IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 9, 2019, accepted June 10, 2019, date of publication June 17, 2019, date of current version July 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2923450

Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami-*m* Channel

CHAO YU[1,2], HAK-LIM KO[2], XIN PENG[1], AND WENWU XIE[1]
[1]College of Information Science and Engineering, Hunan Institute of Science and Technology, Yueyang 414006, China
[2]Department of Information and Communication Engineering, Hoseo University, Asan 31499, South Korea

Corresponding author: Wenwu Xie (gavinxie2015@qq.com)

This work was a part of the project titled "Development of Distributed Underwater Monitoring and Control Networks", funded by the Ministry of Oceans and Fisheries, Korea, and was supported by the Ministry of Science and ICT (MSIT), Korea, under the Information Technology Research Center (ITRC) support program (IITP-2019-2018-08-01417) supervised by the Institute for Information and communications Technology Promotion (IITP). This work was supported in part by the Natural Science Foundation of China under Grant 61772195, in part by the Natural Science Foundation of Hunan Province, China under Grant 2018JJ2154, in part by the Science and Technology Program of Hunan Province under Grant 2016TP1021, in part by the Outstanding Youth Project of Hunan Provincial Education Department under Grant 18B353, and in part by the Emergency Communication Engineering Technology Research Center of Hunan Province under Grant 2018TP2022.

ABSTRACT In this paper, we investigate the secrecy outage performance of a typical cooperative downlink non-orthogonal multiple access (NOMA) system over Nakagami-m fading channel, in which the base station transmits a superimposed signal to two users via a relay. First, the secrecy outage behavior of the considered system over Nakagami-*m* fading channel under three wiretapping cases, e.g., one eavesdropper (Eve), non-colluding and colluding eavesdroppers, are studied, and both analytical and asymptotic expressions for the secrecy outage probability are derived. Next, by considering the availability of Eves' channel state information, we adopt the two-stage relay selection (RS) strategy to improve the system's secrecy outage performance. Finally, simulation results are provided to corroborate the accuracy of our derived expressions. The results show that: 1) there exists secrecy performance floor for cooperative NOMA system, and it was determined by the weak user's secrecy requirement and the channel conditions of the Eves; 2) the two-stage RS scheme can increase the secrecy outage performance significantly under three wiretapping cases; 3) the secrecy performance of cooperative NOMA network is superior to that of orthogonal multiple access network on the condition of low and medium signal-to-noise ratio regions.

INDEX TERMS Physical layer security, non-orthogonal multiple access, cooperative communication, relay selection.

I. INTRODUCTION

With the rapid growth of the demand for wireless communications, non-orthogonal multiple access (NOMA) has been recognized as a potential multiple access technique in the fifth generation (5G) wireless networks due to its band-efficient [1]–[3]. Different from the traditional orthogonal multiple access (OMA), the NOMA solution multiplex additional users' information at the transmitter in the power-domain. Specifically, the transmitter adopts superposition coding scheme to send mixture signal to multiple users, while each user applies successive interference cancellation (SIC) technology to extract its own message. By allocating different transmission power to the signals for different users, the communication from transmitter to multiple users can share the same resource block, e.g., frequency/time/code. The authors of [4] analyzed the outage probability and ergodic sum rate of NOMA system with random deployed users, and demonstrated that the NOMA system is superior to the OMA system. The works in [5] investigated the impact of different user pairing schemes in NOMA and demonstrated that the performance gain achieved by NOMA can be further enlarged by pairing the users whose channel conditions have more difference. The combination of multiple-input-multiple-output (MIMO) and NOMA was investigated in [6]. The results show that NOMA also outperforms traditional OMA in the multiple-antenna scenario.

Adopting cooperative communication technique into NOMA has also received significant attention, since it can form a virtual MIMO system. The authors of [7] first studied cooperative communication in NOMA system. In this work,

The associate editor coordinating the review of this manuscript and approving it for publication was Yinghui Zhang.

the strong users were act as relays to forward signals for users who are in poor channel conditions. The outage probability and ergodic sum rate capacity of cooperative NOMA with full-duplex (FD) and half-duplex (HD) technique was studied in [8]. The results indicate that the FD-based NOMA outperforms HD-based NOMA on the condition of low SNR region due to the impact of self-interference. In [9], the achievable average rate of cooperative NOMA system was analyzed. The work in [10] has proposed a more effective relay selection (RS) scheme to improve the outage probability for cooperative NOMA. The aim of this RS strategy is to maximize the strong user's channel capacity under the condition that the poor user could satisfy its quality of service (QoS). The authors of [11] further investigated a pair of RS schemes for cooperative FD-based NOMA network with randomly deployed relays.

The broadcast nature of wireless transmissions makes it easy for any receiver to obtain the transmitted information, which makes the information security a major concern in the 5G wireless network. The concept of physical layer security (PLS) has received remarkable attention since it exploits the randomness of wireless fading channel rather than cryptography techniques to secure the communication link. As a result, the secure communications can still be guaranteed even if the eavesdroppers in the network are equipped with powerful computational devices [12]–[16]. The authors in [17]–[19] have investigated the secure communication in relaying system. In [17], a link selection scheme was proposed for a buffer-aided relaying network. In [18], secrecy outage performance and achievable secrecy rate were analyzed for a vehicular relay network by exploiting cooperative jamming and superposition coding schemes. In [19], a distributed secure switch-and-stay combining scheme was proposed to safeguard the communications. Adopting PLS in NOMA system has also received increasing research interests. The work in [20] first study the secure transmission in NOMA system. Optimal power allocation policy is proposed for the secrecy sum rate maximization. The work in [21] derived the analytical expressions of secrecy outage probability (SOP) for NOMA system under single-antenna and multiple-antenna scenarios. In [22], a new secure beamforming scheme that based on the application of artificial noise technique was proposed. In [23], the secrecy issues in a NOMA-based network with mixed multicast and unicast traffic was studied. In [24]–[26], some transmit antenna selection (TAS) schemes were proposed to enhance the secrecy of NOMA system. In [24], several TAS schemes were proposed to enhance the secrecy outage performance of NOMA users. In [25], a max-min TAS scheme was proposed to further improve the overall secrecy performance of NOMA system. The authors of [26] analyzed the impact of TAS scheme over Nakagami-*m* fading channel, while the case that the near user should satisfy both the secrecy and QoS requirements was considered.

Although there are many literatures that studied the security issues in NOMA system, the secrecy performance analysis in cooperative NOMA system is limited. In [27], the secrecy performance of a simple cooperative NOMA system was analyzed. The results show that there is no difference in secrecy performance between amplify-and-forward (AF) and decode-and-forward (DF) protocol. The authors of [28] employed the artificial noise (AN) technique in a full-duplex NOMA-based two-way relay network. In [29], a two-stage RS scheme was proposed to enhance the secrecy performance of the cooperative NOMA system. The aforementioned literatures suggest that the cooperative NOMA system has a wide range of application scenarios in 5G network. First, NOMA can improve the spectral efficiency and provide massive connectivity in order to support the 5G network, which connecting billions of Internet of Things (IoT) devices with diversified QoS [30]. Second, relaying technology can increase the coverage of a base station, improve the topology of the cellular network, magnify the connectivity strength through diversity techniques, and support tremendous access [31]. Therefore, the combination of NOMA and relaying technology can gain more benefits for supporting 5G wireless network, and it is important to study the secrecy issues for the wide used NOMA relaying system. Basically, the existing works on secrecy issues of cooperative NOMA are assumed that the channel has Rayleigh fading. It is well known that Nakagami-*m* fading covers a wide range of fading scenarios, and can model the empirical data better than Rayleigh, or Rician fading.

In this paper, we provide a thorough study for the secrecy outage performance of cooperative NOMA system over Nakagami-*m* fading. The main contributions are summarized as follows:

- We consider the secrecy performance for cooperative NOMA system over Nakagami-*m* fading channel. We first derive the closed-form expressions of secrecy outage probability (SOP) for three wiretapping cases, i.e., one eavesdropper, non-colluding eavesdroppers and colluding eavesdroppers. To gain more insights, the asymptotic SOP is also provided.
- In addition, the two-stage RS scheme that focus on enhancing the secrecy performance is considered. The expressions of SOP under two-stage RS scheme are also provided.

The rest of this paper is organized as follows. In Section II, the system model and signal model are presented. The SOP analysis of the cooperative NOMA with random RS scheme is provided in Section III. In Section IV, two-stage RS scheme is considered, and exact and asymptotic expressions of SOP are derived. Simulation results are presented in Section V. Section VI concludes this paper.

II. SYSTEM MODEL

A. SYSTEM MODEL DESCRIPTION

Let us consider a typical downlink HD NOMA relaying system, which includes one BS, K half-duplex relays, a pair of users (D_1 and D_2) and L eavesdroppers (Eve), as shown in Fig. 1. This cooperative NOMA model can be easily

extended to multiple users' case by adopting a hybrid multiple access scheme, where users are divided into multiple orthogonal groups and the NOMA protocol is implemented within each group. Each node in the network is equipped with a single antenna. In this system, the users and Eves are close to the cell edge,[1] so the transmission from BS to user needs the help of a relay, and the information leakage only exists in the transmission between the relay and users [27], [29]. Note that AF-relaying and DF-relaying achieve the similar SOP for cooperative NOMA system [27], for simplifying the analysis, we assume that DF-protocol is employed at each relay. All the channels in the system are assumed undergo quasi-static independent and identically Nakagami-m fading and additive Gaussian white noise (AWGN). The channel coefficient between BS and relay k, $1 \leq k \leq K$, is denoted by h_{SR_k} with integer fading severity parameter m_R and channel mean power $\Omega_R = \mathbb{E}\left(\left|h_{SR_k}\right|^2\right)$, the channel coefficient between relay k and user D_i, $(i = 1, 2)$ is denoted by $h_{R_kD_i}$ with fading parameter m_D and channel mean power $\Omega_{RD} = \mathbb{E}\left(\left|h_{R_kD_i}\right|^2\right)$, and the channel coefficient pertaining to the link relay-Eve is denoted by $h_{R_kE_l}$, $1 \leq l \leq L$, with fading parameter m_E and $\Omega_{RE} = \mathbb{E}\left(\left|h_{R_kE_l}\right|^2\right)$. According to [10], two NOMA users are classified as weak user and strong user based on their QoS requirements, where the weak user's QoS requirements should be given a higher priority. This classification is practical, since some users in the network need quickly connected to receive some critical control message while other users could be served in an opportunistic manner for its purpose of high data rate download requirement.

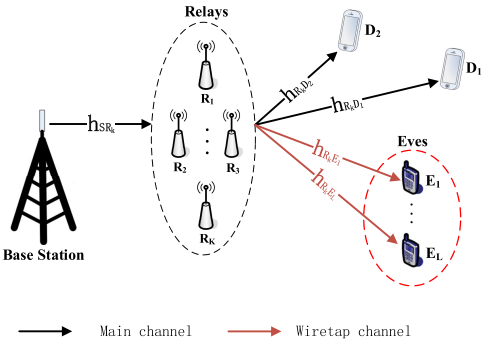

FIGURE 1. A cooperative half-duplex NOMA network includes one base station, K relays, multiple eavesdroppers and a pair of NOMA users.

B. SIGNAL MODEL

During the first time slot, the BS sends a superimposed mixture, $\sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2$, where x_i $(i = 1, 2)$ denotes the united power signal for D_i, i.e. $\mathbb{E}\left(|x_i|^2\right) = 1$, P_s denotes the transmit power and α_i denotes the power allocation coefficient. Without loss of generality, we set $\alpha_1 \geq \alpha_2$ with $\alpha_1 + \alpha_2 = 1$ in order to meet D_1's QoS. Therefore, the observation at relay k can be expressed as

$$y_{R_k} = h_{SR_k}\left(\sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2\right) + n_{SR_k}, \tag{1}$$

where n_{SR_k} denotes the Gaussian noise at relay k.

Similar to [10], by following the principle of SIC,[2] the relays first decode the signal x_1 which has a higher power level, and then remove it from their received signal. Then, the relays decode the signal x_2 without interference. Therefore, the signal-to-interference-plus-noise ratio (SINR) for relay to detect both messages are given by

$$\gamma_{D_1 \to R_k} = \frac{\rho_R \alpha_1 \left|h_{SR_k}\right|^2}{\rho_R \alpha_2 \left|h_{SR_k}\right|^2 + 1}, \tag{2}$$

and

$$\gamma_{D_2 \to R_k} = \rho_R \alpha_2 \left|h_{SR_k}\right|^2, \tag{3}$$

respectively, where $\rho_R = \frac{P_s}{N_{SR_k}}$ is the transmit signal-to-noise ratio (SNR), and N_{SR_k} is the variance of the AWGN at relay k.

During the second time slot, assuming that the relay k is capable of decoding both users' information from a secrecy perspective, i.e. satisfying the following conditions, 1) $\frac{1}{2}\log\left(\frac{1+\gamma_{D_1 \to R_k}}{1+\gamma_{E_1}}\right) \geq R_1$; and 2) $\frac{1}{2}\log\left(\frac{1+\gamma_{D_2 \to R_k}}{1+\gamma_{E_2}}\right) \geq R_2$, where γ_{E_i} denotes the SNR at Eve to decode the message for D_i and will be introduced later, and R_i is the target secrecy rate. Then the relay k is selected to send $\sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2$ to the NOMA user Therefore, the received signal at D_i and l-th Eve can be expressed as

$$y_i = h_{R_kD_i}\left(\sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2\right) + n_{R_kD_i}, \tag{4}$$

and

$$y_{E_l} = h_{R_kE_l}\left(\sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2\right) + n_{E_l}, \tag{5}$$

respectively, where n_A denotes the Gaussian noise at node A, $(A = D_i, E_l)$.

In similar, assuming perfect SIC can be employed at D_2 to detect the message for D_1 which has a higher transmit power. Therefore, the SINR for D_2 to detect x_1 is given by

$$\gamma_{D_1 \to D_2} = \frac{\rho_D \alpha_1 \left|h_{R_kD_2}\right|^2}{\rho_D \alpha_2 \left|h_{R_kD_2}\right|^2 + 1}, \tag{6}$$

where $\rho_D = \frac{P_s}{N_{D_i}}$ is the transmit SNR with N_{D_i} being the variance of the AWGN at D_i. For simplicity, we assume $\rho_D = \rho_R = \rho_R$.

Then, the received SINR at D_2 to detect its own message is given by

$$\gamma_{D_2} = \rho \alpha_2 \left|h_{R_kD_2}\right|^2, \tag{7}$$

[1] We would like to point out that a more general model is that the Eves are not close to the cell edge, and can receive the signal from both BS and relay [18] [28]. This model can lead to a more complicated analysis, and we would like to consider this model in our future work.

[2] There are some literatures [33] [34] investigate the effect of imperfect SIC. We assume perfect SIC for providing an intuitive view of the secrecy performance of cooperative NOMA system, and we will relax this assumption in our future work.

Meanwhile, D_1 decode its own message by treating x_2 as noise, and the SINR can be expressed as

$$\gamma_{D_1} = \frac{\rho\alpha_1 \left|h_{R_k D_1}\right|^2}{\rho\alpha_2 \left|h_{R_k D_1}\right|^2 + 1}, \tag{8}$$

We now consider the SNR for eavesdropper to decode x_1 and x_2. In this work, we consider three wiretapping cases, i.e., 1) one eavesdropper case; 2) non-colluding case, which indicates that each eavesdropper works independently without cooperation to decode the messages; 3) colluding case, which means that all the eavesdroppers' received signals can be processed by a central node. Like [16], [17] and [20], we also consider the worst-case scenario that the Eves are assumed to have powerful detection capabilities. Under this assumption, the Eves can distinguish multiuser data stream, which can detect x_1 (or x_2) without being interfered by x_2 (or x_1). Since the capabilities of Eves are often unknown, it is reasonable to adopt this assumption to overestimate the Eves' decodability and to offer a lower bound of actual cases. Then, the instantaneous SNR at Eve to wiretap the signal for legitimate user D_i is given by

$$\gamma_{E_i}^O = \rho_E \alpha_i \left|h_{R_k E}\right|^2, \tag{9}$$

where $\rho_E = \frac{P_s}{N_{E_l}}$ is the transmit SNR with N_{E_l} being the variance of the AWGN at Eves.

For the non-colluding case, the most detrimental Eve is considered. That means

$$\gamma_{E_i}^N = \rho_E \alpha_i \max_{1 \le l \le L} \left\{ \left|h_{R_k E_l}\right|^2 \right\}. \tag{10}$$

For the colluding case, all the Eves' received signals are assumed to be combined at a central node, that means

$$\gamma_{E_i}^Y = \rho_E \alpha_i \sum_{l=1}^{L} \left\{ \left|h_{R_k E_l}\right|^2 \right\}. \tag{11}$$

Since the relays adopt the DF protocol, the channel capacity of BS-D_1, BS-D_2 and relay-Eve links can be expressed as

$$C_{D_1} = \frac{1}{2} \log\left(1 + \min\left\{\gamma_{D_1 \to R_k}, \gamma_{D_1 \to D_2}, \gamma_{D_1}\right\}\right) \tag{12}$$

$$C_{D_2} = \frac{1}{2} \log\left(1 + \min\left\{\gamma_{D_2 \to R_k}, \gamma_{D_2}\right\}\right), \tag{13}$$

and

$$C_{E_i} = \frac{1}{2} \log\left(1 + \gamma_{E_i}\right), \tag{14}$$

respectively, where the use of the coefficient $\frac{1}{2}$ is because that two time slots are needed during each transmission under half-duplex relaying model.

III. SECRECY OUTAGE PERFORMANCE WITH RANDOM RELAY SELECTION SCHEME

In this section, we analyze the SOP for the cooperative NOMA system under three wiretapping cases with random RS scheme in order to provide a basic secrecy performance analysis. It is noted that randomly selecting a relay to forward the signal from the BS to user is the same case as only one relay exists in the relaying system.

A. PRELIMINARY

First, we present the definition of SOP in cooperative NOMA system. According to [6], The SOP is defined as the likelihood of achieving a non-negative target secrecy rate, and can be formulated as

$$P_{out} = \Pr\left(\left[C_{D_i} - C_{E_i}\right]^+ < R_S\right), \tag{15}$$

where $\lceil x \rceil^+ = \max\{0, x\}$, $i = \{1, 2\}$, and R_S denotes the target secrecy rate.

Therefore, in the cooperative NOMA scenario, the SOP can be expressed as

$$\begin{aligned} SOP &= Pr\left(\left[C_{D_1} - C_{E_1}\right]^+ < R_{S_1} or \left[C_{D_2} - C_{E_2}\right]^+ < R_{S_2}\right) \\ &= 1 - \underbrace{\Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} > \varepsilon_1, \frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2\right)}_{P_1}, \end{aligned} \tag{16}$$

where $\varepsilon_i = 2^{2R_{s_i}}$, $\gamma_1 = \min\left\{\gamma_{D_1 \to R_k}, \gamma_{D_1 \to D_2}, \gamma_{D_1}\right\}$, $\gamma_2 = \min\left\{\gamma_{D_2 \to R_k}, \gamma_{D_2}\right\}$, $\gamma_{E_i} = \left\{\gamma_{E_i}^O, \gamma_{E_i}^N, \gamma_{E_i}^Y\right\}$ for three wiretapping cases. It is noted that the two events in P_1 are correlated, which makes it mathematically intractable to obtain an exact analysis of (16). To overcome this intractability, we focus on the analysis of high SNR region, and an upper bound of SINR for γ_1 can be obtain as $\gamma_{D_1 \to R} \approx \gamma_{D_1 \to D_2} \approx \gamma_{D_1} \approx \frac{\alpha_1}{\alpha_2}$. Therefore, P_1 can be approximated as

$$P_1 < \Pr\left(\frac{\alpha_1}{\alpha_2} > \varepsilon_1\left(1 + \gamma_{E_1}\right) - 1, \frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2\right). \tag{17}$$

Then, we derive several channel statistics in order to obtain the analysis result of (17). Since all the channels are assumed to experience Nakagami-m fading, each channel power gain follows gamma distribution, and its probability density function (PDF) and cumulative distribution function (CDF) are given by

$$f_X(x) = \frac{\beta^m x^{m-1}}{\Gamma(m)} \exp(-\beta x), \tag{18}$$

$$F_X(x) = 1 - \sum_{i=1}^{m-1} \frac{\beta^i x^i}{i!} \exp(-\beta x), \tag{19}$$

where $\Gamma(x)$ is the gamma function defined in [14, eq. 8.339.1], $\beta = \frac{m}{\Omega}$, and m and Ω are defined in Section II-A.

Based on (3), (7) and (17), the CDF of γ_2 can be obtained as

$$\begin{aligned} F_{\gamma_2}(x) &= \Pr\left(\min\left\{\gamma_{D_2 \to R_k}, \gamma_{D_2}\right\} < x\right) \\ &= 1 - \Pr\left(\gamma_{D_2 \to R_k} > x, \gamma_{D_2} > x\right) \\ &= 1 - \left(1 - \Pr\left(\gamma_{D_2 \to R_k} < x\right)\right)\left(1 - Pr\left(\gamma_{D_2} < x\right)\right) \\ &= 1 - \left(1 - F_{\left|h_{SR_k}\right|^2}\left(\frac{x}{\rho\alpha_2}\right)\right)\left(1 - F_{\left|h_{R_k D_2}\right|^2}\left(\frac{x}{\rho\alpha_2}\right)\right) \end{aligned}$$

$$= 1 - e^{-\frac{(\beta_R+\beta_D)x}{\rho\alpha_2}} \sum_{i=0}^{m_R-1} \sum_{j=0}^{m_D-1} \frac{\beta_R^i \beta_D^j x^{i+j}}{i!j! \left(\rho\alpha_2\right)^{i+j}}. \quad (20)$$

For simplifying the analysis of (17), We set $\bar{\gamma}_E^O = \rho_E \left|h_{R_k E}\right|^2$. Therefore, the CDF and PDF of $\bar{\gamma}_E^O$ can be obtained as

$$\begin{aligned} F_{\bar{\gamma}_E^O}(x) &= \Pr\left(\rho_E \left|h_{R_k E}\right|^2 < x\right) \\ &= F_{\left|h_{R_k E}\right|^2}\left(\frac{x}{\rho_E}\right) \\ &= 1 - \sum_{i=0}^{m_E-1} \frac{\beta_E^i x^i}{\rho_E^i i!} \exp\left(-\frac{\beta_E x}{\rho_E}\right), \end{aligned} \quad (21)$$

and

$$f_{\bar{\gamma}_E^O}(x) = \frac{\beta_E^{m_E} x^{m_E-1}}{\rho_E^{m_E}\Gamma(m_E)} \exp\left(-\frac{\beta_E x}{\rho_E}\right), \quad (22)$$

respectively.

For non-colluding case, we set $\bar{\gamma}_E^N = \rho_E \max\limits_{1\le l\le L}\left\{\left|h_{R_k E_l}\right|^2\right\}$, and its CDF can be expressed as

$$\begin{aligned} F_{\bar{\gamma}_E^N}(x) &= \Pr\left(\rho_E \max_{1\le l\le L}\left\{\left|h_{R_k E_l}\right|^2\right\} < x\right) \\ &= \left(F_{\left|h_{R_k E}\right|^2}\left(\frac{x}{\rho_E}\right)\right)^L \\ &= \left(1 - \sum_{i=0}^{m_E-1} \frac{\beta_E^i x^i}{\rho_E^i i!} \exp\left(-\frac{\beta_E x}{\rho_E}\right)\right)^L. \end{aligned} \quad (23)$$

Based on (23), by using multinomial theorem [17], we derive the PDF of $\bar{\gamma}_E^N$ as

$$\begin{aligned} & f_{\bar{\gamma}_E^N}(x) \\ &= L\left(F_{\left|h_{R_k E}\right|^2}\left(\frac{x}{\rho_E}\right)\right)^{L-1} f_{\left|h_{R_k E}\right|^2}\left(\frac{x}{\rho_E}\right)\cdot\frac{1}{\rho_E} \\ &= L\left(1-\mathrm{e}^{-\frac{\beta_E x}{\rho_E}} \sum_{i=0}^{m_E-1} \frac{\beta_E^i x^i}{\rho_E^i i!}\right)^{L-1} \frac{\beta_E^{m_E} x^{m_E-1}}{\rho_E^{m_E}\Gamma(m_E)} \exp\left(-\frac{\beta_E x}{\rho_E}\right) \\ &= \frac{\beta_E^{m_E} L}{\rho_E^{m_E}\Gamma(m_E)} \sum_{\Phi_E} A_E x^{D_E+m_E-1} \exp\left(-\frac{B_E \beta_E x}{\rho_E}\right), \end{aligned} \quad (24)$$

where $\Phi_E = \left\{\left(n_1,\ldots,n_{m_E+1}\right) \in \mathbb{Z}^{\ge 0} \middle| \sum_{p=1}^{m_E+1} n_p = L-1\right\}$, $A_E = \frac{(L-1)!}{\prod_{p=1}^{m_E+1} n_p!} \prod_{p=1}^{m_E} \left(-\frac{1}{(p-1)!}\left(\frac{\beta_E}{\rho_E}\right)^{p-1}\right)^{n_p}$, $B_E = L - n_{m_E+1}$, and $D_E = \sum_{p=1}^{m_E} n_p\,(p-1)$.

For colluding case, we also set $\bar{\gamma}_E^Y = \rho_E \sum\limits_{l=1}^{L} \left|h_{R_k E_l}\right|^2$. Utilizing the summation and scaling properties of gamma distribution, the CDF and PDF of $\bar{\gamma}_{E_i}^Y$ are given by

$$F_{\bar{\gamma}_E^Y}(x) = 1 - \sum_{i=0}^{L\cdot m_E-1} \frac{\beta_E^i x^i}{\rho_E^i i!} \exp\left(-\frac{\beta_E x}{\rho_E}\right), \quad (25)$$

and

$$f_{\bar{\gamma}_E^Y}(x) = \frac{\beta_E^{L\cdot m_E} x^{L\cdot m_E-1}}{\rho_E^{L\cdot m_E}\Gamma(L\cdot m_E)} \exp\left(-\frac{\beta_E x}{\rho_E}\right), \quad (26)$$

respectively.

B. SECRECY OUTAGE PERFORMANCE ANALYSIS

In this subsection, the SOP of three wiretapping cases without RS scheme are derived as Theorem 1.

Theorem 1: Under Nakagami-*m* fading, the SOP of cooperative NOMA system under three wiretapping case are approximately expressed as

$$\begin{aligned} SOP^O = 1 &- \frac{\varpi\beta_E^{m_E}}{\rho_E^{m_E}\Gamma(m_E)} \sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1} \frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}} \\ &\times \sum_{q=0}^{i+j} \Delta_q \mu_1^{-n_1-1} \gamma\left(n_1+1, \mu_1\tau\right), \end{aligned} \quad (27)$$

$$\begin{aligned} SOP^N = 1 &- \frac{\varpi L\beta_E^{m_E}}{\rho_E^{m_E}\Gamma(m_E)} \sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\sum_{\Phi_E} \frac{A_E\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}} \\ &\times \sum_{q=0}^{i+j} \Delta_q \mu_2^{-n_2-1} \gamma\left(n_2+1, \mu_2\tau\right), \end{aligned} \quad (28)$$

and

$$\begin{aligned} SOP^Y = 1 &- \frac{\varpi\beta_E^{L\cdot m_E}}{\rho_E^{L\cdot m_E}\Gamma(L\cdot m_E)} \sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1} \frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}} \\ &\times \sum_{q=0}^{i+j} \Delta_q \mu_1^{-n_3-1} \gamma\left(n_3+1, \mu_1\tau\right), \end{aligned} \quad (29)$$

respectively, where $\mu_1 = \frac{(\beta_R+\beta_D)\varepsilon_2\rho_E+\beta_E\rho}{\rho\rho_E}$, $\mu_2 = \frac{(\beta_R+\beta_D)\varepsilon_2\rho_E+B_E\beta_E\rho}{\rho\rho_E}$, $n_1 = m_E+q-1$, $n_2 = D_E+n_1$, $n_3 = L\cdot m_E+q-1$, $\tau = \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}$, $\Delta_q = \binom{i+j}{q}(\varepsilon_2-1)^{i+j-q}(\varepsilon_2\alpha_2)^q$, $\varpi = e^{-\frac{(\beta_R+\beta_D)(\varepsilon_2-1)}{\rho\alpha_2}}$, and $\gamma(a,x)$ denotes the lower incomplete gamma function [14, eq. 8.350.1].

Proof: Based on (16) and (17), the SOP of one Eve case can be rewritten as

$$\begin{aligned} SOP &= 1 - \Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}, \gamma_2 > \varepsilon_2\left(1+\alpha_2\bar{\gamma}_E\right)-1\right) \\ &= 1 - \underbrace{\int_0^\tau \left(1 - F_{\gamma_2}\left(\varepsilon_2\left(1+\alpha_2 x\right)-1\right)\right) f_{\bar{\gamma}_E}(x)dx}_{J_1}, \end{aligned} \quad (30)$$

where $\bar{\gamma}_E = \left\{\bar{\gamma}_E^O, \bar{\gamma}_E^N, \bar{\gamma}_E^Y\right\}$.

Substituting (20) and (22) into (28), and utilizing binomial theorem and [14, eq. 3.351.1], J_1 can be derived as

$$J_1 = \int_0^\tau e^{-\frac{(\beta_R+\beta_D)(\varepsilon_2(1+\alpha_2 x)-1)}{\rho\alpha_2}} \sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1} \frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}$$

$$\times \left(\varepsilon_2\left(1+\alpha_2 x\right)-1\right)^{i+j}\frac{\beta_E^{m_E}x^{m_E-1}}{\rho_E^{m_E}\Gamma\left(m_E\right)}\exp\left(-\frac{\beta_E x}{\rho_E}\right)dx$$
$$=\frac{\beta_E^{m_E}}{\rho_E^{m_E}\Gamma\left(m_E\right)}e^{-\frac{\left(\beta_R+\beta_D\right)\left(\varepsilon_2-1\right)}{\rho\alpha_2}}\sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}$$
$$\times\sum_{q=0}^{i+j}\binom{i+j}{q}\left(\varepsilon_2-1\right)^{i+j-q}\left(\varepsilon_2\alpha_2\right)^q$$
$$\times\int_0^{\tau}x^{m_E+q-1}e^{-\frac{\left(\beta_R+\beta_D\right)\varepsilon_2\rho_E+\beta_E\rho}{\rho\rho_E}x}dx$$
$$=\frac{\varpi\beta_E^{m_E}}{\rho_E^{m_E}\Gamma\left(m_E\right)}\sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}$$
$$\times\sum_{q=0}^{i+j}\Delta_q\mu_1^{-n_1-1}\gamma\left(n_1+1,\mu_1\tau\right). \tag{31}$$

Substituting (31) into (30), we can obtain the SOP of the cooperative NOMA system in the presence of one eavesdropper case as (27).

Then, substituting (20), (24) and (20), (26) into (28), respectively, and following a procedure similar to that used to obtain (31), we can derive the SOP of the cooperative NOMA system under non-colluding and colluding wiretapping cases as (28) and (29), respectively. The proof is complete. ■

C. ASYMPTOTIC SECRECY OUTAGE PROBABILITY ANALYSIS

To investigate the asymptotical secrecy outage probability of cooperative NOMA over Nakagami-*m* fading, we derive closed-form expressions for the SOP under three wiretapping cases in the high SNR region and present the asymptotic SOP in the following Theorem.

Theorem 2: When $\rho\to\infty$, the asymptotic SOP of the cooperative NOMA system over Nakagami-m fading under three wiretapping cases are derived as

$$ASOP^O=\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{\rho_E^i i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right), \tag{32}$$

$$ASOP^N=1-\left(1-\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{\rho_E^i i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^L, \tag{33}$$

and

$$ASOP^Y=\sum_{i=0}^{L\cdot m_E-1}\frac{\beta_E^i\tau^i}{\rho_E^i i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right), \tag{34}$$

respectively.

Proof: As $\rho\to\infty$, it is obvious that the SOP of the cooperative NOMA system under each wiretapping case was determined by legitimate user D_1, since $\gamma_2\to\infty$. Therefore, the Asymptotical SOP of cooperative NOMA is given by

$$ASOP=Pr\left(\left\lceil C_{D_1}-C_{E_1}\right\rceil^+<R_{S_1}or\left\lceil C_{D_2}-C_{E_2}\right\rceil^+<R_{S_2}\right)$$
$$\approx \Pr\left(\left\lceil C_{D_1}-C_{E_1}\right\rceil^+<R_{S_1}\right)$$
$$\approx \Pr\left(\bar{\gamma}_E>\frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}\right)$$
$$=1-F_{\bar{\gamma}_E}\left(\tau\right). \tag{35}$$

Substituting (21), (23), and (25) into (35), respectively, we can obtain the asymptotic SOP expressions for three wiretapping cases as (32), (33) and (34), respectively. The proof is complete. ■

Remark 1: From the asymptotic expressions of SOP, we can see that there exists a secrecy performance floor in cooperative NOMA system, which was determined by the power allocation coefficients, the secrecy requirement of legitimate user D_1, and the channel condition at Eve. The reason for this phenomenon is because that the achievable data rate of D_1 is limited by the ratio of the power allocation coefficients, $\frac{\alpha_1}{\alpha_2}$, while the Eve has no such limitation on the achievable data rate.

IV. SECRECY OUTAGE PERFORMANCE WITH TWO-STAGE RELAY SELECTION

In this section, we consider the case that all the channel state information (CSI) are available. This assumption is valid when the Eve works in an active way [36], [37]. In this case, the Eve may act as a legitimate user by registering in the network, so the legitimate node could estimate the Eve's CSI. Furthermore, even for the passive Eve, there has a method that allows the legitimate nodes to estimate the Eve's CSI from the local oscillator power that unwittingly leaked from the Eve's RF front end [38]. Under this assumption, the two-stage RS strategy can be used to improve the secrecy performance of the cooperative NOMA system [5], [29], and the analytical and asymptotic expressions for the SOP are derived.

A. RELAY SELECTION SCHEME

The aim of the two-stage RS strategy is mainly focused on maximizing the strong user's data rate under the condition that the QoS of the weak user is satisfied [5]. From the secrecy perspective, the two-stage RS can be described as: 1) Build a subset of the relays that could satisfy weak user's secrecy requirement; 2) Select the best relay from the subset that can maximizing the strong user's secrecy capacity. Hence, the first stage is to build a relay set that satisfy the following condition

$$\mathbb{S}_R=\left\{k:1\le k\le K,\frac{1}{2}\log\left(\frac{1+\gamma_1}{1+\gamma_{E_1}}\right)\ge R_{S_1}\right\}. \tag{36}$$

Then, the second stage selects a relay from $\mathbb{S}_R$ that can maximize the secrecy capacity of D_2, and can be expressed as

$$i^*=\arg\max_i\left\{\frac{1}{2}\log\left(\frac{1+\gamma_2}{1+\gamma_{E_2}}\right),i\in\mathbb{S}_R\right\}. \tag{37}$$

B. SECRECY OUTAGE PERFORMANCE ANALYSIS

From the above explanations, the SOP of the cooperative NOMA based on two-stage RS scheme can be expressed as

$$SOP_{TS}=Pr\left(\mathcal{O}_1\right)+\Pr\left(\mathcal{O}_2\right), \tag{38}$$

where event $\mathcal{O}_1$ denotes that x_1 cannot be securely decoded by all the relays or either of the two legitimate users, and event $\mathcal{O}_2$ denotes that the secrecy transmission of x_2 cannot be guaranteed, given that x_1 can be securely decoded by relay and two users. Based on the first stage of the selection scheme, $\Pr(\mathcal{O}_1)$ can be expressed as

$$\begin{aligned}\Pr(\mathcal{O}_1) &= \Pr(|\mathbb{S}_R| = 0) \\ &= \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{1+\gamma_{D_1\to R_k}}{1+\gamma_{E_1}} > \varepsilon_1, \right.\right. \\ &\quad \left.\left. \frac{1+\gamma_{D_1\to D_2}}{1+\gamma_{E_1}} > \varepsilon_1, \frac{1+\gamma_{D_1}}{1+\gamma_{E_1}} > \varepsilon_1\right)\right], \quad (39)\end{aligned}$$

where $|\mathbb{S}_R|$ denotes the size of $\mathbb{S}_R$. Based on the analytical results in Section III, we also focus on the high SNR region, and (39) can be approximately expressed as

$$\begin{aligned}\Pr(\mathcal{O}_1) &= \prod_{k=1}^{K}\left[1 - \Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}\right)\right] \\ &= \left(1 - F_{\bar{\gamma}_E}(\tau)\right)^K. \quad (40)\end{aligned}$$

Consider the description of the second stage, $\Pr(\mathcal{O}_2)$ is given by

$$\Pr(\mathcal{O}_2) = \sum_{k=1}^{K} \underbrace{\Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} < \varepsilon_2 | |\mathbb{S}_R| = k\right)}_{Q_1} \underbrace{\Pr(|\mathbb{S}_R| = k)}_{Q_2}. \quad (41)$$

According to the analysis in Section III-A, we focus on the high SNR region due to the mathematical intractability of (16). Then, the term Q_1 can be derived as

$$\begin{aligned}Q_1 &= 1 - Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2 | |\mathbb{S}_R| = k\right) \\ &= \left[1 - \frac{\Pr\left(\frac{1+\gamma_2}{1+\alpha_2\bar{\gamma}_E} > \varepsilon_2, \frac{\alpha_1}{\alpha_2} > \varepsilon_1(1+\alpha_1\bar{\gamma}_E) - 1\right)}{\Pr\left(\frac{\alpha_1}{\alpha_2} > \varepsilon_1(1+\alpha_1\bar{\gamma}_E) - 1\right)}\right]^k \\ &= \left[1 - \frac{\Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}, \gamma_2 > \varepsilon_2(1+\alpha_2\bar{\gamma}_E) - 1\right)}{\Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}\right)}\right]^k \\ &= \left[1 - \frac{J_1}{F_{\bar{\gamma}_E}(\tau)}\right]^k. \quad (42)\end{aligned}$$

The term Q_2 can be calculated as follow

$$\begin{aligned}Q_2 &= \binom{K}{k}\left(\Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}\right)\right)^k \\ &\quad \times \left(1 - Pr\left(\bar{\gamma}_E < \frac{1-\alpha_2\varepsilon_1}{\alpha_1\alpha_2\varepsilon_1}\right)\right)^{K-k} \\ &= \binom{K}{k}\left(1 - F_{\bar{\gamma}_E}(\tau)\right)^{K-k}\left(F_{\bar{\gamma}_E}(\tau)\right)^k. \quad (43)\end{aligned}$$

Substituting (40), (41), (42) and (43) into (38), the SOP achieved by the two-stage RS scheme can be obtained as in the following theorem.

Theorem 3: The SOP of the cooperative NOMA system with two-stage RS scheme can be expressed as

$$SOP_{TS} = \sum_{k=0}^{K}\binom{K}{k}\left(1 - F_{\bar{\gamma}_E}(\tau)\right)^{K-k}\left(F_{\bar{\gamma}_E}(\tau) - J_1\right)^k, \quad (44)$$

where J_1 is defined by (31).

Therefore, by substituting (21), (22) and (30) into (44), the SOP for the one eavesdropper case is given by (45), as shown at the bottom of the next page.

In similar, the SOP for the non-colluding and colluding case are given by (46) and (47), respectively, as shown at the bottom of the next page.

C. ASYMPTOTIC SECRECY OUTAGE PROBABILITY ANALYSIS

In this subsection, to gain more insight into secrecy performance enhancement of adopting the two-stage RS scheme, we analyze the asymptotic SOP of the two-stage relay selection strategy under three wiretapping cases, where the transmit power at the BS and the relay approaches infinity. The following theorem presented the asymptotic SOP of the proposed system under three wiretapping cases.

Theorem 4: The asymptotical SOP of the cooperative NOMA system over Nakagami-m fading under three wiretapping cases can be expressed as

$$ASOP_{TS}^{O} = \left(\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^K, \quad (48)$$

$$ASOP_{TS}^{N} = \left(1 - \left(1 - \sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^L\right)^K, \quad (49)$$

and

$$ASOP_{TS}^{Y} = \left(\sum_{i=0}^{L\cdot m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^K, \quad (50)$$

respectively.

Proof: Based on (39) and (40), we find that $\Pr(O_1)$ tends to a constant value as $\rho\to\infty$. Moreover, consider the second RS stage, it is noted that $\gamma_2 \to \infty$ as $\rho\to\infty$. Then, the term Q_1 in (41) tends to zero since $\gamma_2 \to \infty$. Thus, we can obtain that $\Pr(O_2) = 0$.Through the above analysis, the asymptotic SOP under two-stage RS scheme is given by

$$ASOP_{TS} = \left(1 - F_{\bar{\gamma}_E}(\tau)\right)^K. \quad (51)$$

Considering the analysis of the asymptotic SOP in Section III-C, and substituting (32), (33) and (34) into (51), respectively, we can obtain the closed-form expressions of asymptotic SOP for three wiretapping cases. The proof is complete. ■

Remark 2: Comparing theorem 4 to theorem 2, we can find that the secrecy outage performance can gain a remarkable improvement if the two-stage RS scheme is adopted, and the

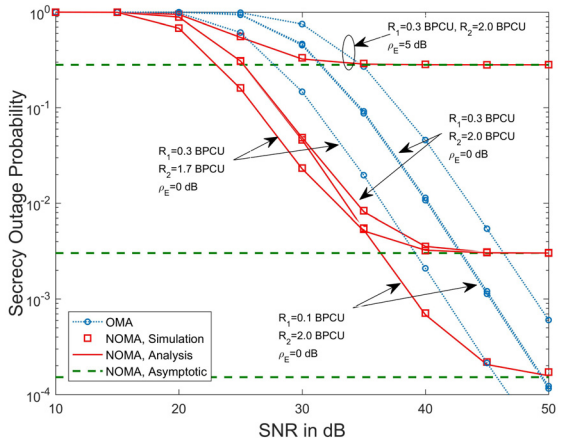

FIGURE 2. SOP of one eavesdropper case under random RS scheme for different parameters. $\alpha_1 = 0.85$, $\alpha_2 = 0.15$.

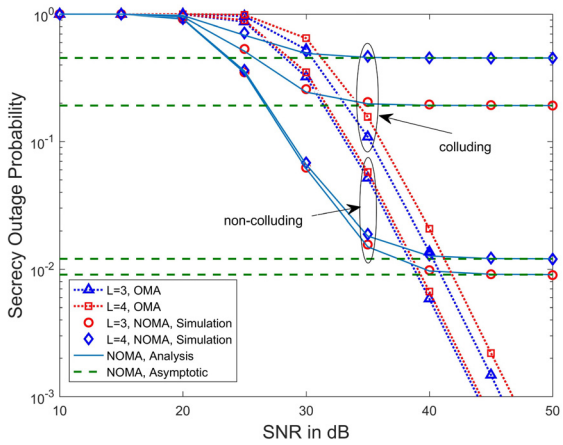

FIGURE 3. SOP of non-colluding and colluding cases under random RS scheme. $\alpha_1 = 0.85$, $\alpha_2 = 0.15$, $R_{S_1} = 0.3$ BPCU, $R_{S_2} = 2$ BPCU, and $\rho_E = 0$ dB.

secrecy performance can be further improved by increasing the number of relays. We could also see that both the random RS and the two-stage RS schemes achieve zero secrecy diversity order. This is because that the weak user's achievable data rate is limited due to the application of NOMA protocol.

V. SIMULATION RESULTS

In this section, simulation results are presented to validate the derived analytical expressions of the SOP for the cooperative NOMA over Nakagami-m fading channel. The main adopted parameters are set as $m_R = m_D = m_E = 2$, $\Omega_R = \Omega_{RE} = \Omega_{RD} = 1$, and BPCU is short for bit per channel use.

Fig. 2 plots the SOP of cooperative NOMA in the presence of one eavesdropper under random RS scheme for different parameters. Conventional orthogonal multiple access (OMA) scheme is adopted as a benchmark. For OMA scheme, four time slots are needed. We can see from Fig. 2 that the SOP of the NOMA system increases as the target secrecy rate or the SNR at the Eve increases. We can also see that the SOPs are saturated in the high SNR region, and the performance floors were determined by the target secrecy rate of the legitimate user D_1 and the SNR at the Eve. The main reason for this phenomenon is that the achievable data rate of the weak user D_1 was limited due to the NOMA protocol, and the larger value of ρ_E leads to higher channel capacity at Eve. The simulation results also reveal that the secrecy requirement of the strong user D_2 has no impact on the secrecy performance floor, which verifies the analysis of the asymptotic SOP in Section III-C. It is also noted that the NOMA scheme is superior to the OMA scheme on the condition of low and medium SNR region. This is because that the NOMA scheme

$$SOP_{TS}^{O} = \sum_{k=0}^{K}\binom{K}{k}\left(\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^{K-k}\left(1-\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right.$$
$$\left.-\frac{\beta_E^{m_E}}{\rho_E^{m_E}\Gamma(m_E)}\varpi\sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}\sum_{q=0}^{i+j}\Delta_q\mu_1^{-n_1-1}\gamma\left(n_1+1,\mu_1\tau\right)\right)^{k} \quad (45)$$

$$SOP_{TS}^{N} = \sum_{k=0}^{K}\binom{K}{k}\left(1-\left(1-\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^{L}\right)^{K-k}\left(\left(1-\sum_{i=0}^{m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^{L}\right.$$
$$\left.-\frac{L\beta_E^{m_E}}{\rho_E^{m_E}\Gamma(m_E)}\varpi\sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\sum_{\Phi_E}A_E\frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}\sum_{q=0}^{i+j}\Delta_q\mu_2^{-n_2-1}\gamma\left(n_2+1,\mu_2\tau\right)\right)^{k} \quad (46)$$

$$SOP_{TS}^{Y} = \sum_{k=0}^{K}\binom{K}{k}\left(\sum_{i=0}^{L\cdot m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right)^{K-k}\left(1-\sum_{i=0}^{L\cdot m_E-1}\frac{\beta_E^i\tau^i}{i!}\exp\left(-\frac{\beta_E\tau}{\rho_E}\right)\right.$$
$$\left.-\frac{\beta_E^{L\cdot m_E}}{\rho_E^{L\cdot m_E}\Gamma(L\cdot m_E)}\varpi\sum_{i=0}^{m_R-1}\sum_{j=0}^{m_D-1}\frac{\beta_R^i\beta_D^j}{i!j!\left(\rho\alpha_2\right)^{i+j}}\sum_{q=0}^{i+j}\Delta_q\mu_1^{-n_3-1}\gamma\left(n_3+1,\mu_1\tau\right)\right)^{k}. \quad (47)$$

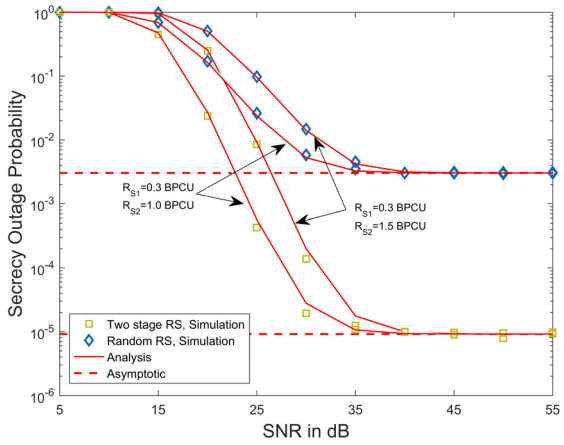

FIGURE 4. SOP of one eavesdropper cases under two-stage RS scheme. $\alpha_1 = 0.85$, $\alpha_2 = 0.15$, $K = 2$, and $\rho_E = 0$ dB.

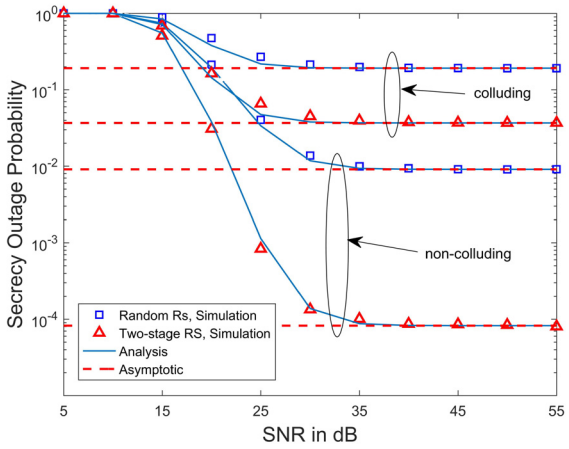

FIGURE 5. SOP of non-colluding and colluding cases under two-stage RS scheme. $\alpha_1 = 0.85$, $\alpha_2 = 0.15$, $R_{S_1} = 0.3$ BPCU, $R_{S_2} = 1$ BPCU, $K = 2$, and $L = 3$.

provides a higher spectrum efficiency. However, the OMA scheme outperforms the NOMA scheme in the high SNR region, since the limitation of the achievable data rate of D_1 in the NOMA scheme is not exist in the OMA scheme.

In Fig. 3, the SOP curves for non-colluding and colluding cases are presented. It is obvious that the secrecy performance degrades as the number of Eves increases. Specifically, in the non-colluding case, increasing the number of Eves does not have much negative impact on the secrecy outage performance of the system. However, in the colluding case, the SOP for cooperative NOMA degrades significantly as the number of Eves increases. We can also see that the colluding case is more detrimental to the system secrecy performance than the non-colluding case. This is because that the multi Eves' case can be actually modelled as a single eavesdropper with multiple antennas. The non-colluding case can be explained as the case that receive antenna selection scheme is used, while the colluding case can be explained as the maximum ratio combining is adopted at the multi-antenna eavesdropper. As a result, increasing the number of Eves leads more improvement of the eavesdropping ability in colluding case than that of non-colluding case. We could also see that the secrecy performance saturated as $\rho \to \infty$, which is proved in Section IV-C. Again, the NOMA scheme outperforms the OMA scheme in the medium SNR region under both non-colluding and colluding wiretapping cases.

In Fig. 4 and 5, we compared the secrecy outage performance for two-stage RS scheme with that for random RS scheme. It is obvious that the secrecy performance can be improved in each wiretapping case by adopting two-stage RS scheme. Again, there also exists secrecy performance floor even though the effective RS scheme is implemented. This is because that the application of two-stage RS scheme cannot remove the limitation, $\frac{\alpha_1}{\alpha_2}$, which caused by the NOMA protocol. From Fig. 2, 3, 4 and 5, we can observe that our derived analytical expressions for the SOPs in each wiretapping case under two RS schemes accurately match the simulation results, which confirms the correctness of our approximate analysis. It is also noted that the exact analytical and simulation results for each scenario tends to the asymptotical ones as $\rho \to \infty$, which demonstrates the accuracy of our asymptotic analysis.

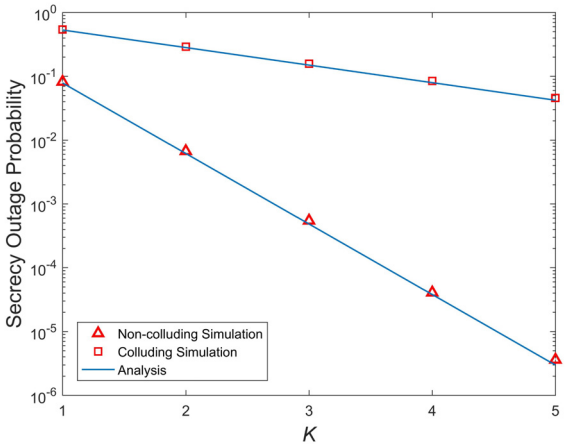

FIGURE 6. SOP of non-colluding and colluding cases versus K. $\alpha_1 = 0.85$, $\alpha_2 = 0.15$, $R_{S_1} = 0.5$ BPCU, $R_{S_2} = 1$ BPCU, $\rho = 35$dB, $\rho_E = 0$dB, and $L = 3$.

Fig. 6 shows the SOP of non-colluding case and colluding case under two-stage relay selection with respect to the number of relays K. We can observe that the SOPs of both multiple Eves' cases decrease as the number of relays K increases. This improvement is cause by the implementation of the effective RS scheme, which exploit the diversity of relaying network.

As we can see from the asymptotic analysis, the power allocation coefficients have a great impact on secrecy performance of cooperative NOMA system. In Fig. 7, we plot the SOP curves with respect to α_1 in order to clarify the effect of different power allocation scheme on the SOP of the system, where $\alpha_1 > \alpha_2$ and $\alpha_2 = 1-\alpha_1$. As we can see from the figure, there exists optimal values of α_1 and α_2 for both multiple Eves wiretapping scenarios, denoted by α_1^* and α_2^*, that

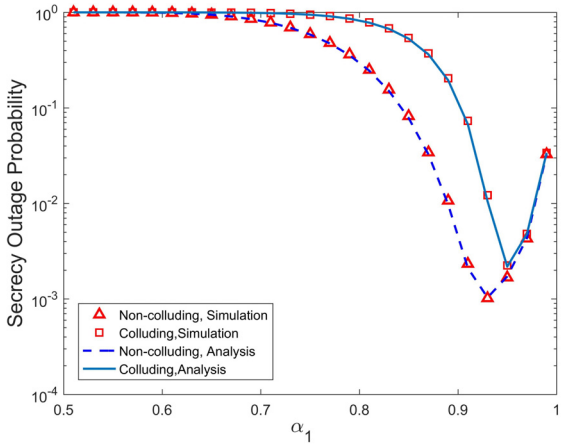

FIGURE 7. SOP of non-colluding and colluding cases versus α_1. $R_{S_1} = 0.5$ BPCU, $R_{S_2} = 1$ BPCU, $\rho_E = 0$dB, $K = 1$, and $L = 3$.

minimize the secrecy outage performance. The main reason for this phenomenon is that when α_1 increases within $\alpha_1 < \alpha_1^*$, the secrecy performance of the weak user increases significantly since more power is allocated to transmit the message for D_1. Therefore, the overall secrecy outage performance can be improved. However, within the range $(\alpha_1^*, 1)$, the overall secrecy outage performance degrades with the increase of α_1. This is because that the secrecy performance of legitimate user D_2 decreases remarkably due to the reduction of α_2, while the improvement of weak user D_1 is limited. From the figure, we can observe that the optimal power allocation coefficients (α_1^*, α_2^*) are roughly equal to $(0.92, 0.08)$ for non-colluding case and $(0.94, 0.06)$ for colluding case.

VI. CONCLUSION

In this paper, the secrecy outage performance of cooperative NOMA over Nakagami-*m* fading under three wiretapping cases is investigated. Furthermore, the effective RS scheme is considered to enhance the secrecy performance of the system. Both the analytical and asymptotic expressions of SOPs for each wiretapping case are obtained in closed-form. Simulation results are provided to verify the accuracy of our analysis. It is noted that there exists secrecy performance floor for each wiretapping case due to the application of NOMA scheme, and it cannot be removed through either RS scheme or power allocation scheme. The results also show that the SOP of NOMA system is superior to that of OMA system in the low and medium regimes. We noted that our analysis is based on the assumptions that perfect CSI can be obtained and perfect SIC is implemented. Our future works will relax these assumptions for more practical implementations. Moreover, our system model is focused on the case that the Eves just wiretap the relay-user link. The case that the Eves can wiretap both the source-relay and relay-user links (device-to-device aided NOMA scheme [18]) may be a promising research direction. The outcomes of this work can be used as guidelines for the design of secure cooperative NOMA network in 5G communication system.

REFERENCES

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

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

[3] 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, Sep. 2015.

[4] 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.

[5] 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.

[6] 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. 2015.

[7] 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.

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

[9] 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.

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

[11] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Spatially random relay selection for full/half-duplex cooperative NOMA networks," *IEEE Trans. Commun.*, vol. 66, no. 8, pp. 3294–3308, Aug. 2018.

[12] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.

[13] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, to be published.

[14] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[15] D. Wang, P. Ren, J. Cheng, and Y. Wang, "Achieving full secrecy rate with energy-efficient transmission control," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5386–5400, Dec. 2017.

[16] Y. Xu, J. Xia, H. Wu, and L. Fan, "Q-learning based physical-layer secure game against multiagent attacks," *IEEE Access*, vol. 7, pp. 49212–49222, 2019.

[17] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972–985, Mar. 2018.

[18] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10732–10747, Dec. 2017.

[19] X. Lai, L. Fan, X. Lei, J. Li, N. Yang, and G. K. Karagiannidis, "Distributed secure switch-and-stay combining over correlated fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2088–2101, Aug. 2019.

[20] 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.

[21] 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.

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

[23] 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.
[24] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, and B. Alomair, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
[25] H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, and M.-S. Alouini, "Secrecy outage of max–min TAS scheme in MIMO-NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.
[26] D.-D. Tran, H.-V. Tran, D.-B. Ha, and G. Kaddoum, "Secure transmit antenna selection protocol for MIMO NOMA networks over Nakagami-*m* channels," *IEEE Syst. J.*, to be published.
[27] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.
[28] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.
[29] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1670–1683, Jun. 2019.
[30] Z. Ding, L. Dai, and H. V. Poor, "MIMO-NOMA design for small packet transmission in the Internet of Things," *IEEE Access*, vol. 4, pp. 1393–1405, 2016.
[31] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
[32] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.
[33] M. F. Kader, M. B. Shahab, and S. Y. Shin, "Exploiting non-orthogonal multiple access in cooperative relay sharing," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1159–1162, May 2017.
[34] G. Im and J. H. Lee, "Outage probability for cooperative NOMA systems with imperfect SIC in cognitive radio networks," *IEEE Commun. Lett.*, vol. 23, no. 4, pp. 692–695, Apr. 2019.
[35] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed. New York, NY, USA: Addison-Wesley, 1994.
[36] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
[37] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2012.
[38] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Mar. 2012, pp. 2809–2812.

CHAO YU received the B.S. degree in electronic and information engineering from the North China University of Technology, in 2008, and the M.S. degree from the Guilin University of Electronic Technology, in 2012. He is currently pursuing the Ph.D. degree with Hoseo University in South Korea. His research interests include cooperative communications, non-orthogonal multiple access, and physical layer security.

HAK-LIM KO received the B.S. degree in electronic engineering from Soongsil University, Seoul, South Korea, in 1983, the M.S. degree in electrical engineering from Fairleigh Dickinson University, Teaneck, NJ, USA, in 1986, and the Ph.D. degree in electrical and computer engineering from North Carolina State University, Raleigh, NC, USA, in 1995. Since 1996, he has been with the Department of Information and Communications Engineering, Hoseo University, Asan-Si, South Korea, where he is currently a Professor. His current research interests include underwater communications and array signal processing.

XIN PENG received the B.S. degree in comÂmunication engineering and the M.S. and Ph.D. degrees in computer science from Hunan UniÂversity, Changsha, China, in 2003, 2008, and 2011, respectively. He was a Visiting Researcher with Auburn University, USA, in 2014. His main research interests include the Internet of Things, CPS, and cloud computing. His research work is sponsored by the National Natural Science Foundation of China, the Natural Science Foundation of Hunan Province, the 13th Five-Year Plan of Education Science Program of Hunan Province, and the Key Research Foundation of Education Bureau of Hunan Province.

WENWU XIE was born in Jingzhou, Hubei, China, in 1979. He received the B.S., M.S., and Ph.D. degrees in communication engineering from Huazhong Normal University, in 2004, 2007, and 2017, respectively. From 2007 to 2009, he was a Communication Algorithm Engineer with Spreadtrum Communication Co. Ltd. Since 2012, he was an Algorithm Manager with Mediatek Co. Ltd. Since 2017, he has been a Lecturer with Hunan Institute of Science and Technology. His research interests include communication algorithm, such as channel estimation, equalizer and encoding/decoding, and so on. And he holds two patents.