\gamma_{A1}^E = \frac{|h_{AE}|^2 \alpha P_A}{|h_{BE}|^2 \alpha P_B + \frac{P_R \|\mathbf{h}_{RE}^T \mathbf{w}_E\|^2}{N_R-2} + \sigma_E^2}. \quad (31)$$

After applying the SIC to cancel the interference of s_{A1} in (30), the eavesdropper then decodes s_{B1} with the SINR given by

$$\gamma_{B1}^E = \frac{|h_{BE}|^2 \alpha P_B}{\frac{P_R \|\mathbf{h}_{RE}^T \mathbf{w}_E\|^2}{N_R-2} + \sigma_E^2}. \quad (32)$$

As revealed in (28), (29), (31), and (32), the eavesdropper first decodes the data symbols from User A and then from User B , which is a specific decoding order that we consider for the

eavesdropper. It is worth pointing out different decoding orders will result in different SINRs and further different ergodic rates of data symbols achieved by the eavesdropper, which will not be discussed further due to the limited space.

III. PERFORMANCE ANALYSIS FOR THE SINGLE-EAVESDROPPER CASE

In this section, we analyze the performance of the proposed network in terms of secrecy rate. Specifically, the instantaneous and ergodic secrecy rates of each data symbol are respectively given by [51]

$$C_\delta^{sec} = [C_\delta - C_\delta^E]^+, \quad \bar{C}_\delta^{sec} = [\bar{C}_\delta - \bar{C}_\delta^E]^+ \quad (33)$$

for $\delta \in \{A1, A2, B1, B2\}$ and $[x]^+ = \max\{x, 0\}$, where C_δ and \bar{C}_δ denote the instantaneous and ergodic rates of data symbol s_δ for the legitimate channel, respectively, and C_δ^E and \bar{C}_δ^E denote the instantaneous and ergodic rates of data symbol s_δ for the wiretap channel, respectively. In the following, we will derive both the instantaneous and ergodic rates for different data symbols, based on which the secrecy rates can be calculated via (33).

A. Achievable Rate Analysis for Legitimate Users

As illustrated in Section II-B, regardless of the eavesdropper, data symbols s_{A1} , s_{A2} , s_{B1} , and s_{B2} should be decoded at the legitimate users as well as the relay. To ensure the decoding correctness of s_{A1} at the relay and User B , the achievable rate of s_{A1} using (20) and (24) should be

$$\begin{aligned} C_{A1} &= \frac{1}{2} \min \{ \log_2 (1 + \gamma_{A1}^R), \log_2 (1 + \gamma_{A1}^B) \} = \frac{1}{2} \log_2 (1 + \min \{ \gamma_{A1}^R, \gamma_{A1}^B \}) \\ &= \frac{1}{2} \log_2 \left(1 + \min \left\{ \frac{\alpha P_A}{(1 - \alpha) P_A + \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR} \rho_A}}, \frac{|h_{AB}|^2 \alpha P_A}{|h_{AB}|^2 (1 - \alpha) P_A + P_B \beta_{BB} + \sigma_B^2} \right\} \right) \\ &= \frac{1}{2} \log_2 \left(1 + \frac{\alpha P_A \min \left\{ \frac{\beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|h_{AB}|^2}{P_B \beta_{BB} + \sigma_B^2} \right\}}{(1 - \alpha) P_A \min \left\{ \frac{\beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|h_{AB}|^2}{P_B \beta_{BB} + \sigma_B^2} \right\} + 1} \right) \\ &= \frac{1}{2} \log_2 \left(1 + P_A \min \left\{ \frac{\beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|h_{AB}|^2}{P_B \beta_{BB} + \sigma_B^2} \right\} \right) \\ &\quad - \frac{1}{2} \log_2 \left(1 + (1 - \alpha) P_A \min \left\{ \frac{\beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|h_{AB}|^2}{P_B \beta_{BB} + \sigma_B^2} \right\} \right). \end{aligned} \quad (34)$$

Following a procedure similar to (34), for symbol s_{B1} decoded at the relay and User A, its achievable rate using (21) and (25) is given by

$$\begin{aligned} C_{B1} &= \frac{1}{2} \min \{ \log_2 (1 + \gamma_{B1}^R), \log_2 (1 + \gamma_{B1}^A) \} = \frac{1}{2} \log_2 (1 + \min \{ \gamma_{B1}^R, \gamma_{B1}^A \}) \\ &= \frac{1}{2} \log_2 \left(1 + P_B \min \left\{ \frac{\beta_{BR}\rho_B}{P_R\beta_{RR} + \sigma_R^2}, \frac{|h_{BA}|^2}{P_A\beta_{AA} + \sigma_A^2} \right\} \right) \\ &\quad - \frac{1}{2} \log_2 \left(1 + (1 - \alpha) P_B \min \left\{ \frac{\beta_{BR}\rho_B}{P_R\beta_{RR} + \sigma_R^2}, \frac{|h_{BA}|^2}{P_A\beta_{AA} + \sigma_A^2} \right\} \right). \end{aligned} \quad (35)$$

By using (22) and (26), the achievable rate associated with symbol s_{A2} is obtained as

$$\begin{aligned} C_{A2} &= \frac{1}{2} \min \{ \log_2 (1 + \gamma_{A2}^R), \log_2 (1 + \gamma_{A2}^B) \} = \frac{1}{2} \log_2 (1 + \min \{ \gamma_{A2}^R, \gamma_{A2}^B \}) \\ &= \frac{1}{2} \log_2 \left(1 + \min \left\{ \frac{(1 - \alpha) P_A \beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2 \phi P_R}{2\sigma_B^2} \right\} \right). \end{aligned} \quad (36)$$

Similarly, by using (23) and (27), the achievable rate of symbol s_{B2} is obtained as

$$\begin{aligned} C_{B2} &= \frac{1}{2} \min \{ \log_2 (1 + \gamma_{B2}^R), \log_2 (1 + \gamma_{B2}^B) \} = \frac{1}{2} \log_2 (1 + \min \{ \gamma_{B2}^R, \gamma_{B2}^B \}) \\ &= \frac{1}{2} \log_2 \left(1 + \min \left\{ \frac{(1 - \alpha) P_B \beta_{BR} \rho_B}{P_R \beta_{RR} + \sigma_R^2}, \frac{|\mathbf{h}_{RA}^T \mathbf{w}_A|^2 \phi P_R}{2\sigma_A^2} \right\} \right). \end{aligned} \quad (37)$$

Based on the above instantaneous results on achievable rates, we will derive the ergodic rates of the four data symbols for the legitimate users in the following.

Proposition 1: By defining the function

$$\mathbb{D}(k, \mu, b) \triangleq \int_0^\infty \frac{x^k \exp(-\mu x)}{x + b} dx = -(-b)^k \exp(b\mu) \text{Ei}(-b\mu) + \sum_{n=1}^k (n-1)! (-b)^{k-n} \mu^{-n} \quad (38)$$

in which $\text{Ei}(\cdot)$ denotes the exponential integral function [52, Eq. (8.211.1)], the ergodic rate of s_{A1} can be expressed as

$$\begin{aligned} \bar{C}_{A1} &= \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} \right)^k}{k!} \left(\mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}}, \frac{1}{P_A} \right) \right. \\ &\quad \left. - \mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}}, \frac{1}{(1 - \alpha) P_A} \right) \right). \end{aligned} \quad (39)$$

Proof: See Appendix A. ■

Following the similar derivations in the proof of Proposition 1, we can obtain the ergodic rate of s_{B1} as

$$\begin{aligned} \bar{C}_{B1} = & \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{BR}} \right)^k}{k!} \left(\mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{BR}} + \frac{P_A \beta_{AA} + \sigma_A^2}{\beta_{BA}}, \frac{1}{P_B} \right) \right. \\ & \left. - \mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{BR}} + \frac{P_A \beta_{AA} + \sigma_A^2}{\beta_{BA}}, \frac{1}{(1-\alpha) P_B} \right) \right). \end{aligned} \quad (40)$$

Proposition 2: Given the function defined in (38), the ergodic rate of s_{A2} can be expressed as

$$\bar{C}_{A2} = \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{(1-\alpha) P_A \beta_{AR}} \right)^k}{k!} \mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{(1-\alpha) P_A \beta_{AR}} + \frac{2\sigma_B^2}{\phi P_R \beta_{RB}}, 1 \right). \quad (41)$$

Proof: See Appendix B. ■

Following a similar methodology in the proof of Proposition 2, we can obtain the ergodic rate of s_{B2} as

$$\bar{C}_{B2} = \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{(1-\alpha) P_B \beta_{BR}} \right)^k}{k!} \mathbb{D} \left(k, \frac{P_R \beta_{RR} + \sigma_R^2}{(1-\alpha) P_B \beta_{BR}} + \frac{2\sigma_A^2}{\phi P_R \beta_{RA}}, 1 \right). \quad (42)$$

B. Achievable Rate Analysis for Eavesdropper

According to (28), (29), (31), and (32), the instantaneous achievable rate of each data symbol at the eavesdropper can be calculated via

$$C_{\delta}^E = \frac{1}{2} \log_2 (1 + \gamma_{\delta}^E) \quad (43)$$

for $\delta \in \{A1, A2, B1, B2\}$. Given the instantaneous results of achievable rates above, in the following we will derive the ergodic rates of the four data symbols achieved at the eavesdropper.

Proposition 3: By defining the function

$$\mathbb{G}(i, \mu, b) \triangleq \int_0^{\infty} \frac{\exp(-\mu x)}{(x+b)^i} dx = \frac{1}{(i-1)!} \sum_{k=1}^{i-1} (k-1)! (-\mu)^{i-k-1} b^{-k} - \frac{(-\mu)^{i-1}}{(i-1)!} \exp(b\mu) \text{Ei}(-b\mu) \quad (44)$$

the ergodic rate of s_{A2} at the eavesdropper can be expressed as

$$\bar{C}_{A2}^E = \frac{1}{2 \ln 2} \left(\sum_{i=1}^{N_R-2} \Omega_{A2}^i \mathbb{G} \left(i, \frac{2\sigma_E^2}{\phi P_R \beta_{RE}}, \frac{\phi(N_R-2)}{2(1-\phi)} \right) + \sum_{i=1}^2 \Psi_{A2}^i \mathbb{G} \left(i, \frac{2\sigma_E^2}{\phi P_R \beta_{RE}}, 1 \right) \right) \quad (45)$$

where

$$\Omega_{A2}^i = \left(\frac{\phi(N_R-2)}{2(1-\phi)} \right)^{N_R-2} (-1)^{(N_R-2-i)} (N_R-1-i) \left(1 - \frac{\phi(N_R-2)}{2(1-\phi)} \right)^{i-N_R} \quad (46)$$

$$\Psi_{A2}^i = \left(\frac{\phi(N_R-2)}{2(1-\phi)} \right)^{N_R-2} \frac{(-1)^{(2-i)} (N_R-1-i)!}{(N_R-3)!} \left(\frac{\phi(N_R-2)}{2(1-\phi)} - 1 \right)^{i-N_R}. \quad (47)$$

Proof: See Appendix C. ■

Following the similar derivations in the proof of the Proposition 3, we can obtain the CCDFs of γ_{B2}^E , γ_{A1}^E , and γ_{B1}^E in (29), (31), and (32) as

$$\bar{F}_{\gamma_{B2}^E} = \exp \left(-\frac{2\sigma_E^2}{\phi P_R \beta_{RE}} x \right) \left(1 + \frac{2(1-\phi)}{\phi(N_R-2)} x \right)^{2-N_R} \quad (48)$$

$$\bar{F}_{\gamma_{A1}^E} = \exp \left(-\frac{\sigma_E^2}{\alpha P_A \beta_{AE}} x \right) \left(1 + \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R-2)} x \right)^{2-N_R} (x+1)^{-1} \quad (49)$$

$$\bar{F}_{\gamma_{B1}^E} = \exp \left(-\frac{\sigma_E^2}{\alpha P_B \beta_{BE}} x \right) \left(1 + \frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R-2)} x \right)^{2-N_R}. \quad (50)$$

The ergodic rates of s_{B2} , s_{A1} , s_{B1} achieved by the eavesdropper are given by

$$\bar{C}_{B2}^E = \frac{1}{2 \ln 2} \left(\sum_{i=1}^{N_R-2} \Omega_{B2}^i \mathbb{G} \left(i, \frac{2\sigma_E^2}{\phi P_R \beta_{RE}}, \frac{\phi(N_R-2)}{2(1-\phi)} \right) + \Psi_{B2}^1 \mathbb{G} \left(1, \frac{2\sigma_E^2}{\phi P_R \beta_{RE}}, 1 \right) \right) \quad (51)$$

$$\bar{C}_{A1}^E = \frac{1}{2 \ln 2} \left(\sum_{i=1}^{N_R-2} \Omega_{A1}^i \mathbb{G} \left(i, \frac{\sigma_E^2}{\alpha P_A \beta_{AE}}, \frac{\alpha P_A \beta_{AE} (N_R-2)}{P_R \beta_{RE}} \right) + \sum_{i=1}^2 \Psi_{A1}^i \mathbb{G} \left(i, \frac{\sigma_E^2}{\alpha P_A \beta_{AE}}, 1 \right) \right) \quad (52)$$

$$\bar{C}_{B1}^E = \frac{1}{2 \ln 2} \left(\sum_{i=1}^{N_R-2} \Omega_{B1}^i \mathbb{G} \left(i, \frac{\sigma_E^2}{\alpha P_B \beta_{BE}}, \frac{\alpha P_A \beta_{BE} (N_R-2)}{P_R \beta_{RE}} \right) + \Psi_{B1}^1 \mathbb{G} \left(1, \frac{\sigma_E^2}{\alpha P_B \beta_{BE}}, 1 \right) \right) \quad (53)$$

where Ω_δ^i and Ψ_δ^i for $\delta \in \{A1, B1, B2\}$ are the coefficients obtained by using the partial-fraction expansion [53, appendix], similar to (46) and (47). After we have the results for the legitimate users in (39)–(42) and for the eavesdropper in (45) and (51)–(53), the ergodic secrecy rate of each data symbol can be calculated via (33) for the proposed network under the single-eavesdropper case.

IV. EXTENSION TO MULTIPLE EAVESDROPPERS

In this section, we consider the network under the existence of multiple eavesdroppers, where the number of eavesdroppers is denoted by N_E . When multiple eavesdroppers sneak into the network, their noise levels may be different and even unknown to the legitimate users and the relay. Therefore, to ensure secure communications, it is reasonable to consider the worst-case scenario where the noises are extremely small at the eavesdroppers (i.e., $\sigma_{E_i}^2 = 0$ for $i = 1, \dots, N_E$) [27], [30], [31]. We assume each eavesdropper experiences independent channel fading and follows the same signal model as the single-eavesdropper case in Section II-A. In the following, we consider two cases, namely, non-colluding and colluding eavesdroppers.

A. Non-colluding Case

According to the SINRs of different data symbols given in (28), (29), (31), and (32) with $\sigma_E^2 = 0$ and following the similar derivations in (83), we can obtain

$$\bar{F}_{\gamma_{A1}^{E_i}} = \left(1 + \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R - 2)} x\right)^{2-N_R} (x+1)^{-1} \quad (54)$$

$$\bar{F}_{\gamma_{A2}^{E_i}} = \left(1 + \frac{2(1-\phi)}{\phi(N_R-2)} x\right)^{2-N_R} (x+1)^{-1} \quad (55)$$

$$\bar{F}_{\gamma_{B1}^{E_i}} = \left(1 + \frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R - 2)} x\right)^{2-N_R} \quad (56)$$

$$\bar{F}_{\gamma_{B2}^{E_i}} = \left(1 + \frac{2(1-\phi)}{\phi(N_R-2)} x\right)^{2-N_R} \quad (57)$$

for $i = 1, \dots, N_E$. We assume the eavesdroppers work in a non-colluding way to wiretap the information [28], [54], [55] and the highest SINR of each data symbol is chosen for decoding, i.e., $\gamma_\delta^E = \max\{\gamma_\delta^{E_1}, \gamma_\delta^{E_2}, \dots, \gamma_\delta^{E_{N_E}}\}$, whose CDF can be obtained as

$$\begin{aligned} F_{\gamma_\delta^E}(x) &= \Pr\{\gamma_\delta^E < x\} = \Pr\{\gamma_\delta^{E_1} < x, \gamma_\delta^{E_2} < x, \dots, \gamma_\delta^{E_{N_E}} < x\} \\ &= \prod_{i=1}^{N_E} F_{\gamma_\delta^{E_i}} = \left(1 - \bar{F}_{\gamma_\delta^{E_1}}\right)^{N_E} = 1 + \sum_{i=1}^{N_E} \binom{N_E}{i} \left(-\bar{F}_{\gamma_\delta^{E_1}}\right)^i \end{aligned} \quad (58)$$

where $\delta \in \{A1, A2, B1, B2\}$ and $\binom{N_E}{i}$ denotes the binomial coefficient. With (58), the ergodic rate of each data symbol achieved by the non-colluding eavesdroppers is given by

$$\bar{C}_\delta^E = \int_0^\infty \frac{1}{2} \log_2(1+x) f_{\gamma_\delta^E}(x) dx = \frac{1}{2 \ln 2} \ln(1+x) F_{\gamma_\delta^E}(x) \Big|_0^\infty - \frac{1}{2 \ln 2} \int_0^\infty F_{\gamma_\delta^E}(x) d \ln(1+x)$$

$$\begin{aligned}
&= \frac{1}{2 \ln 2} \ln(1+x) \Big|_0^\infty - \frac{1}{2 \ln 2} \int_0^\infty F_{\gamma_\delta^E}(x) d \ln(1+x) = \frac{1}{2 \ln 2} \int_0^\infty \frac{1 - F_{\gamma_\delta^E}(x)}{1+x} dx \\
&= -\frac{1}{2 \ln 2} \sum_{i=1}^{N_E} \binom{N_E}{i} \int_0^\infty \frac{\left(-\bar{F}_{\gamma_\delta^{E_1}}\right)^i}{1+x} dx
\end{aligned} \tag{59}$$

where $\delta \in \{A1, A2, B1, B2\}$ and integration by parts is applied to (59). By substituting (54)–(57) into (59) and using [52, Eq. (3.197.5)] to the integral parts, we can obtain

$$\begin{aligned}
\bar{C}_{A1}^E &= \frac{1}{2 \ln 2} \sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^i B(1, (N_R - 1) i) \\
&\quad \times {}_2F_1 \left((N_R - 2) i, 1; (N_R - 1) i + 1; 1 - \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R - 2)} \right)
\end{aligned} \tag{60}$$

$$\begin{aligned}
\bar{C}_{A2}^E &= \frac{1}{2 \ln 2} \sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^i B(1, (N_R - 1) i) \\
&\quad \times {}_2F_1 \left((N_R - 2) i, 1; (N_R - 1) i + 1; 1 - \frac{2(1 - \phi)}{\phi (N_R - 2)} \right)
\end{aligned} \tag{61}$$

$$\begin{aligned}
\bar{C}_{B1}^E &= \frac{1}{2 \ln 2} \sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^i B(1, (N_R - 2) i) \\
&\quad \times {}_2F_1 \left((N_R - 2) i, 1; (N_R - 2) i + 1; 1 - \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R - 2)} \right)
\end{aligned} \tag{62}$$

$$\begin{aligned}
\bar{C}_{B2}^E &= \frac{1}{2 \ln 2} \sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^i B(1, (N_R - 2) i) \\
&\quad \times {}_2F_1 \left((N_R - 2) i, 1; (N_R - 2) i + 1; 1 - \frac{2(1 - \phi)}{\phi (N_R - 2)} \right)
\end{aligned} \tag{63}$$

where $B(x, y)$ is the Beta function [52, Sect. 8.38], and ${}_2F_1(\alpha, \beta; \gamma; z)$ is the Gauss hypergeometric function and its transformation formulas can be referred to [52, Sect. 9.10-9.13]. **With the results for the legitimate users in (39)–(42) and for the non-colluding eavesdroppers in (60)–(63), the ergodic secrecy rate of each data symbol can be finally obtained via (33).**

B. Colluding Case

Next, we study the case under multiple colluding eavesdroppers, where $N_R \geq N_E + 2$ to guarantee secure communications [30]. By extending the signal model of single-eavesdropper in (19) and (30) to the noiseless case with multiple colluding eavesdroppers, we have

$$\mathbf{y}_E^{(1)} = \mathbf{h}_{AE}\sqrt{\alpha P_A} s_{A1} + \mathbf{h}_{BE}\sqrt{\alpha P_B} s_{B1} + \mathbf{H}_{RE}^T \mathbf{W}_E \sqrt{\frac{P_R}{N_R - 2}} \mathbf{v}^{(1)} \quad (64)$$

$$\mathbf{y}_E^{(2)} = \mathbf{H}_{RE}^T \mathbf{w}_B \sqrt{\frac{\phi P_R}{2}} s_{A2} + \mathbf{H}_{RE}^T \mathbf{w}_A \sqrt{\frac{\phi P_R}{2}} s_{B2} + \mathbf{H}_{RE}^T \mathbf{W}_E \sqrt{\frac{(1-\phi) P_R}{N_R - 2}} \mathbf{v}^{(2)} \quad (65)$$

where $\mathbf{y}_E^{(\tau)} = [y_{E1}^{(\tau)} y_{E2}^{(\tau)} \cdots y_{E_{N_T}}^{(\tau)}]$ with $\tau = 1, 2$ representing the two phases, and \mathbf{h}_{AE} , \mathbf{h}_{BE} and \mathbf{H}_{RE} denote the channels from Users A and B and the relay to the multiple eavesdroppers, respectively. For notational simplicity, we denote $\mathbf{g}_A = \mathbf{H}_{RE}^T \mathbf{w}_A$, $\mathbf{g}_B = \mathbf{H}_{RE}^T \mathbf{w}_B$ and $\mathbf{G}_E = \mathbf{H}_{RE}^T \mathbf{W}_E$ in (65). Based on (65), the ergodic rate of s_{A2} at the eavesdroppers is given by

$$\begin{aligned} \bar{C}_{A2}^E &= \mathbb{E}_{\mathbf{g}_A, \mathbf{g}_B, \mathbf{G}_E} \left\{ \frac{1}{2} \log_2 \left| \mathbf{I} + \frac{\phi P_R}{2} \mathbf{g}_B \mathbf{g}_B^H \left(\frac{\phi P_R}{2} \mathbf{g}_A \mathbf{g}_A^H + \frac{(1-\phi) P_R}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \right| \right\} \\ &= \frac{1}{2 \ln 2} \mathbb{E}_{\mathbf{g}_A, \mathbf{g}_B, \mathbf{G}_E} \left\{ \ln \left(1 + \frac{\phi}{2} \mathbf{g}_B^H \left(\frac{\phi}{2} \mathbf{g}_A \mathbf{g}_A^H + \frac{(1-\phi)}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{g}_B \right) \right\}. \end{aligned} \quad (66)$$

Following the similar transformation, the ergodic rates of the other symbols at the eavesdroppers can be expressed as

$$\bar{C}_{B2}^E = \frac{1}{2 \ln 2} \mathbb{E}_{\mathbf{g}_A, \mathbf{G}_E} \left\{ \ln \left(1 + \frac{\phi}{2} \mathbf{g}_A^H \left(\frac{(1-\phi)}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{g}_A \right) \right\} \quad (67)$$

$$\bar{C}_{A1}^E = \frac{1}{2 \ln 2} \mathbb{E}_{\mathbf{h}_{AE}, \mathbf{h}_{BE}, \mathbf{G}_E} \left\{ \ln \left(1 + \alpha P_A \mathbf{h}_{AE}^H \left(\alpha P_B \mathbf{h}_{BE} \mathbf{h}_{BE}^H + \frac{P_R}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{h}_{AE} \right) \right\} \quad (68)$$

$$\bar{C}_{B1}^E = \frac{1}{2 \ln 2} \mathbb{E}_{\mathbf{h}_{BE}, \mathbf{G}_E} \left\{ \ln \left(1 + \alpha P_B \mathbf{h}_{BE}^H \left(\frac{P_R}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{h}_{BE} \right) \right\}. \quad (69)$$

For the channel related to the eavesdroppers, we assume that the entries in \mathbf{h}_{AE} , \mathbf{h}_{BE} and \mathbf{H}_{RE} are i.i.d zero-mean complex Gaussian variables with variances β_{AE} , β_{BE} and β_{RE} , respectively. Moreover, due to the unitarity of $\mathbf{W} = [\mathbf{w}_A \ \mathbf{w}_B \ \mathbf{W}_E]$, the entries of $\mathbf{H}_{RE}^T \mathbf{W} = [\mathbf{g}_A \ \mathbf{g}_B \ \mathbf{G}_E]$ are also the i.i.d. complex Gaussian variables with variance β_{RE} . Therefore, \mathbf{h}_{AE} , \mathbf{h}_{BE} , \mathbf{g}_A , \mathbf{g}_B and \mathbf{G}_E are independent of each other. As a result, $\eta_{A2}^E = \frac{\phi}{2} \mathbf{g}_B^H \left(\frac{\phi}{2} \mathbf{g}_A \mathbf{g}_A^H + \frac{(1-\phi)}{N_R - 2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{g}_B$ can be regarded as the SINR of an N_E -branch MMSE linear diversity combiner operating in a Rayleigh-fading channel with $(N_R - 1)$ interferers [56]. Then, the CCDF of η_{A2}^E is given by

$$\bar{F}_{\eta_{A2}^E} = \sum_{i=0}^{N_E-1} \Phi_i \left(\frac{2(1-\phi)}{\phi(N_R-2)} x \right)^i \left(1 + \frac{2(1-\phi)}{\phi(N_R-2)} x \right)^{2-N_R} (x+1)^{-1} \quad (70)$$

where $\Phi_i = \binom{N_R-2}{i} + \binom{N_R-2}{i-1}$ for $i = 1, \dots, N_E - 1$ and $\Phi_0 = 1$. Similarly, by defining $\eta_{B2}^E = \frac{\phi}{2} \mathbf{g}_A^H \left(\frac{(1-\phi)}{N_R-2} \mathbf{G}_E^H \mathbf{G}_E \right)^{-1} \mathbf{g}_A$, $\eta_{A1}^E = \alpha P_A \mathbf{h}_{AE}^H \left(\alpha P_B \mathbf{h}_{BE} \mathbf{h}_{BE}^H + \frac{P_R}{N_R-2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{h}_{AE}$, and $\eta_{B1}^E = \alpha P_B \mathbf{h}_{BE}^H \left(\frac{P_R}{N_R-2} \mathbf{G}_E \mathbf{G}_E^H \right)^{-1} \mathbf{h}_{BE}$, their CCDFs can be written as

$$\bar{F}_{\eta_{B2}^E} = \sum_{i=0}^{N_E-1} \binom{N_R-2}{i} \left(\frac{2(1-\phi)}{\phi(N_R-2)} x \right)^i \left(1 + \frac{2(1-\phi)}{\phi(N_R-2)} x \right)^{2-N_R} \quad (71)$$

$$F_{\eta_{A1}^E} = \sum_{i=0}^{N_E-1} \Phi_i \left(\frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R-2)} x \right)^i \left(1 + \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R-2)} x \right)^{2-N_R} (x+1)^{-1} \quad (72)$$

$$\bar{F}_{\eta_{B1}^E} = \sum_{i=0}^{N_E-1} \binom{N_R-2}{i} \left(\frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R-2)} x \right)^i \left(1 + \frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R-2)} x \right)^{2-N_R}. \quad (73)$$

The ergodic rate of each data symbol in (66)–(69) at the colluding eavesdroppers can be further written as

$$\bar{C}_\delta^E = \frac{1}{2 \ln 2} \int_0^\infty (1+x) f_{\eta_\delta^E}(x) dx = \frac{1}{2 \ln 2} \int_0^\infty \frac{\bar{F}_{\eta_\delta^E}(x)}{1+x} dx \quad (74)$$

where $\delta \in \{A1, A2, B1, B2\}$. By substituting (70)–(73) into (74) and invoking [52, Eq. (3.197.5)] to the integral parts, we can obtain

$$\begin{aligned} \bar{C}_{A1}^E &= \frac{1}{2 \ln 2} \Phi_i \left(\frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R-2)} \right)^i B(i+1, N_R-i-1) \\ &\quad \times {}_2F_1 \left(N_R-2, i+1; N_R; 1 - \frac{P_R \beta_{RE}}{\alpha P_A \beta_{AE} (N_R-2)} \right) \end{aligned} \quad (75)$$

$$\begin{aligned} \bar{C}_{A2}^E &= \frac{1}{2 \ln 2} \Phi_i \left(\frac{2(1-\phi)}{\phi(N_R-2)} \right)^i B(i+1, N_R-i-1) \\ &\quad \times {}_2F_1 \left(N_R-2, i+1; N_R; 1 - \frac{2(1-\phi)}{\phi(N_R-2)} \right) \end{aligned} \quad (76)$$

$$\begin{aligned} \bar{C}_{B1}^E &= \frac{1}{2 \ln 2} \sum_{i=0}^{N_E-1} \binom{N_R-2}{i} \left(\frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R-2)} \right)^i B(i+1, N_R-i) \\ &\quad \times {}_2F_1 \left(N_R-2, i+1; N_R-1; 1 - \frac{P_R \beta_{RE}}{\alpha P_B \beta_{BE} (N_R-2)} \right) \end{aligned} \quad (77)$$

$$\begin{aligned} \bar{C}_{B2}^E &= \frac{1}{2 \ln 2} \sum_{i=0}^{N_E-1} \binom{N_R-2}{i} \left(\frac{2(1-\phi)}{\phi(N_R-2)} \right)^i B(i+1, N_R-i) \\ &\quad \times {}_2F_1 \left(N_R-2, i+1; N_R-1; 1 - \frac{2(1-\phi)}{\phi(N_R-2)} \right). \end{aligned} \quad (78)$$

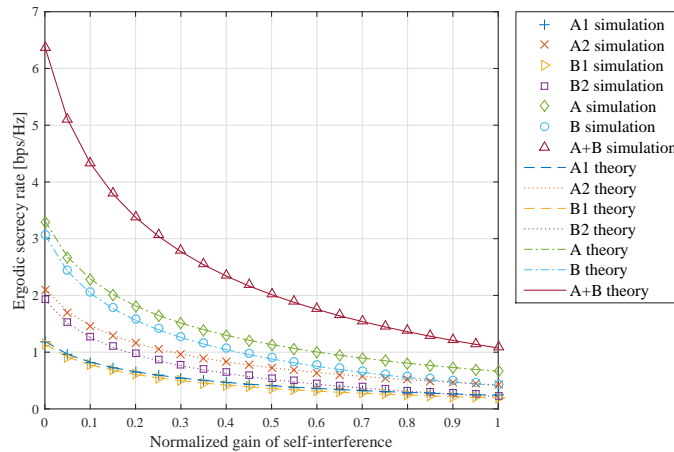


Fig. 2. Ergodic secrecy rate vs. normalized gain of self-interference $\bar{\beta}$ when $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\phi = 0.5$, and SNR = 15 dB.

With the results for the legitimate users in (39)–(42) and for the colluding eavesdroppers in (75)–(78), we can obtain the ergodic secrecy rate of each data symbol via (33) for the network under multiple colluding eavesdroppers.

V. RESULTS AND ANALYSIS

In this section, we evaluate the performance of our proposed secure NOMA-based two-way relay network in terms of ergodic secrecy rate. In the simulations, we assume two legitimate users and the relay transmit with identical power, i.e., $P_A = P_B = P_R = P$ and the noise variance is identical at all nodes, i.e., $\sigma_A^2 = \sigma_B^2 = \sigma_R^2 = \sigma_E^2 = \sigma^2$. It is also assumed that the normalized gain of residual interference introduced by the full-duplex mode is identical at each legitimate user and the relay, i.e., $\beta_{AA} = \beta_{BB} = \beta_{RR} = \bar{\beta}$, where $0 \leq \bar{\beta} \leq 1$ [57]. The transmit SNR is defined as P/σ^2 . As the links related to the relay are usually stronger than the links between users, we set $\beta_{AR} = \beta_{BR} = \beta_{RA} = \beta_{RB} = \beta_{RE} = 10$ and $\beta_{AB} = \beta_{BA} = \beta_{AE} = \beta_{BE} = 1$ in the simulations. In the following figures, we use A1, A2, B1, B2, A, B, and A + B to represent the ergodic secrecy rates of four data symbols s_{A1} , s_{A2} , s_{B1} , and s_{B2} , Users A and B, and the total network, respectively.

Fig. 2 shows the ergodic secrecy rates of different data symbols with respect to the normalized gain of self-interference $\bar{\beta}$, when $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\phi = 0.5$, and SNR = 15 dB. Notably, Fig. 2 and the following figures demonstrate that the theoretical analysis of the ergodic

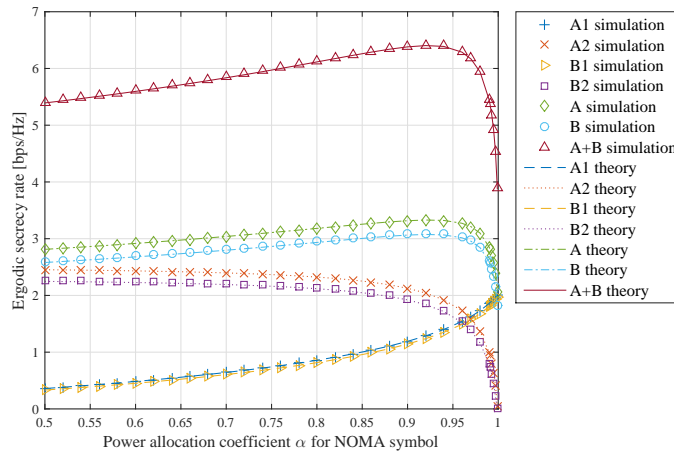


Fig. 3. Ergodic secrecy rate vs. power ratio α of NOMA symbols in (1) and (2) when $N_R = 3$, $N_E = 1$, $\phi = 0.5$, $\bar{\beta} = 0$, and SNR = 15 dB.

secrecy rates in Sections III and IV is in perfect agreement with the simulation results. As seen from Fig. 2, the ergodic secrecy rate of each data symbol decreases as the normalized gain of self-interference $\bar{\beta}$ increases. **This can be well understood since the strong self-interference has a negative effect on the decoding performance of the relay as well as the legitimate users during the first phase.** However, even when the normalized gain of self-interference $\bar{\beta}$ is as high as 1, we can still obtain the positive results for all the ergodic secrecy rates, which implies that secure information exchange can always be guaranteed in our proposed network.

In Fig. 3, we show the ergodic secrecy rates of different data symbols with respect to the power ratio α of NOMA symbols in (1) and (2), where $N_R = 3$, $N_E = 1$, $\phi = 0.5$, $\bar{\beta} = 0$, and SNR = 15 dB. As seen from the figure, with the increase of the power ratio α of NOMA symbols, the ergodic secrecy rates of data symbols s_{A1} and s_{B1} increase while those of data symbols s_{A2} and s_{B2} decrease. On the other hand, Fig. 3 indicates that there exists an optimal value of α that maximizes the ergodic secrecy rates of Users A and B and the ergodic sum secrecy rate.

Fig. 4 shows the ergodic secrecy rates of different data symbols with respect to power allocation coefficient ϕ for the artificial noise scheme in (14), where $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\bar{\beta} = 0.1$, and SNR = 15 dB. From the figure, we observe that an optimal value of ϕ exists to maximize the ergodic secrecy rates of data symbols s_{A2} and s_{B2} while the ergodic secrecy rates of data symbols s_{A1} and s_{B1} keep constant regardless of ϕ . Such phenomenon can be explained by the

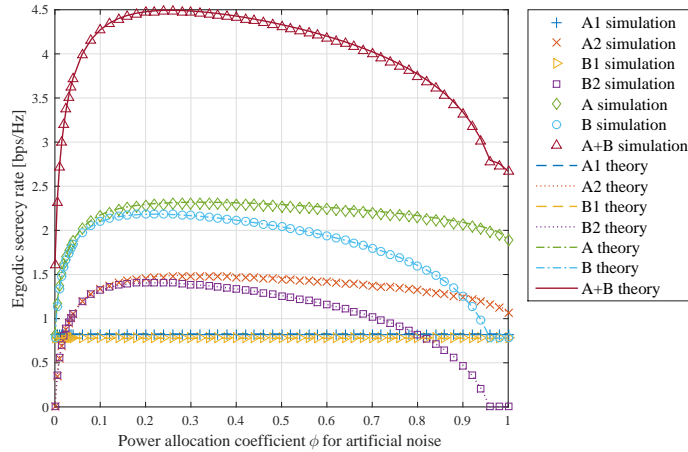


Fig. 4. Ergodic secrecy rate vs. power allocation coefficient ϕ for the artificial noise scheme in (14) when $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\bar{\beta} = 0.1$, and SNR = 15 dB.

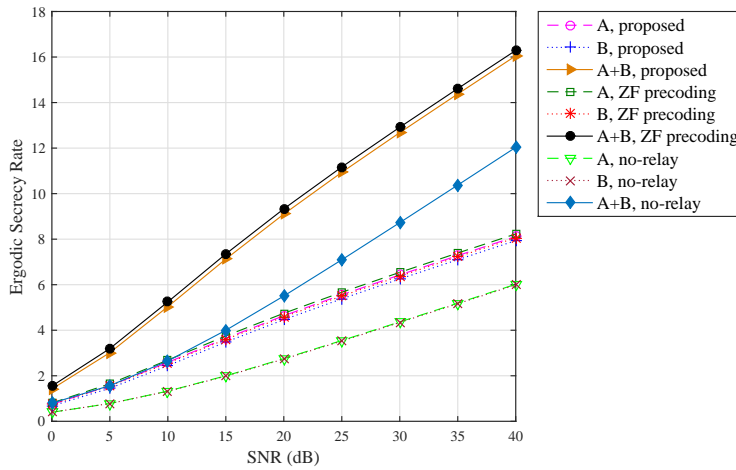


Fig. 5. Ergodic secrecy rates of different relay schemes vs. the transmit SNR when $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\bar{\beta} = 0$, and $\phi = 0.3$.

fact that the artificial noise scheme in (14) only contains data symbols s_{A2} and s_{B2} . Specially, when $\phi = 0$, the relay only broadcasts the pure jamming signals and data symbols s_{A2} and s_{B2} cannot be decoded in the second phase based on (26) and (27). When $\phi = 1$, the relay only forwards the data symbols s_{A2} and s_{B2} and no protection is afforded, which fails to guarantee the secure transmission of s_{B2} . As can be seen, by choosing a proper ϕ , the network performance in terms of ergodic secrecy rate can be significantly improved.

In Fig. 5, we compare the ergodic secrecy rates of different relay schemes with respect to

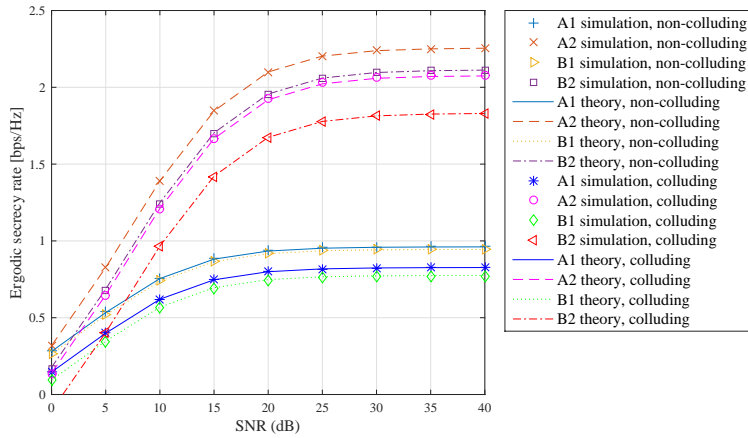


Fig. 6. Ergodic secrecy rates under non-colluding and colluding manners vs. the transmit SNR when $N_R = 5$, $N_E = 2$, $\alpha = 0.9$, $\phi = 0.5$, and $\bar{\beta} = 0.1$.

the transmit SNR, where $N_R = 3$, $N_E = 1$, $\alpha = 0.9$, $\bar{\beta} = 0$, and $\phi = 0.3$. As can be seen, by using the ZF precoding to replace the range space \mathbf{W}_U at the relay, the network only achieves a secrecy performance that is marginally better than that of using the range space \mathbf{W}_U in (3). Therefore, for simplicity, we mainly focus on the performance analysis of our proposed scheme. On the other hand, the proposed two-way network achieves a significant performance gain over the network without a relay, which corroborates the important role of the relay for security enhancements.

In Fig. 6, we compare the network performance under multiple eavesdroppers with the non-colluding and colluding manners with respect to the transmit SNR, where $N_R = 5$, $N_E = 2$, $\alpha = 0.9$, $\phi = 0.5$, and $\bar{\beta} = 0.1$. As can be observed, the network performance under the colluding eavesdroppers is worse than that under the non-colluding eavesdroppers. It can be well understood since by jointly processing the received signals at multiple eavesdroppers, colluding manner can wiretap more information than the non-colluding one, leading to worse secure performance for the proposed network.

Fig. 7 shows the ergodic secrecy rates of different data symbols with respect to the number of eavesdroppers N_E , where $N_R = 12$, $\alpha = 0.9$, $\phi = 0.5$, $\bar{\beta} = 0.1$, and SNR = 30 dB. Considering multiple eavesdroppers with colluding manner, we observe that the ergodic secrecy rates of different data symbols decrease as the number of eavesdroppers N_E increases. This adverse effect is caused by the improvement of the eavesdropping ability with the increasing number of

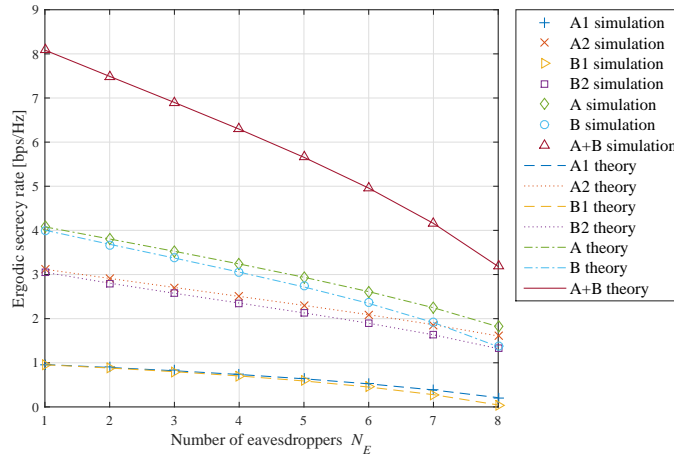


Fig. 7. Ergodic secrecy rate vs. number of eavesdroppers N_E when $N_R = 12$, $\alpha = 0.9$, $\phi = 0.5$, $\bar{\beta} = 0.1$, and SNR = 30 dB.

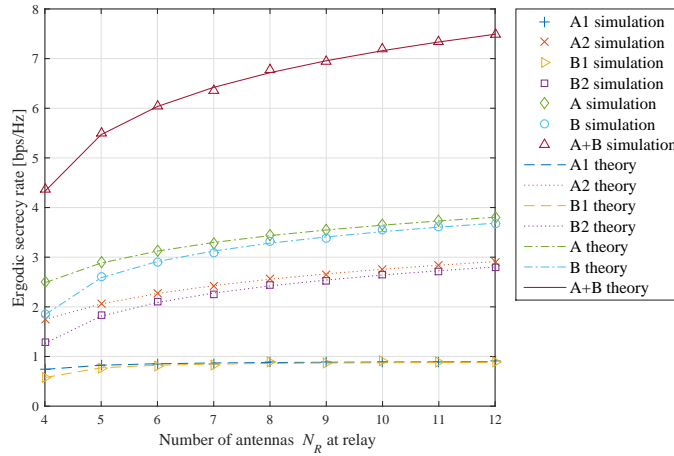


Fig. 8. Ergodic secrecy rate vs. number of antennas N_R at the relay when $N_E = 2$, $\alpha = 0.9$, $\phi = 0.5$, $\bar{\beta} = 0.1$, and SNR = 30 dB.

eavesdroppers.

In Fig. 8, we show the ergodic secrecy rates of different data symbols with respect to the number of antennas N_R at the relay, where $N_E = 2$, $\alpha = 0.9$, $\phi = 0.5$, $\bar{\beta} = 0.1$, and SNR = 30 dB. As can be seen, the ergodic secrecy rates of different data symbols increase as the number of antennas N_R increases at the relay. However, the performance improvement of data symbols s_{A1} and s_{B1} is marginal when increasing the number of antennas N_R at the relay beyond $N_R = 5$. It should be noted that the decoding of both data symbols s_{A1} and s_{B1} in (20)–(21) and (24)–(25) is associated with the user-to-relay link and the user-to-user link, respectively.

Since the user-to-user link is much weaker and the decoding performance of data symbols s_{A1} and s_{B1} is almost limited by it, increasing the number of antennas N_R at the relay does not improve the user-to-user link as well as their decoding performance. On the other hand, we observe significant performance improvement of data symbols s_{A2} and s_{B2} as the number of antennas N_R increases at the relay, which is attributed to the reliable enhancement of the links between the relay and the users.

VI. CONCLUSIONS

In this paper, a novel secure NOMA-based two-way relay network has been proposed with the considerations of different eavesdropping cases. Specifically, by employing the full-duplex and the artificial noise techniques at the relay, we have enhanced the ability of the relay to combat the eavesdropping without impairing the legitimate users for ensuring secure information exchange. On the other hand, with the full-duplex mode applied to the user nodes in the first phase, we have improved the data transmission efficiency without requiring any extra bandwidth resource. Moreover, we have designed different decoding strategies based on SIC for different types of nodes, in which we have provided the eavesdroppers with a sophisticated strategy with jointly processing to examine the secure performance of the proposed network in the harsh wiretap condition. Finally, we have analyzed the performance of the secure NOMA-based two-way relay network and derived the closed-form expressions for the ergodic secrecy rates under single eavesdropper, multiple non-colluding, and colluding eavesdroppers. The theoretical derivations have been shown to agree with the simulation results perfectly. **Our future concerns will be the enhancement design of secure NOMA-based networks and the optimization problems on the power allocations for the NOMA symbols and the artificial noise scheme in the proposed network.**

APPENDIX A

PROOF OF PROPOSITION 1

Letting $\eta_{A1} = \min \left\{ \frac{\beta_{AR}\rho_A}{P_R\beta_{RR} + \sigma_R^2}, \frac{|h_{AB}|^2}{P_B\beta_{BB} + \sigma_B^2} \right\}$ in (34), and using the CCDF of ρ_A in (9) and the CCDF of $|h_{AB}|^2$ as $\bar{F}_{|h_{AB}|^2}(x) = \exp\left(-\frac{x}{\beta_{AB}}\right)$, we can obtain the CCDF of η_{A1} as

$$\bar{F}_{\eta_{A1}}(x) = \Pr \{ \eta_{A1} > x \} = \Pr \left\{ \frac{\beta_{AR}\rho_A}{P_R\beta_{RR} + \sigma_R^2} > x, \frac{|h_{AB}|^2}{P_B\beta_{BB} + \sigma_B^2} > x \right\}$$

$$\begin{aligned}
&= \bar{F}_{\rho_A} \left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} x \right) \bar{F}_{|h_{AB}|^2} \left((P_B \beta_{BB} + \sigma_B^2) x \right) \\
&= \exp \left(- \left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}} \right) x \right) \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} x \right)^k}{k!}. \tag{79}
\end{aligned}$$

With (79), the ergodic rate of s_{A1} can be derived as

$$\begin{aligned}
\bar{C}_{A1} &= \int_0^\infty \frac{1}{2} (\log_2(1 + P_A x) - \log_2(1 + (1 - \alpha) P_A x)) f_{\eta_{A1}}(x) dx \\
&= \frac{1}{2 \ln 2} \left(\int_0^\infty \ln(1 + P_A x) f_{\eta_{A1}}(x) dx - \int_0^\infty \ln(1 + (1 - \alpha) P_A x) f_{\eta_{A1}}(x) dx \right) \\
&= \frac{1}{2 \ln 2} \left(P_A \int_0^\infty \frac{\bar{F}_{\eta_{A1}}(x)}{1 + P_A x} dx - (1 - \alpha) P_A \int_0^\infty \frac{\bar{F}_{\eta_{A1}}(x)}{1 + (1 - \alpha) P_A x} dx \right) \\
&= \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} \right)^k}{k!} \left(\int_0^\infty \frac{\exp \left(- \left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}} \right) x \right) x^k}{\frac{1}{P_A} + x} dx \right. \\
&\quad \left. - \int_0^\infty \frac{\exp \left(- \left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}} \right) x \right) x^k}{\frac{1}{(1 - \alpha) P_A} + x} dx \right). \tag{80}
\end{aligned}$$

By applying [52, Eq. (3.353.5)] to the integral parts in (80), we finally obtain (39).

APPENDIX B

PROOF OF PROPOSITION 2

Let $\eta_{A2} = \min \left\{ \frac{(1 - \alpha) P_A \beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2}, \frac{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2 \phi P_R}{2\sigma_B^2} \right\}$ in (36). As \mathbf{w}_B is one column of the orthonormal basis \mathbf{W} , it can be readily verified that $\mathbf{h}_{RB}^T \mathbf{w}_B$ follows the zero-mean complex Gaussian distribution with variance β_{RB} and we have the CCDF of $|\mathbf{h}_{RB}^T \mathbf{w}_B|^2$ as $\bar{F}_{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2}(x) = \exp \left(-\frac{x}{\beta_{RB}} \right)$. With the CCDF of ρ_A given in (9), we can obtain the CCDF of η_{A2} as

$$\begin{aligned}
\bar{F}_{\eta_{A2}}(x) &= \Pr \{ \eta_{A2} > x \} = \Pr \left\{ \frac{(1 - \alpha) P_A \beta_{AR} \rho_A}{P_R \beta_{RR} + \sigma_R^2} > x, \frac{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2 \phi P_R}{2\sigma_B^2} > x \right\} \\
&= \bar{F}_{\rho_A} \left(\frac{P_R \beta_{RR} + \sigma_R^2}{(1 - \alpha) P_A \beta_{AR}} x \right) \bar{F}_{|\mathbf{h}_{RB}^T \mathbf{w}_B|^2} \left(\frac{2\sigma_B^2}{\phi P_R} x \right) \\
&= \exp \left(- \left(\frac{P_R \beta_{RR} + \sigma_R^2}{(1 - \alpha) P_A \beta_{AR}} + \frac{2\sigma_B^2}{\phi P_R \beta_{RB}} \right) x \right) \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{(1 - \alpha) P_A \beta_{AR}} x \right)^k}{k!}. \tag{81}
\end{aligned}$$

With (81), the ergodic rate of s_{A2} can be written as

$$\bar{C}_{A2} = \int_0^\infty \frac{1}{2} \log_2(1+x) f_{\eta_{A2}}(x) dx = \frac{1}{2 \ln 2} \int_0^\infty \frac{\bar{F}_{\eta_{A2}}(x)}{1+x} dx. \quad (82)$$

As (81) has a similar form to (79), after substituting (81) into (82) and applying [52, Eq. (3.353.5)] to the integral part, we can finally obtain (41).

APPENDIX C

PROOF OF PROPOSITION 3

Let us denote $\mathbf{g}^T = [g_A \ g_B \ \mathbf{g}_E^T]^T = \mathbf{h}_{RE}^T \mathbf{W}$. We can obtain $\mathbf{g} \sim \mathcal{N}_c(\mathbf{0}_{N_R \times 1}, \beta_{RE} \mathbf{I}_{N_R})$, which has i.i.d. complex Gaussian entries as \mathbf{W} is a unitary matrix. By denoting $v_A = \frac{|g_A|^2}{\beta_{RE}} = \frac{|\mathbf{h}_{RE}^T \mathbf{w}_A|^2}{\beta_{RE}}$, $v_B = \frac{|g_B|^2}{\beta_{RE}} = \frac{|\mathbf{h}_{RE}^T \mathbf{w}_B|^2}{\beta_{RE}}$, and $v_E = \frac{\|\mathbf{g}_E\|^2}{\beta_{RE}} = \frac{\|\mathbf{h}_{RE}^T \mathbf{W}_E\|^2}{\beta_{RE}}$, we have $v_A \sim \exp(1)$, $v_B \sim \exp(1)$, and $v_E \sim \Gamma(N_R - 2, 1)$, where $\Gamma(\alpha, x)$ is the upper incomplete gamma function [52, Eq. (8.350.2)].

Then, we can derive the CCDF of γ_{A2}^E in (28) as

$$\begin{aligned} \bar{F}_{\gamma_{A2}^E} &= \Pr \left\{ \frac{\phi(N_R - 2) |\mathbf{h}_{RE}^T \mathbf{w}_A|^2}{\phi(N_R - 2) |\mathbf{h}_{RE}^T \mathbf{w}_B|^2 + 2(1 - \phi) \|\mathbf{h}_{RE}^T \mathbf{W}_E\|^2 + \frac{2(N_R - 2)\sigma_E^2}{P_R}} > x \right\} \\ &= \Pr \left\{ \frac{\phi(N_R - 2) v_A}{\phi(N_R - 2) v_B + 2(1 - \phi) v_E + \frac{2(N_R - 2)\sigma_E^2}{P_R \beta_{RE}}} > x \right\} \\ &= \Pr \left\{ v_A > \left(v_B + \frac{2(1 - \phi) v_E}{\phi(N_R - 2)} + \frac{2\sigma_E^2}{\phi P_R \beta_{RE}} \right) x \right\} \\ &= \mathbb{E}_{v_E, v_B} \left[\exp \left(- \left(v_B + \frac{2(1 - \phi) v_E}{\phi(N_R - 2)} + \frac{2\sigma_E^2}{\phi P_R \beta_{RE}} \right) x \right) \right] \\ &= \int_0^\infty \int_0^\infty \exp \left(- \left(v_B + \frac{2(1 - \phi) v_E}{\phi(N_R - 2)} + \frac{2\sigma_E^2}{\phi P_R \beta_{RE}} \right) x \right) (v_E)^{N_R - 3} \frac{\exp(-v_E)}{(N_R - 3)!} \exp(-v_B) dv_E dv_B \\ &= \exp \left(- \frac{2\sigma_E^2}{\phi P_R \beta_{RE}} x \right) \left(1 + \frac{2(1 - \phi)}{\phi(N_R - 2)} x \right)^{2 - N_R} (x + 1)^{-1} \end{aligned} \quad (83)$$

where the double integral is solved by using the formulas [52, Eq. (3.381.3)] and [52, Eq. (3.310)]. With (83), the ergodic rate of s_{A2} at the eavesdropper can be derived as

$$\bar{C}_{A2}^E = \frac{1}{2 \ln 2} \int_0^\infty \frac{\bar{F}_{\gamma_{A2}^E}(x)}{1+x} dx = \frac{1}{2 \ln 2} \int_0^\infty \frac{\exp \left(- \frac{2\sigma_E^2}{\phi P_R \beta_{RE}} x \right)}{\left(1 + \frac{2(1 - \phi)}{\phi(N_R - 2)} x \right)^{N_R - 2} (x + 1)^2} dx$$

$$= \frac{1}{2 \ln 2} \left(\sum_{i=1}^{N_R-2} \int_0^\infty \frac{\Omega_{A2}^i \exp\left(-\frac{2\sigma_E^2}{\phi P_R \beta_{RE}} x\right)}{\left(x + \frac{\phi(N_R-2)}{2(1-\phi)}\right)^i} dx + \sum_{i=1}^2 \int_0^\infty \frac{\Psi_{A2}^i \exp\left(-\frac{2\sigma_E^2}{\phi P_R \beta_{RE}} x\right)}{(x+1)^i} dx \right) \quad (84)$$

where (84) is obtained by using the partial-fraction expansion [53, appendix], and Ω_{A2}^i and Ψ_{A2}^i are given in (46) and (47), respectively. By applying [52, Eq. (3.353.2)] to the integral parts in (84), we finally obtain (45).

REFERENCES

- [1] 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.
- [2] F. Zhou, Y. Wu, R. Q. Hu, Y. Wang, and K. K. Wong, "Energy-efficient NOMA enabled heterogeneous cloud radio access networks," *IEEE Network*, to be published.
- [3] 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.
- [4] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE VTC'13 Spring*, Dresden, Germany, Jun. 2013, pp. 1–5.
- [5] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *Proc. IEEE PIMRC'13*, London, U.K., Sept. 2013, pp. 611–615.
- [6] M. Al-Imari, P. Xiao, M. A. Imran, and R. Tafazolli, "Uplink non-orthogonal multiple access for 5G wireless networks," in *Proc. IEEE ISWCS'14*, Barcelona, Spain, Aug. 2014, pp. 781–785.
- [7] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.
- [8] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.
- [9] J. Choi, "Minimum power multicast beamforming with superposition coding for multiresolution broadcast and application to NOMA systems," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 791–800, Mar. 2015.
- [10] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Trans. Signal Process.*, vol. 64, no. 1, pp. 76–88, Jan. 2016.
- [11] Z. Ding, F. Adachi, and H. V. Poor, "The application of MIMO to non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 537–552, Jan. 2016.
- [12] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.
- [13] Y. Liu, Z. Ding, M. Elkashlan, and J. Yuan, "Non-orthogonal multiple access in large-scale underlay cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10 152–10 157, Dec. 2016.
- [14] L. Lv, J. Chen, Q. Ni, and Z. Ding, "Design of cooperative non-orthogonal multicast cognitive multiple access for 5G systems: User scheduling and performance analysis," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2641–2656, Jun. 2017.
- [15] X. Liang, Y. Wu, D. W. K. Ng, Y. Zuo, S. Jin, and H. Zhu, "Outage performance for cooperative NOMA transmission with an AF relay," *IEEE Commun. Lett.*, in press.

- [16] 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.
- [17] 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.
- [18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [19] Y. Wu, J. B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, in press.
- [20] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.
- [21] A. Khina, Y. Kochman, and A. Khisti, "The MIMO wiretap channel decomposed," *IEEE Trans. Inf. Theory*, in press.
- [22] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT'07*, Nice, France, Jun. 2007, pp. 2466–2470.
- [23] 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.
- [24] —, "Secure transmission with multiple antennas – part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [25] 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.
- [26] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [27] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [28] 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.
- [29] 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.
- [30] 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.
- [31] 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.
- [32] C. Wang, H. M. Wang, and X. G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.
- [33] 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 networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.
- [34] M. Yang, B. Zhang, Y. Huang, N. Yang, D. B. da Costa, and D. Guo, "Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise," *IEEE Trans. Veh. Technol.*, in press.
- [35] H. M. Wang, M. Luo, Q. Yin, and X. G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
- [36] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

- [37] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.
- [38] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "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.
- [39] 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. ICC'16*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
- [40] 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, Jul. 2017.
- [41] 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.*, in press.
- [42] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.
- [43] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO non-orthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, in press.
- [44] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1113–1117, Aug. 2017.
- [45] J. Tang, D. K. C. So, A. Shojaeifard, K. K. Wong, and J. Wen, "Joint antenna selection and spatial switching for energy efficient MIMO SWIPT system," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4754–4769, Jul. 2017.
- [46] Y. Jiang, M. K. Varanasi, and J. Li, "Performance analysis of ZF and MMSE equalizers for MIMO systems: An in-depth study of the high SNR regime," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2008–2026, Apr. 2011.
- [47] T. W. Anderson, T. W. Anderson, T. W. Anderson, T. W. Anderson, and E.-U. Mathématicien, *An introduction to multivariate statistical analysis*. Wiley New York, 1958, vol. 2.
- [48] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y. S. Choi, L. Anttila, S. Talwar, and M. Valkama, "Full-duplex mobile device: pushing the limits," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 80–87, Sept. 2016.
- [49] L. Wang, F. Tian, T. Svensson, D. Feng, M. Song, and S. Li, "Exploiting full duplex for device-to-device communications in heterogeneous networks," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 146–152, May 2015.
- [50] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.
- [51] 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.
- [52] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products (seventh edition)*. Academic press, 2007.
- [53] A. V. Oppenheim, A. Willsky, and S. Nawab, *Signals and systems (second edition)*. New Jersey: Prentice Hall, 1997.
- [54] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, Mar. 2017.
- [55] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.
- [56] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.
- [57] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. IEEE ASILOMAR'11*, Pacific Grove, CA, USA, Nov. 2011, pp. 265–269.

Responses to Editor and Reviewers' Comments

Manuscript ID: IEEE JSAC SI in PLS for 5G #1570397899

Title: Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex

Dear Editors and Reviewers,

We would like to thank you for reviewing our paper. We appreciate your insightful comments and valuable remarks, which helped us to significantly improve the overall technical quality as well as the presentation of this submission. In response to your comments, the paper has substantially been improved. Specifically, in the revised manuscript, the following major changes have been made:

- C1. We have clarified some definitions and the motivation of performing superposition coding.
- C2. In Fig. 5, we have compared our proposed scheme with the ZF precoding and no-relay schemes for the network.
- C3. For (4), we have explained the power normalization factor.
- C4. In Section II, we have clarified our proposed decoding scheme for exploiting channel gain differences between sub-users.
- C5. In Section II.B, we have added some discussions on the effect of decoding order at the eavesdropper.
- C6. We have provided more details for the derivations of (59).
- C7. In Section V, we have discussed the effects of different system parameters on the secrecy performance.

Detailed point-by-point responses are given in the following. With these revisions, we hope the Editor and the anonymous Reviewers will find that the review comments have been sufficiently addressed and the current version is acceptable for publication in *IEEE Journal on Selected Areas in Communications (JSAC)*.

Best regards,
All authors

Responses to Reviewer 1's Comments:

1. It is very confused that whether the proposed scheme is a NOMA technique. In my opinion, it is a special two-way relaying scheme. S_{A1} , S_{A2} , S_{B1} and S_{B2} are not well defined, thus it is unclear why to perform superposition coding at A and B.

Response: In power-domain NOMA systems, a multitude of users share the same radio resource via superposition coding, where different users are distinguished with different power levels and the successive interference cancellation (SIC) is applied to cancel the multi-user interference. For ease of explanation, we take User A as an example. By using the proposed scheme, User A splits itself into two sub-users, say A1 and A2, with the power allocations αP_A and $(1-\alpha)P_A$ respectively. In that way, the receiver (relay or User B) is provided with the freedom to decide which fraction of the interference to decode along with the desired signal, which helps improve the spectral efficiency. Moreover, NOMA generally exploits the channel gain differences between users for multiplexing via power allocation to use spectral resource more efficiently. The decoding of data symbols s_{A1} and s_{A2} is associated with different channels, which exploits the channel gain differences between Sub-users A1 and A2 to achieve better system performance with NOMA proposal. Finally, by adopting superposition coding at Users A and B, the decoding of the eavesdropper not only suffers from the artificial noise but also suffers from the multi-user interference. In summary, the NOMA based two-way relay network can achieve better secrecy performance for two reasons:

- Increasing the legitimate channel rate by adopting NOMA proposal with the leverage of heterogeneous channel condition;
- Decreasing the wiretap channel rate by the full-duplex jamming and the multi-user interference introduced by NOMA proposal.

In the revised manuscript, we have clarified the definition of the data symbols and the motivation of performing superposition coding at Users A and B.

2. It is a too strong assumption that the nodes have perfect CSI in practical systems, especial for the multiple-antenna relay. Please explicitly explain how to obtain perfect CSI. Moreover, why the uplink and downlink channels are reciprocal.

Response: We agree with the Reviewer that in practical systems, it is not possible to obtain the perfect CSI due to the channel estimation error. However, the interference caused by the imperfect CSI may be incorporated in the noise term or the interference term (e.g., multi-user interference and residual interference caused by full duplex) for the simplicity of analysis [ref1].

In our network model, we did not assume that the uplink and downlink channels are reciprocal. For

example, we use \mathbf{h}_{AR} and \mathbf{h}_{RA} to distinguish the uplink and downlink channels of User A, and they are not necessarily equal in our assumption.

[ref1]Z. Yang, Z. Ding, P. Fan and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," in *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 654-667, Feb. 2016.

3. The variances in (7) are independent of the self-interference channel \mathbf{H}_{RR} , which is incorrect. Thus, the theoretical results in the rest might not be exact.

Response: In (5), we denote $\tilde{\mathbf{H}}_{RR}$ as the residual self-interference channel due to the imperfect interference mitigation at the relay node, whose entries are independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with variance β_{RR} . The variances in (7) are shown as

$$\begin{aligned}\bar{\sigma}_A^2 &= (P_R \beta_{RR} + \sigma_R^2) \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{1,1} \\ \bar{\sigma}_B^2 &= (P_R \beta_{RR} + \sigma_R^2) \left[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \right]_{2,2}\end{aligned}$$

As can be seen, both variances $\bar{\sigma}_A^2$ and $\bar{\sigma}_B^2$ depend on the variance of the residual self-interference channel β_{RR} and the transmit power.

4. This paper derives very complicated expressions, but not any insight. It is difficult to know how the system parameters affect the secrecy performance.

Response: Although the expressions are complicated, the effects of some system parameters can still be observed after some simple manipulations and we have tried to provide more insights regarding the impact of some system parameters on the secrecy performance. For example, the ergodic rate of s_{A1} for the legitimate channel in (80) can be further written as

$$\bar{C}_{A1} = \frac{1}{2 \ln 2} \sum_{k=0}^{N_R-2} \frac{\left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} \right)^k}{k!} \int_0^\infty \Upsilon(x) dx$$

where

$$\Upsilon(x) = \frac{\alpha \exp \left(- \left(\frac{P_R \beta_{RR} + \sigma_R^2}{\beta_{AR}} + \frac{P_B \beta_{BB} + \sigma_B^2}{\beta_{AB}} \right) x \right) x^k}{\left(\frac{1}{P_A} + x \right) (1 + (1 - \alpha) P_A x)}.$$

It can be observed that $\Upsilon(x)$ increases as α increases and thus the ergodic rate \bar{C}_{A1} also increases with the increasing value of α . Moreover, since $\Upsilon(x) > 0$ for $x > 0$, it can be readily obtained that \bar{C}_{A1} increases with the increasing number of summation terms, which is associated

with the number of antennas N_R at the relay. The ergodic rate of other data symbols can also be analyzed in a similar way. Unfortunately, due to the interplay of multiple system parameters and the foulness of multiple terms, the effects of some system parameters are not obvious from the derived expressions. Therefore, we resort to extensive simulations to examine the effects of different system parameters on the secrecy performance in the revised manuscript.

Responses to Reviewer 2's Comments:

1. Regarding (15) and (16), why the ZF precoding is not used at the relay node, where the inter-user-interference can be cancelled at the relay nodes, can this scheme achieve the better performance than the proposed one? It should be verified in simulations.

Response: The ZF precoding applied at the relay node requires the feedback of CSI at the transmitter side, which increases the system overhead. On the other hand, for our proposed scheme, since symbol s_{A2} is generated by User A, User A can perform the self-interference cancellation of s_{A2} before decoding its desired signal s_{B2} in (15), and so can User B in (16). As shown in (17) and (18), both Users A and B are free of inter-user-interference. Per your suggestion, in Fig. 5 of the revised manuscript, we have included the ZF precoding scheme at the relay for comparison. Specifically, by using the ZF precoding at the relay during the second phase, \mathbf{W}_U in (15) and (16) is replaced by

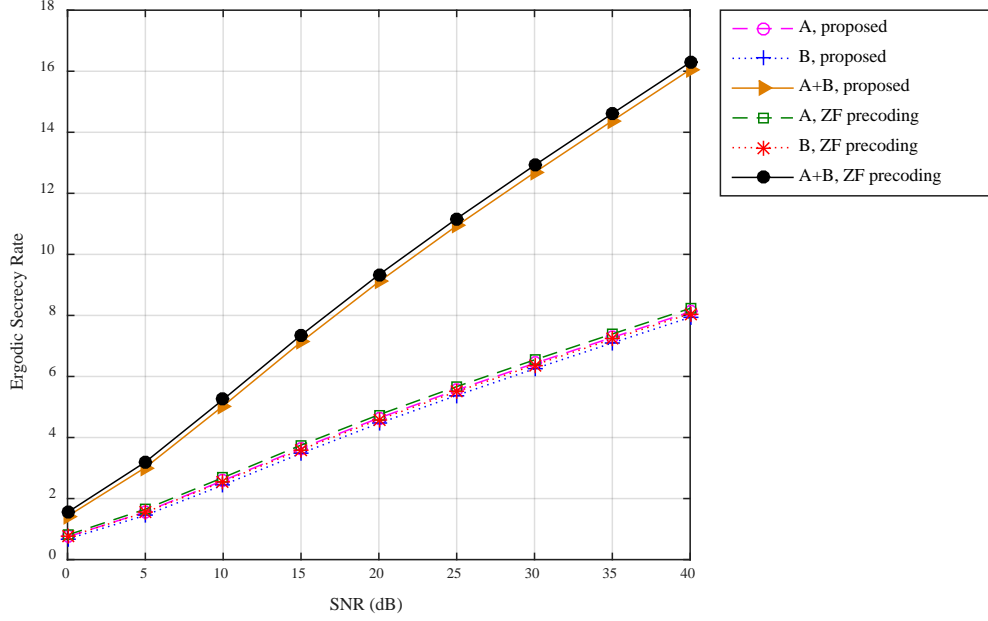
$$\mathbf{W}_U = \mathbf{P}_{ZF} \mathbf{D}$$

where $\mathbf{P}_{ZF} = \mathbf{H}_{RU}^H (\mathbf{H}_{RU} \mathbf{H}_{RU}^H)^{-1}$ denotes the ZF precoder applied at the relay and $\mathbf{D} = \text{diag} \left(\sqrt{1/\|\mathbf{p}_1\|^2}, \sqrt{1/\|\mathbf{p}_2\|^2} \right)$ is a 2×2 diagonal matrix which is used to ensure that the transmitted power is not amplified by the precoder. Here, \mathbf{p}_i is the i -th column of \mathbf{P}_{ZF} with $i = 1, 2$. The signals received at the legitimate user nodes in (15) and (16) are respectively replaced by

$$y_A^{(2)} = \mathbf{h}_{RA}^T \mathbf{x}_R^{(2)} + n_A^{(2)} = \sqrt{\frac{\phi P_R}{2\|\mathbf{p}_1\|^2}} s_{B2} + n_A^{(2)}$$

$$y_B^{(2)} = \mathbf{h}_{RB}^T \mathbf{x}_R^{(2)} + n_B^{(2)} = \sqrt{\frac{\phi P_R}{2\|\mathbf{p}_2\|^2}} s_{A2} + n_B^{(2)}$$

both of which cancel the inter-user-interference via ZF precoding. The comparison results are also shown below for your convenience.



As can be seen from the figure, the ZF precoding scheme only achieves a secrecy performance that is marginally better than that of the proposed one. Therefore, for simplicity, we mainly focus on the performance analysis of our proposed scheme.

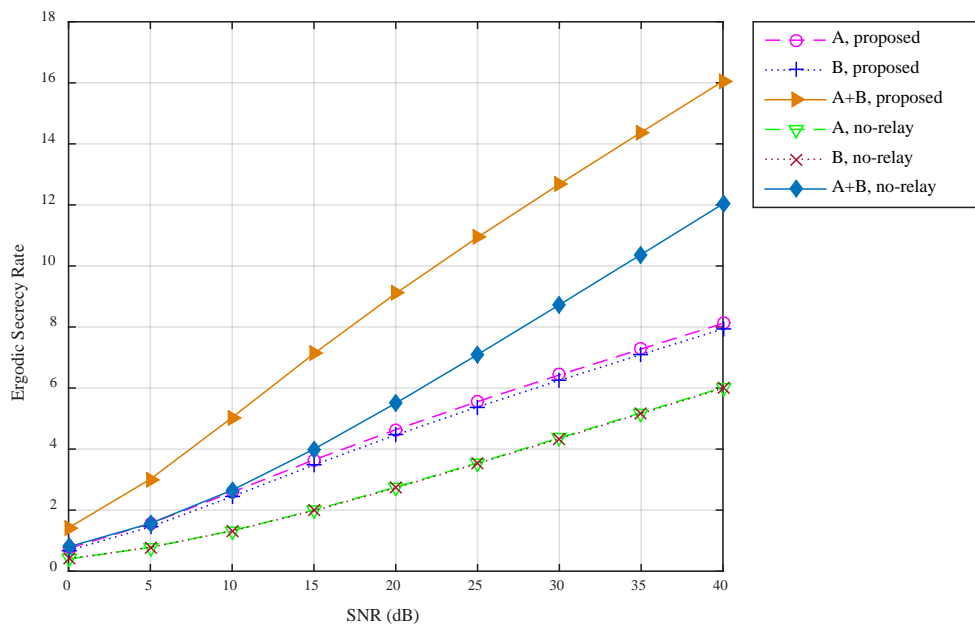
2. One critical problem in the proposed scenario is, this paper considers the two stages. However, the first stages can happen in the first slot, while multiple-access phase + broadcast phase can simultaneously happen in the following multiple slots, thanks to the full duplex. In this way, the eavesdropper can not only receive the Sa1, Sa2, Sb1, Sb2 from the users transmitted in the current slot, and also receives the Sa2 and Sb2 from the relay node (transmitted by the user a and b in the last time slot). Obviously, this process can be more efficient than your one.

Response: We totally agree with the Reviewer that the suggested scheme is much more efficient than our proposed scheme. However, the suggested scheme will introduce more severe interference to the system and higher decoding cost to the receiver. Specifically, during the t -th ($t > 1$) slot of the suggested scheme, the relay transmits the mixture of $s_{A2}(t-1)$ and $s_{B2}(t-1)$, while User A transmits the superposition of $s_{A1}(t)$ and $s_{A2}(t)$ and User B transmits the superposition of $s_{B1}(t)$ and $s_{B2}(t)$. As can be seen, six different data symbols (two former data symbols + four current data symbol) are broadcast simultaneously in the network, which incurs not only multi-user interference but also inter-symbol interference. Meanwhile, due to the severe interference, the receiver requires higher complexity to separate multiple interfered symbols and those interfered symbols may suffer from lower SINRs as well as lower rates. Therefore, we apply two phases to complete one transmission in our proposed scheme to avoid the former symbol interference and reduce the decoding cost at the receiver. Nevertheless, we would like to thank the Reviewer for

bringing us such a good idea to further improve the transmission efficiency and we will consider this direction as our future work.

3. Can the authors compare the scheme without relay, in this way, all the power transmitted by the user a and b can be directly delivered to their destination, and the eavesdropper can only receive the information once.

Response: In Fig. 5 of the revised manuscript, we have included the case without a relay for comparison. The results are also shown below for your convenience.



As can be seen, the performance of the network without a relay is much poorer than that of the proposed network with the aid of relay, which corroborates the importance of the relay for security enhancements. Specifically, the relay plays two important roles in the proposed secure NOMA-based network:

- Increasing the legitimate channel rate by shortening the access distance and coordinating the NOMA transmission;
- Decreasing the wiretap channel rate by the full-duplex jamming without impairing legitimate users.

4. Some variables are not well defined. For example. for (1) and (2), $\{A1\}$, $\{A2\}$, $\{B1\}$, $\{B2\}$ are not well defined. The reviewers can understand them until read (6); Another example is (33), where the variables in the right hand are not well defined.

Response: In the revised manuscript, we have defined the above-mentioned notations.

5. For (4), why the factor is $\sqrt{P_R/(N_R-2)}$, could the authors explain this? I do not understand.

Response: The factor $\sqrt{P_R/(N_R-2)}$ was obtained by considering the average transmit power constraint at the relay. According to (4), as the artificial noise vector $\mathbf{v}^{(1)} \sim \mathcal{N}_c(\mathbf{0}_{(N_R-2) \times 1}, \mathbf{I}_{N_R-2})$ is of dimensions $(N_R-2) \times 1$, the average transmit power P_R can be verified by

$$\begin{aligned} P_R &= \mathbb{E} \left[\|\mathbf{x}_R^{(1)}\|^2 \right] = \mathbb{E} \left[(\mathbf{x}_R^{(1)})^H \mathbf{x}_R^{(1)} \right] = \mathbb{E} \left[(\mathbf{v}^{(1)})^H \sqrt{\frac{P_R}{N_R-2}} \mathbf{W}_E^H \mathbf{W}_E \sqrt{\frac{P_R}{N_R-2}} \mathbf{v}^{(1)} \right] \\ &= \frac{P_R}{N_R-2} \mathbb{E} \left[(\mathbf{v}^{(1)})^H \mathbf{v}^{(1)} \right] = \frac{P_R}{N_R-2} \cdot (N_R-2) = P_R \end{aligned}$$

where $\mathbf{W}_E^H \mathbf{W}_E = \mathbf{I}_{N_R-2}$. As can be seen, the transmit power P_R is equally allocated to the N_R-2 entries of $\mathbf{v}^{(1)}$. In the revised manuscript, we have clarified the power normalization factor.

6. The reviewer questions the correction of (7). I believe $[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1}]_{\{1,1\}}$ should be replaced by $\|[\mathbf{C}_{ZF}]_{\{1,1\}}\|^2 + \|\mathbf{C}_{ZF}\}_{\{1,2\}}\|^2$, similarly, $[(\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1}]_{\{2,2\}}$ should be replaced by $\|[\mathbf{C}_{ZF}]_{\{2,1\}}\|^2 + \|\mathbf{C}_{ZF}\}_{\{2,2\}}\|^2$;

Response: Both (7) and the suggested expression are correct since they are equivalent. Specifically, the covariance matrix of noise vector $[\bar{n}_A \quad \bar{n}_B]^T$ can be expressed as

$$\begin{aligned} \mathbb{E} \left[[\bar{n}_A \quad \bar{n}_B]^T [\bar{n}_A^* \quad \bar{n}_B^*] \right] &= \mathbb{E} \left[\mathbf{C}_{ZF} \tilde{\mathbf{n}}_R \tilde{\mathbf{n}}_R^H \mathbf{C}_{ZF}^H \right] = \mathbf{C}_{ZF} \mathbb{E} \left[\tilde{\mathbf{n}}_R \tilde{\mathbf{n}}_R^H \right] \mathbf{C}_{ZF}^H \\ &= (P_R \beta_{RR} + \sigma_R^2) \mathbf{C}_{ZF} \mathbf{C}_{ZF}^H \end{aligned}$$

which agrees with the expressions suggested by the Reviewer. However, for the ZF equalization at the relay, we have $\mathbf{C}_{ZF} = (\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \mathbf{H}_{UR}^H$ and the above formula can be further obtained as

$$\begin{aligned} \mathbb{E} \left[[\bar{n}_A \quad \bar{n}_B]^T [\bar{n}_A^* \quad \bar{n}_B^*] \right] &= (P_R \beta_{RR} + \sigma_R^2) (\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \mathbf{H}_{UR}^H \mathbf{H}_{UR} (\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \\ &= (P_R \beta_{RR} + \sigma_R^2) (\mathbf{H}_{UR}^H \mathbf{H}_{UR})^{-1} \end{aligned}$$

which verifies the expression of (7).

7. Please check the Ei(.) below (39);

Response: Ei(.) is the notation of the exponential integral function in (38). To make it clear, we define Ei(.) immediately after (38).

8. I believe user a and user b are similar, so (54) should have the same form as (56), so does (55) and

(57). While the current version does not indicates that.

Response: As the eavesdroppers would like to decode the data symbols from both Users A and B in sequence, the difference is caused by the decoding order at the eavesdroppers. It should be noted that different decoding orders will result in different SINRs and further different ergodic rates of data symbols achieved by the eavesdroppers. Specifically, based on (19), the eavesdropper decodes s_{A2} by treating s_{B2} as interference and then decodes s_{B2} free of s_{A2} . After subtracting s_{A2} and s_{B2} in (13) to obtain (30), the eavesdropper decodes s_{A1} by treating s_{B1} as interference and then decodes s_{B1} free of s_{A1} . As can be seen, the eavesdropper first decodes the data symbols from User A and then from User B, which is in sequence but not in parallel. That is why Expressions (54) and (55) are different from (56) and (57) for the eavesdroppers. If we swap the decoding order of Users A and B at the eavesdroppers, the expressions of SINRs will also be swapped for Users A and B. In our work, we have only considered a specific decoding order based on SIC scheme for the eavesdropper as shown in Section II.B. To avoid confusion, we have added some discussions on the effect of decoding order in Section II.B of the revised manuscript.

9. For (59), the second equation confuses me. I cannot obtain the second equation from its left hand. Please provide more details.

Response: Applying integration by parts to (59), we can obtain

$$\begin{aligned} \int_0^{\infty} \frac{1}{2} \log_2(1+x) f_{\gamma_s^E}(x) dx &= \frac{1}{2 \ln 2} \int_0^{\infty} \ln(1+x) dF_{\gamma_s^E}(x) \\ &= \frac{1}{2 \ln 2} \ln(1+x) F_{\gamma_s^E}(x) \Big|_0^{\infty} - \frac{1}{2 \ln 2} \int_0^{\infty} F_{\gamma_s^E}(x) d \ln(1+x). \end{aligned}$$

For the CDF $F_{\gamma_s^E}(x)$, we have $F_{\gamma_s^E}(0) = 0$ and $F_{\gamma_s^E}(\infty) = 1$. Moreover, with $\ln(1+0) = 0$, we can further simplify the above formula as

$$\begin{aligned} &\int_0^{\infty} \frac{1}{2} \log_2(1+x) f_{\gamma_s^E}(x) dx \\ &= \frac{1}{2 \ln 2} \ln(1+x) F_{\gamma_s^E}(x) \Big|_0^{\infty} - \frac{1}{2 \ln 2} \int_0^{\infty} F_{\gamma_s^E}(x) d \ln(1+x) \\ &= \frac{1}{2 \ln 2} \ln(1+x) \Big|_0^{\infty} - \frac{1}{2 \ln 2} \int_0^{\infty} F_{\gamma_s^E}(x) d \ln(1+x) \\ &= \frac{1}{2 \ln 2} \int_0^{\infty} 1 d \ln(1+x) - \frac{1}{2 \ln 2} \int_0^{\infty} F_{\gamma_s^E}(x) d \ln(1+x) \\ &= \frac{1}{2 \ln 2} \int_0^{\infty} (1 - F_{\gamma_s^E}(x)) d \ln(1+x) \\ &= \frac{1}{2 \ln 2} \int_0^{\infty} \frac{1 - F_{\gamma_s^E}(x)}{1+x} dx \end{aligned}$$

This completes the proof.

In (59) of the revised manuscript, we have provided more details for the derivations.

Responses to Reviewer 3's Comments:

1. In this paper, the authors assumed that the relay is equipped with N_r antennas and all the other nodes only have one antennas each. The authors should verify this scenario.

Response: In our network model, we regard the legitimate users and the eavesdroppers as the mobile users, each of which is equipped with a single antenna due to the size limitation. On the other hand, the relay can be regarded as a small base station that helps with information exchange among users, which is equipped with multiple antennas to achieve better performance. For more application details of this scenario, the Reviewer may kindly refer to the following survey paper:

[ref2] X. Chen, C. Zhong, C. Yuen and H. H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40-46, Dec. 2015.

2. A related paper should be cited in order to highlight the novelty of this paper.

[1] F. Zhou, Y. Wu, Rose Q. Hu, Y. Wang, and K. K. Wong, "Energy-Efficient NOMA Enabled Heterogeneous Cloud Radio Access Networks". *IEEE Network*, to be published, 2017.

Response: In the Introduction of the revised manuscript, we have cited the paper for its contributions to NOMA.

3. The decoding scheme is different from the conventional scheme that users with strong channel state information first decodes information then users with weak channel state information decodes information. The authors should verify their decoding schemes.

Response: We agree with the Reviewer that NOMA generally exploits the channel gain differences between users for multiplexing via power allocation to use spectral resource more efficiently. By using the proposed scheme, User A splits itself into two sub-users, say A1 and A2, with the power allocations αP_A and $(1-\alpha)P_A$, respectively. As revealed in Section II.B, the decoding of data symbols s_{A1} and s_{A2} is associated with different channels, which exploits the channel gain differences between Sub-users A1 and A2 to achieve better system performance with NOMA proposal. Similarly, User B also splits itself into two sub-users to exploit the channel gain differences for decoding.

In Section II of the revised manuscript, we have clarified our proposed decoding scheme for exploiting channel gain differences between sub-users.

4. The reviewer has a problem about the derivation for the achievable rate of the eavesdropper.

What's the decoding order of the eavesdropper? The authors should clarify it.

Response: As shown in Section II.B, based on (19), the eavesdropper first decodes s_{A2} by treating s_{B2} as interference and then decodes s_{B2} free of s_{A2} . After subtracting s_{A2} and s_{B2} in (13) to obtain (30), the eavesdropper decodes s_{A1} by treating s_{B1} as interference and then decodes s_{B1} free of s_{A1} . In Section II.B of the revised manuscript, we have clarified the decoding order of the eavesdropper to avoid confusion.

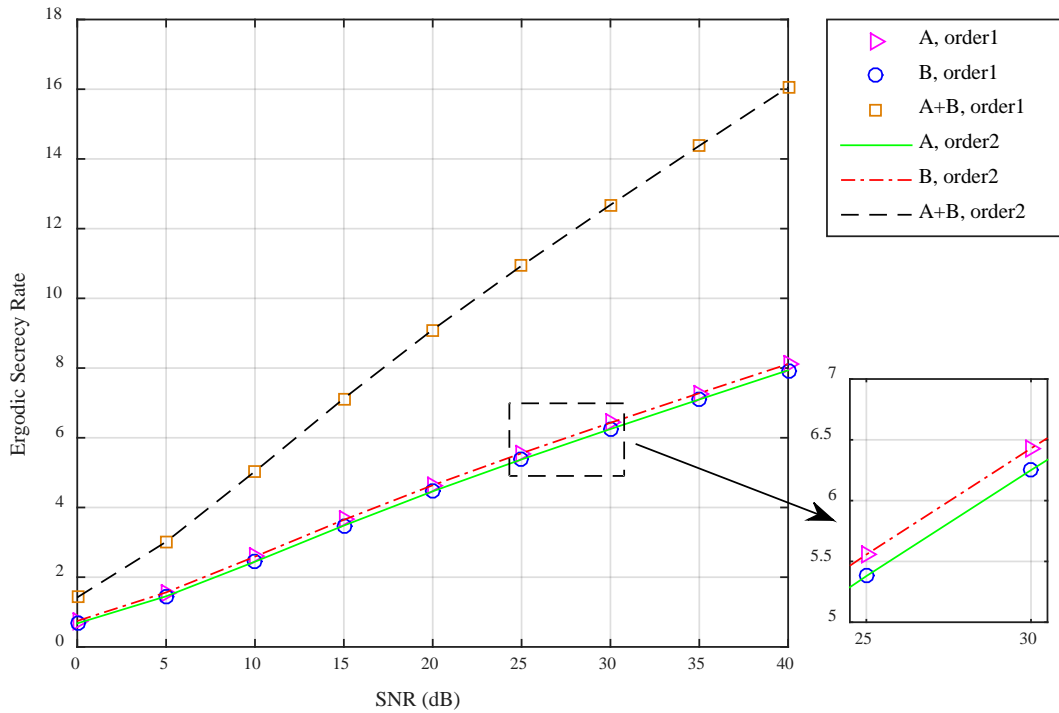
5. For the multiple eavesdropper case, the expression for the secrecy rate should be given. In this case, what's the decoding order of the eavesdroppers? And does the decoding order influence the performance in terms of secrecy rate?

Response: In the revised manuscript, we have given the expressions for the secrecy rate under the multiple-eavesdropper case. For the case of colluding eavesdroppers, all eavesdroppers perform joint processing and can be regarded as a virtual multiple-antenna eavesdropper. The Reviewer may kindly refer the decoding order of the eavesdroppers to the responses to your 4th comment.

Notably, different decoding orders will result in different SINRs and further different performance in terms of secrecy rates achieved by the eavesdroppers. As revealed in Section II.B, we only consider a specific decoding order based on SIC scheme for the eavesdroppers.

6. In the simulation, the authors may add the results related to the effect of the decoding order of the eavesdropper on the secrecy rate.

Response: As revealed in the responses to your 4th comment, the eavesdropper first decodes the data symbols from User A and then from User B. Therefore, the data symbols from User A will suffer from the interference of User B and thus its corresponding ergodic rate is expected to be lower than that of User B for the eavesdropper. Eventually, the secrecy ergodic rate of User A is higher than that of User B. If we swap the decoding order of Users A and B at the eavesdropper, the results of ergodic rates will also be swapped for Users A and B, which are shown below for your convenience.



In the figure, “order1” denotes the case that the eavesdropper first decodes the data symbols from User A and then from User B while “order2” denotes the case that the eavesdropper first decodes the data symbols from User B and then from User A. As can be seen, the ergodic secrecy rates of Users A and B are swapped due the change of decoding order while the ergodic sum secrecy rate remains unchanged. However, due to space limitations, we do not add the above results. In Section II.B of the revised manuscript, we have discussed the effect of decoding order.