IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.xxxx.DOI

Secrecy Outage Probability of Relay Selection Based Cooperative NOMA for IoT Networks

HUI LI[1], YAPING CHEN[1], MINGFU ZHU[2], JIANGFENG SUN[3], DINH-THUAN DO[4], VARUN G MENON[5], SHYNU P. G.[6]

[1]School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454003, China
[2]Huawei-Chuitian 5G Edge Computing Lab, Hebi 458000, China
[3]College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China
[4]Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan
[5]Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India
[6]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India

Corresponding author: Jiangfeng Sun (sunjiangfeng@bupt.edu.cn).

ABSTRACT As an important partner of fifth generation (5G) communication, the internet of things (IoT) is widely used in many fields with its characteristics of massive terminals, intelligent processing, and remote control. In this paper, we analyze security performance for the cooperative non-orthogonal multiple access (NOMA) networks for IoT, where the multi-relay Wyner model with direct link between the base station and the eavesdropper is considered. In particular, secrecy outage probability (SOP) for two kinds of relay selection (RS) schemes (i.e., single-phase RS (SRS) and two-phase RS (TRS)) is developed in the form of closed solution. As a benchmark for comparison, the SOP for random RS (RRS) is also obtained. To gain more meaningful insights, approximate derivations of SOP under the high signal-to-noise ratio (SNR) region are provided. Results of statistical simulation confirm the theoretical analysis and testify that: i) Compared with RRS scheme, SRS and TRS may improve secure performance because of obtaining smaller SOPs; ii) There exists secrecy performance floor for the SOP in strong SNR regime, which is dominated by NOMA protocol; iii) The security performance can be enhanced by augmenting the quantity of relays for SRS and TRS strategies. The purpose of this work is to provide theoretical basis for the analysis and design of anti-eavesdropping for NOMA systems in IoT.

INDEX TERMS Non-orthogonal multiple access, physical layer security, secrecy outage probability, single-phase relay selection, two-phase relay selection.

I. INTRODUCTION

Recently, the rapid development of IoT makes all walks of life get convenient and fast services. However, due to the importance of ownership and privacy protection, the IoT system must provide corresponding security mechanisms. The classical method to deal with the security problem is complex encryption and decryption scheme [1]. Quantum computing can crack complex keys. Moreover, the terminals of IoT are often limited in size and power, and do not have strong computing power. These contradictions lead that the classical method is not so effective in many scenarios [2]. So an alternative mechanism, i.e., physical layer security (PLS) exhibits more advances. The method of PLS was initially discussed by Wyner from the standpoint of information theory [3]. PLS is a new approach to enhance network security by utilizing the characteristics of channels, which has catched quantity of attention due to the randomness of fading channels rather than encryption technology [4]–[7]. In [8], the authors studied the secrecy behaviours for underlay cooperative relaying networks. Recently, NOMA is deemed to have a bright prospect in 5G networks on account that it can improve the band-efficient and spectral efficiency [9]–[13]. Serving multiple users working at the same frequency band with different power-split is the core thought of NOMA [14]. Do *et al.* put forward a model which can serve cellular networks better in NOMA [15]. The authors of [16] discussed a large-scale network with an antenna and multiple antennas in NOMA systems, and derived the SOP. Lei *et al.* researched a security NOMA system including two different forms of eavesdropping [17].

The ambient backscatter NOMA systems was studied in terms of the secure performance [18]. Jiang *et al.* analyzed the secure performance for uplink NOMA including multiple eavesdroppers in [19]. Therefore, exploring PLS in NOMA systems has also aroused the interests of many researchers.

Cooperative communication is a specially efficient method by furnishing greater diversity and expanding network coverage [20]. At present, two fields are mainly included in cooperative communication for NOMA's research. On the one hand, the use of NOMA in cooperative networks was discussed in [21]–[24]. On the other hand, cooperative NOMA was first put forward by Ding *et al* in [25] and researched in [26]–[29]. Choi studied the transmission rates on the cooperative system in [21]. The authors studied the interruption probability (IP) and systematic capacity of NOMA using decoded and forward (DF) in relaying systems [22]. In [23], the SOP was investigated based full-duplex (FD) in cooperative communication using optimizing power allocation jointly. Men *et al.* discussed the outage character using amplify and forward (AF) protocol on Nakagami-*m* distribution for NOMA in [24]. The core idea of cooperative NOMA is that nearby NOMA users are treated as DF relaying to transfer the messages for far NOMA users. The secrecy behaviors for both AF and DF relaying strategies were investigated in cooperative NOMA system [26]. Simultaneous wireless information and power transmission (SWIPT) was adopted by nearby NOMA users which were counted as DF relaying [27]. The work researched the security transmission and proposed an optimal power distribution scheme with maximum secrecy sum rate, where the precondition was that the users' quality of service (QoS) met the conditions [28]. The authors of [29] employed FD and artificial noise (AN) methods in two-way relaying networks based on NOMA. The mathematical expressions for the ergodic secrecy rate were discussed under containing and excluding eavesdroppers.

As a popular transmission scheme, relay selection (RS) has the advantages of low complexity due to taking full advantage of spatial variety and high spectrum-efficient [30], [31]. Considering that there might be some differences between two users in the QoS requirements, two-stage single-relay-selection and dual-relay-selection strategies were put forward, respectively [32]. Ding *et al.* derived closed-form expressions for the precise and asymptotic outage probability (OP) by employing single-stage RS and two-stage RS strategies in cooperative NOMA. And the two NOMA users were classified as nearby and far users by their QoS, rather than their channel conditions [33]. Accurate analytical formulae for the OP and IP were analyzed by using two relay selection strategies (i.e., optimal RS and suboptimal RS) in wireless communication networks (WCNs) [34]. Under three wiretapping cases including one eavesdropper, non-colluding and colluding eavesdroppers, the secrecy outage behaviors of the TRS strategy based on the system over Nakagami-*m* fading channels were investigated in [35]. Zhang *et al.* analyzed the SOP with optimal relay selection, suboptimal relay selection and multiple relays uniting schemes. In addition, the confidentiality of a cognitive DF relaying network over Nakagami-*m* fading channels with independent but not necessarily identical distributed was also surveyed in [36].

Although these previous contributions provided a firm foundation for understanding collaborative NOMA and RS technologies, it still needs further developments and applications. It should be pointed out that RS schemes can meet the requirements of actual IoT situation. In this paper, we investigate the SRS and TRS methods which can achieve the minimum SOP. As far as we know, there is no research on the security performance of SRS and TRS schemes in cooperative NOMA networks considering direct link between base station and eavesdropper. To this end, we explore SOP using RS schemes for basing on half-duplex (HD) NOMA networks over independently Rayleigh distribution. More specifically, the rate of data transmission for the far user is assured to choose a relay as its auxiliary equipment to forward the messages in the SRS strategy. Under the premise of guaranteeing the data transmission rate of far user, the maximum data rate of the service is provided for nearby user to select the relay opportunistically in the TRS scheme. The key contributions of this paper are summarized as follows:

- This paper describes system model of cooperative NOMA for IoT and focuses on two kinds of relay selection strategies (i.e., SRS and TRS schemes). Moreover, the direct link between the eavesdropper and the base station is considered. The eavesdropper uses selective combination (SC) technique to process the received signals from two slots.
- The theoretical SOP is derived by employing the SRS strategy over Rayleigh fading channel. In addition, the SOP for RRS scheme is also analyzed as a contrast. The results show that SRS strategy obtains the lower SOP. To better understand secure outage performance, the asymptotic behaviors of SOP are analyzed with RRS and SRS schemes in cooperative NOMA.
- We also derive the formulas of SOP for TRS scheme in cooperative NOMA based on HD. What's more, experimental results prove that TRS scheme can obtain the superior SOP. To get more insights, the approximate SOP of TRS scheme under high SNR regime is analyzed in cooperative NOMA. The results also verify that the security performance can be enhanced distinctly by augmenting the quantity of relays.

The specific arrangement of each section is as follows. In Section II, the network system of HD NOMA's RS schemes is established. Section III deduces new analytic formulae of SOP for the RRS, SRS and TRS schemes. In Section IV, the asymptotical SOPs in high SNR regime are derived. Section V presents numerical results and systematic performance. The conclusions are shown in Section VI in the paper.

Notations: The $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes the complex Gaussian distribution with expectation μ and standard variance σ. The $\Pr\left(\cdot\right)$ and $\mathbb{E}\left(\cdot\right)$ are the probability and expectation operation. $f_X\left(\cdot\right)$ and $F_X\left(\cdot\right)$ are the probability density function (PDF)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

and the cumulative distribution function (CDF), respectively.

II. SYSTEM MODEL

As illustrated in Fig.1, a typical dual-hop NOMA relaying system for IoT includes a base station (*BS*), K half-duplex relays, a couple of legitimate users (e.g., the nearby user D_1 and far user D_2 and one eavesdropper (*Eve*). It should be noted that the direct links from *BS* to D_j $(j = 1, 2)$ are not considered, but the direct link between *BS* and *Eve* exists. So, the *Eve* processes the received signals by using SC arithmetic. Adopting a multi-access scheme, multiple users can be easily partitioned into many groups in this cooperative model, each of these groups implements the NOMA protocol [37]. In the network model, all relaying nodes are equipped with receiving and transmitting antennas, but *BS* and users have only one antenna. The *BS* tries to communicate the users via relays, but there exists eavesdropping between transmissions, and the information leakage exists in the transmission between two slots. Each relay is assumed to use DF protocol. All wireless channels are affected by additive white Gaussian noise (AWGN) and modeled as independent non-selective Rayleigh distribution. The distance from X to Y is represented as d_{XY}, α denotes exponent for the path loss, h_{XY} denotes the channel coefficient from X to Y, $XY \in \{SR_i, R_iD_1, R_iD_2, SE, R_iE\}$ and $h_{XY} \sim \mathcal{CN}(0, 1)$. The PDF and CDF for $|h_{XY}|^2$ have an exponential distribution as

$$f_{|h_{XY}|^2}(x) = \frac{1}{g_{XY}} \exp\left(-\frac{x}{g_{XY}}\right), \tag{1}$$

and

$$F_{|h_{XY}|^2}(x) = 1 - \exp\left(-\frac{x}{g_{XY}}\right), \tag{2}$$

respectively, where g_{XY} is the mean channel power gain [38]. The two legitimate users are segmented into nearby and far users on the basis of their QoS. More specifically, with the assistance of relay chosen, the QoS requirements of legal users can be effectively provided for the IoT scenario. Therefore, we assume that D_1 can serve opportunely with low target data rates, D_2 needs to be served quickly.

During the first stage, the *BS* transmits composite messages $\sqrt{a_1 P_s}x_1 + \sqrt{a_2 P_s}x_2$ to the assistances on the basis of NOMA theory, and normalization method of x_1 and x_2 signal is adopted respectively, i.e. $\mathbb{E}\left(|x_1|^2\right) = \mathbb{E}\left(|x_2|^2\right) = 1$, P_s and P_r denote the transmitted power from the *BS* and R_i. a_1 and a_2 are the corresponding power allocation coefficients. In fact, in order to provide better fairness and QoS requirements among users [39], we hypothesize that $a_2 > a_1$ and $a_1 + a_2 = 1$. Hence the received messages at the *i*th relay R_i can be expressed as

$$y_{SR_i} = \frac{h_{SR_i}}{\sqrt{d_{SR}^{\alpha}}}\left(\sqrt{a_1 P_s}x_1 + \sqrt{a_2 P_s}x_2\right) + n_{SR_i}, \tag{3}$$

where n_{SR_i} is written as the superimposed Gaussian noise at relay *i*.

In order to reduce the interference for decoding signal x_1 of D_1 at R_i, the successive interference cancellation (SIC) method is employed to detect the information x_2 of D_2 firstly with the high power allocation coefficient. Therefore, the received signal-to-interference-plus-noise ratios (SINRs) to decode x_1 and x_2 at R_i are shown by

$$\gamma_{R_i,D_2} = \frac{a_2\rho_s|h_{SR_i}|^2}{a_1\rho_s|h_{SR_i}|^2 + d_{SR}^{\alpha}}, \tag{4}$$

and

$$\gamma_{R_i,D_1} = \frac{a_1\rho_s|h_{SR_i}|^2}{d_{SR}^{\alpha}}, \tag{5}$$

where $\rho_x = \frac{P_x}{N_0}, x \in (s, r)$ is the transmit SNR, and N_0 is the mean power of the AWGN in this system.

In the same way, the message received at *Eve* can be expressed as

$$y_{SE} = \frac{h_{SE}}{\sqrt{d_{SE}^{\alpha}}}\left(\sqrt{a_1 P_s}x_1 + \sqrt{a_2 P_s}x_2\right) + n_{SE}. \tag{6}$$

where n_{D_j}, n_X denote the Gaussian noise at users D_j and X $(X = SE, RE)$.

We analyse the SINR for wiretapper to decode x_1 and x_2. Considering a direct link between *BS* and *Eve* in this paper. Therefore, in this time slot, the instantaneous SINRs at *Eve* that eavesdrops the messages from legal users D_j are written by

$$\gamma_{SE_1} = \frac{a_1\rho_s|h_{SE}|^2}{d_{SE}^{\alpha}}, \tag{7}$$

and

$$\gamma_{SE_2} = \frac{a_2\rho_s|h_{SE}|^2}{a_1\rho_s|h_{SE}|^2 + d_{SE}^{\alpha}}. \tag{8}$$

During the second stage, it is assumed that relay R_i can decode received messages and transmit signals to the target nodes, the following situations are met in this phase, i) $\log\left(\frac{1+\gamma_{R_i,D_1}}{1+\gamma_{E_1}}\right) \geq R_{D_1}$, ii) $\log\left(\frac{1+\gamma_{R_i,D_2}}{1+\gamma_{E_2}}\right) \geq R_{D_2}$, where γ_{E_j} is the SNR at *Eve* and will be further analyzed later, R_{D_j} denotes the target data transmission rate. Selective relay R_i

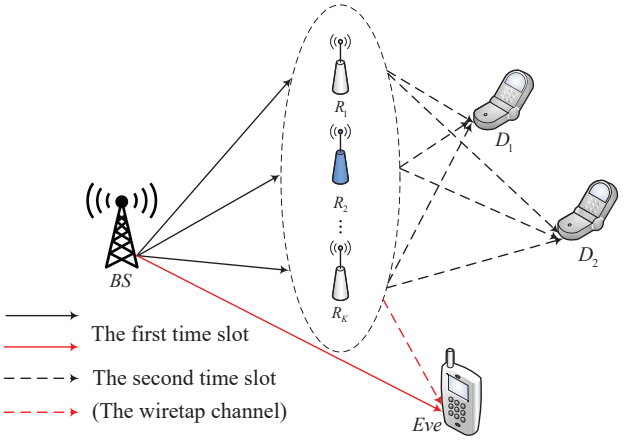

FIGURE 1. system model for IoT

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

forwards the signals to the user, so the signals received in D_j can be represented as

$$y_{D_j} = \frac{h_j}{\sqrt{d_{RD_j}^{\alpha}}}\left(\sqrt{a_1 P_r}x_1 + \sqrt{a_2 P_r}x_2\right) + n_{D_j}. \quad (9)$$

The signals received in *Eve* in this phase can be represented as

$$y_{RE} = \frac{h_{RE}}{\sqrt{d_{RE}^{\alpha}}}\left(\sqrt{a_1 P_r}x_1 + \sqrt{a_2 P_r}x_2\right) + n_{RE}. \quad (10)$$

It is assumed that perfect SIC can be used in D_2 to detect messages from D_1 with a higher transmitting power. Therefore, D_2 detects the SINR of x_1 given by the following formula,

$$\gamma_{D_1,D_2} = \frac{a_2\rho_r|h_1|^2}{a_1\rho_r|h_1|^2 + d_{RD_1}^{\alpha}}. \quad (11)$$

Then, the received SINR at D_1 is given by

$$\gamma_{D_1} = \frac{a_1\rho_r|h_1|^2}{d_{RD_1}^{\alpha}}. \quad (12)$$

Meanwhile, D_2 decodes messages x_2 by regarding x_1 as interference, and the SINR can be shown as

$$\gamma_{D_2} = \frac{a_2\rho_r|h_2|^2}{a_1\rho_r|h_2|^2 + d_{RD_2}^{\alpha}}. \quad (13)$$

For the second time slot, the instantaneous SINRs at *Eve* to wiretap the messages are expressed as

$$\gamma_{R_iE_1} = \frac{a_1\rho_r|h_{R_iE}|^2}{d_{RE}^{\alpha}} \quad (14)$$

$$\gamma_{R_iE_2} = \frac{a_2\rho_r|h_{R_iE}|^2}{a_1\rho_r|h_{R_iE}|^2 + d_{RE}^{\alpha}} \quad (15)$$

III. SOP ANALYSIS

In this part, the SOPs of the cooperative NOMA system using three kinds of relay selection schemes are studied.

To get the SOP for every user, channel statistics for the users and *Eve* are analyzed primarily. Combined with (5) and (12), the CDF of SINR from BS to D_1 can be written as

$$\begin{aligned} F_{\gamma_1}(x) &= \Pr\left(\min\left(\gamma_{R_i,D_1}, \gamma_{D_1}\right) < x\right) \\ &= 1 - \Pr\left(\gamma_{R_i,D_1} > x\right)\Pr\left(\gamma_{D_1} > x\right) \\ &= 1 - \Pr\left(\frac{a_1\rho_s|h_{SR_i}|^2}{d_{SR}^{\alpha}} > x\right)\Pr\left(\frac{a_1\rho_r|h_1|^2}{d_{RD_1}^{\alpha}} > x\right) \\ &= 1 - e^{-\frac{Ax}{a_1}}, \end{aligned} \quad (16)$$

where $\gamma_1 = \min\left\{\gamma_{R_i,D_1}, \gamma_{D_1}\right\}$, $A = \frac{d_{SR}^{\alpha}}{\rho_s g_{SR_i}} + \frac{d_{RD_1}^{\alpha}}{\rho_r g_1}$.

In similar, the CDF of SINR from BS to D_2 is given as

$$F_{\gamma_2}(x) = \begin{cases} 1 - e^{-\frac{Bx}{(a_2 - a_1 x)}} & x \le \frac{a_2}{a_1} \\ 1 & x > \frac{a_2}{a_1}, \end{cases} \quad (17)$$

where $\gamma_2 = \min\left\{\gamma_{R_i,D_2}, \gamma_{D_1,D_2}, \gamma_{D_2}\right\}$, and $B = \frac{d_{SR}^{\alpha}}{\rho_s g_{SR_i}} + \frac{d_{RD_1}^{\alpha}}{\rho_r g_1} + \frac{d_{RD_2}^{\alpha}}{\rho_r g_2}$.

For the signals received in *Eve* ($BS \to E$, $R_i \to E$), the SC algorithm is employed. Then, according to (5), (7) and (14), the CDF of γ_{E_1} is expressed as

$$\begin{aligned} F_{\gamma_{E_1}}(x) &= \Pr\left(\max\left(\gamma_{SE_1}, \min\left(\gamma_{R_i,D_1}, \gamma_{R_iE_1}\right) < x\right)\right) \\ &= \Pr\left(\gamma_{SE_1} < x\right)\left(1 - \Pr\left(\min\left(\gamma_{R_i,D_1}, \gamma_{R_iE_1}\right) > x\right)\right) \\ &= \Pr\left(\gamma_{SE_1} < x\right)\left(1 - \Pr\left(\gamma_{R_i,D_1} > x\right)\Pr\left(\gamma_{R_iE_1} > x\right)\right) \\ &= \left(1 - e^{-\frac{d_{SE}^{\alpha}x}{a_1 g_{SE}}}\right)\left(1 - e^{-\frac{x}{a_1}\left(\frac{d_{SR}^{\alpha}}{g_{SR_i}} + \frac{d_{RE}^{\alpha}}{g_{R_iE}}\right)}\right) \\ &= \left(1 - e^{-\frac{Ex}{a_1}}\right)\left(1 - e^{-\frac{Cx}{a_1}}\right), \end{aligned} \quad (18)$$

where $C = \frac{d_{SR}^{\alpha}}{\rho_s g_{SR_i}} + \frac{d_{RE}^{\alpha}}{\rho_r g_{R_iE}}$, and $E = \frac{d_{SE}^{\alpha}}{\rho_s g_{SE}}$.

The PDF of γ_{E_1} can be obtained as

$$f_{\gamma_{E_1}}(x) = \frac{E}{a_1}e^{-\frac{Ex}{a_1}} + \frac{C}{a_1}e^{-\frac{Cx}{a_1}} - \frac{D}{a_1}e^{-\frac{Dx}{a_1}}, \quad (19)$$

where $D = \frac{d_{SR}^{\alpha}}{\rho_s g_{SR_i}} + \frac{d_{RE}^{\alpha}}{\rho_r g_{R_iE}} + \frac{d_{SE}^{\alpha}}{\rho_s g_{SE}}$.

Referring to the derivation of γ_{E_1}, the PDF of γ_{E_2} can be derived as

$$\begin{aligned} f_{\gamma_{E_2}}(x) = &\frac{Ea_2}{(a_2 - a_1 x)^2}e^{-\frac{Ex}{a_2 - a_1 x}} \\ &+ \frac{Ca_2}{(a_2 - a_1 x)^2}e^{-\frac{Cx}{a_2 - a_1 x}} \\ &- \frac{Da_2}{(a_2 - a_1 x)^2}e^{-\frac{Dx}{a_2 - a_1 x}}. \end{aligned} \quad (20)$$

A. SOP FOR RRS

The SOP is a very important benchmark to evaluate systematic secure performance, we can formulate it as [40]

$$P_{out} = \Pr\left(\left\lceil C_{D_j} - C_{E_j}\right\rceil^+ < R_{th}\right), \quad (21)$$

where $\lceil X\rceil^+ = \max\{X, 0\}$, R_{th} is the threshold of rate.

The SOP for RRS can be rewritten as

$$\begin{aligned} SOP_{RRS} &= \Pr\left(\left\lceil C_{D_1} - C_{E_1}\right\rceil^+ < R_{th_1} or \right. \\ &\qquad \left. \left\lceil C_{D_2} - C_{E_2}\right\rceil^+ < R_{th_2}\right) \\ &= 1 - \Pr\left(\left\lceil C_{D_1} - C_{E_1}\right\rceil^+ > R_{th_1}, \right. \\ &\qquad \left. \left\lceil C_{D_2} - C_{E_2}\right\rceil^+ > R_{th_2}\right) \\ &= 1 - \Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} > \varepsilon_1, \frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2\right), \end{aligned} \quad (22)$$

where $\varepsilon_j = 2^{R_{th_j}}$ with R_{th_j} being the target rates of D_j.

Note that the variables γ_j, γ_{E_j} in (22) are related, acquiring an accurate expression of SOP is difficult. Therefore, the upper bound of SOP is given using the basic probability

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

theory, (22) can be rewritten as

$$SOP_{RRS} \le \min\left\{1, 2 - \Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} > \varepsilon_1\right) - \Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2\right)\right\} \tag{23}$$
$$= \min\left\{1, \underbrace{\Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} < \varepsilon_1\right)}_{p_1^{out}} + \underbrace{\Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} < \varepsilon_2\right)}_{p_2^{out}}\right\}.$$

The term p_j^{out} in (23) represents the SOP for RRS at D_j and can be calculated as

$$p_j^{out} = \Pr\left(\gamma_j < \varepsilon_j\left(1+\gamma_{E_j}\right) - 1\right) = \int_0^{\infty} f_{\gamma_{E_j}}(x) F_{\gamma_j}\left(\varepsilon_j(1+x) - 1\right) dx. \tag{24}$$

Then, on the basis of (16), (19) and (24), p_1^{out} can be obtained as (25), displayed at the top of the next page.

Take full advantage of (24), the SOP for RRS at D_2 can be written as

$$p_2^{out} = \int_0^{\mu} f_{\gamma_{E_2}}(x) F_{\gamma_2}\left(\varepsilon_2(1+x) - 1\right) dx + \int_{\mu}^{\infty} f_{\gamma_{E_2}}(x) dx, \tag{26}$$

where $\mu = \frac{1}{a_1 \varepsilon_2} - 1$.

With the combination of (17), (20), (26) and the Gaussian-Chebyshev quadrature method, the SOP for RRS at D_2 is given by (27), which is at the top of the next page. where $\phi_t = \cos\left(\frac{2t-1}{2N}\pi\right)$, $t \in \{l, m, n\}$, and

$$\varphi_1(x) = \frac{1}{(a_2 - a_1 x)^2} e^{-\frac{Ex}{(a_2 - a_1 x)}} e^{-\frac{B(\varepsilon_2 + \varepsilon_2 x - 1)}{(a_2 - a_1(\varepsilon_2(1+x)-1))}},$$
$$\varphi_2(x) = \frac{1}{(a_2 - a_1 x)^2} e^{-\frac{Cx}{(a_2 - a_1 x)}} e^{-\frac{B(\varepsilon_2 + \varepsilon_2 x - 1)}{(a_2 - a_1(\varepsilon_2(1+x)-1))}},$$
$$\varphi_3(x) = \frac{1}{(a_2 - a_1 x)^2} e^{-\frac{Dx}{(a_2 - a_1 x)}} e^{-\frac{B(\varepsilon_2 + \varepsilon_2 x - 1)}{(a_2 - a_1(\varepsilon_2(1+x)-1))}}.$$

Combining (23), (25) and (27), the SOP for RRS is shown by (28), shown at the top of the next page.

B. SOP FOR SRS

In this part, we consider the SRS scheme for HD-based cooperative NOMA. *BS* can randomly select a relay as its auxiliary to transpond the messages. Maximizing the minimum data transmission rate D_2 is the main idea of SRS method. What's more, the range of data rate for D_2 is dominant by three different data rates: i) the transmission rate for the relay R_i to decode messages x_2, ii) the transmission rate for D_1 to decode messages x_2. iii) the transmission rate for D_2 to decode messages x_2. In relaying networks, the SRS scheme activates a relay, which can be expressed as

$$i_{SRS}^* = \arg\max_i \{\min\{\log(1+\gamma_{R_i,D_2}), \log(1+\gamma_{D_1,D_2}), \log(1+\gamma_{D_2})\}, i \in S_R^1\}, \tag{29}$$

where S_R^1 reveals the amount of relays in the network. Pay attention that the HD-based SRS scheme inherits the advantage of guaranteeing the data rate of D_2, where applications for lower target data rate can be implemented.

In accordance with the above investigations, Ξ_1 denotes that either the relay i_{TRS}^* or any of the legal users is unable to decode x_2 safely. So, the SOP based on SRS scheme with HD can be obtained as follows,

$$SOP_{SRS} = \Pr(\Xi_1) = \Pr\left(\left|S_R^1\right| = 0\right) = \prod_{i=1}^{K}\left(1 - \Pr\left(\frac{1+\min\left(\gamma_{R_i,D_2}, \gamma_{D_1,D_2}, \gamma_{D_2}\right)}{1+\gamma_{E_2}} > \varepsilon_2\right)\right) = \prod_{i=1}^{K}\left(1 - \Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2\right)\right), \tag{30}$$

where $\left|S_R^1\right|$ denotes the size of S_R^1.

Substituting (27) into (30), the SOP for SRS scheme can be obtained, that is shown by (31) at the top of next page.

C. SOP FOR TRS

For HD-based cooperative NOMA, TRS consists of two main periods. In the first period, the objective data rate of D_2 is met. In the second period, we expect to make the data transmission rate of D_1 as high as possible under the condition that the data transmission rate of D_2 is satisfied. Therefore, the first period activates the relays that meet the following conditions,

$$S_R^2 = \{\log(1+\gamma_{R_i,D_2}) \ge R_{D_2}, \log(1+\gamma_{D_1,D_2}) \ge R_{D_2}, \log(1+\gamma_{R_i,D_2}) \ge R_{D_2}, 1 \le i \le K\}, \tag{32}$$

where S_R^2 denotes these relays satisfying the objective data rate of D_2 in the first stage.

For all relays from S_R^2, the second period chooses a relay to transmit messages and maximizes the data rate of D_1, the selected relay is

$$i_{TRS}^* = \arg\max_i \{\min\{\log(1+\gamma_{R_i,D_1}), \log(1+\gamma_{D_1})\}, i \in S_R^2\}. \tag{33}$$

As can be seen from the above explanations, excepting for guaranteeing the data rate of D_2, the TRS scheme based on HD can support D_1 to perform some background tasks.

It is worth noting that the total SOP events can be classified as

$$SOP_{TRS} = \Pr(\Xi_1) + \Pr(\Xi_2), \tag{34}$$

where Ξ_2 means that the relaying i_{TRS}^*, D_1 and D_2 can successfully decode x_2, while the i_{TRS}^* and D_1 cannot successfully decode x_1. Considering the analysis of the second period, $\Pr(\Xi_2)$ is expressed as

$$\Pr(\Xi_2) = \sum_{i=1}^{K} \underbrace{\Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} < \varepsilon_1 \middle| \left|S_R^2\right| = i\right)}_{T_1} \underbrace{\Pr\left(\left|S_R^2\right| = i\right)}_{T_2}, \tag{35}$$

where $\left|S_R^2\right|$ represents the value of S_R^2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

$$\begin{aligned} p_1^{out} &= \int_0^{\infty} f_{\gamma_{E_1}}(x) F_{\gamma_1}(\varepsilon_1(1+x)-1)\, dx \\ &= 1 - \int_0^{\infty} \left(\frac{E}{a_1} e^{-\frac{Ex + A(\varepsilon_1(1+x)-1)}{a_1}} + \frac{C}{a_1} e^{-\frac{Cx + A(\varepsilon_1(1+x)-1)}{a_1}} - \frac{D}{a_1} e^{-\frac{Dx + A(\varepsilon_1(1+x)-1)}{a_1}} \right) dx \\ &= 1 - \left(\frac{E}{E + A\varepsilon_1} + \frac{C}{C + A\varepsilon_1} - \frac{D}{D + A\varepsilon_1} \right) e^{-\frac{A(\varepsilon_1 - 1)}{a_1}}. \end{aligned} \tag{25}$$

$$\begin{aligned} p_2^{out} &= 1 - \int_0^{\mu} f_{\gamma_{E_2}}(x)\, e^{-\frac{B(\varepsilon_2 + \varepsilon_2 x - 1)}{(a_2 - a_1(\varepsilon_2(1+x)-1))}} dx \approx 1 - \frac{E a_2 \mu\pi}{2N} \sum_{l=0}^{N} \sqrt{1-\phi_l^2}\, \varphi_1\left(\frac{\mu\phi_l + \mu}{2}\right) \\ &\quad - \frac{C a_2 \mu\pi}{2N} \sum_{m=0}^{N} \sqrt{1-\phi_m^2}\, \varphi_2\left(\frac{\mu\phi_m + \mu}{2}\right) + \frac{D a_2 \mu\pi}{2N} \sum_{n=0}^{N} \sqrt{1-\phi_n^2}\, \varphi_3\left(\frac{\mu\phi_n + \mu}{2}\right). \end{aligned} \tag{27}$$

$$\begin{aligned} SOP_{RRS} = \min \Bigg\{ 1, 2 - \frac{E}{E + A\varepsilon_1} e^{-\frac{A(\varepsilon_1 - 1)}{a_1}} - \frac{C}{C + A\varepsilon_1} e^{-\frac{A(\varepsilon_1 - 1)}{a_1}} + \frac{D}{D + A\varepsilon_1} e^{-\frac{A(\varepsilon_1 - 1)}{a_1}} - \frac{a_2 \mu\pi}{2N} \times \\ \left(E \sum_{l=0}^{N} \sqrt{1-\phi_l^2}\, \varphi_1\left(\frac{\mu\phi_l + \mu}{2}\right) + C \sum_{m=0}^{N} \sqrt{1-\phi_m^2}\, \varphi_2\left(\frac{\mu\phi_m + \mu}{2}\right) - D \sum_{n=0}^{N} \sqrt{1-\phi_n^2}\, \varphi_3\left(\frac{\mu\phi_n + \mu}{2}\right) \right) \Bigg\}. \end{aligned} \tag{28}$$

$$\begin{aligned} SOP_{SRS} = \Pr(\Xi_1) \approx \Bigg(1 - \frac{a_2 \mu\pi}{2N} \Big(E \sum_{l=0}^{N} \sqrt{1-\phi_l^2}\, \varphi_1\left(\frac{\mu\phi_l + \mu}{2}\right) \\ - C \sum_{m=0}^{N} \sqrt{1-\phi_m^2}\, \varphi_2\left(\frac{\mu\phi_m + \mu}{2}\right) + D \sum_{n=0}^{N} \sqrt{1-\phi_n^2}\, \varphi_3\left(\frac{\mu\phi_n + \mu}{2}\right) \Big) \Bigg)^K. \end{aligned} \tag{31}$$

Because of the mathematical intractability in (22), T_1 can be given as

$$\begin{aligned} T_1 &= 1 - \Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} > \varepsilon_1 \middle| \left|S_R^2\right| = i \right) \\ &= \left[1 - \frac{\Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} > \varepsilon_1, \frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2 \right)}{\Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2 \right)} \right]^i. \end{aligned} \tag{36}$$

So, the term T_1 can be rewritten as (37) by substituting (25) and (27) into (36), it is displayed at the top of next page.

Moreover, there exist i relays in S_R^2, so the corresponding probability T_2 is calculated by

$$\begin{aligned} T_2 &= \binom{K}{i} \left(\Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2 \right) \right)^i \\ &\quad \times \left(1 - \Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} > \varepsilon_2 \right) \right)^{K-i} \\ &= \binom{K}{i} \left(1 - p_2^{out}\right)^i \left(p_2^{out}\right)^{K-i}. \end{aligned} \tag{38}$$

Combining (31), (35), (37) and (38) and employing some arithmetical operations, the SOP for TRS scheme can be expressed as

$$\begin{aligned} SOP_{TRS} = \sum_{i=0}^{K} \binom{K}{i} \left(1 - p_2^{out}\right)^i \left(p_2^{out}\right)^{K-i} \\ \times \min\left(1, \left[\frac{p_1^{out}}{1 - p_2^{out}} \right]^i \right). \end{aligned} \tag{39}$$

IV. ASYMPTOTIC SOP ANALYSIS

To gain deeper insights, the asymptotical SOPs of cooperative NOMA over Rayleigh fading channel are analyzed under these RS schemes. As $\rho \to \infty$ ($\rho_s = \rho_r$), specifically, the SOP of cooperative NOMA systems under each RS scheme depends on far user D_2 when $\gamma_2 \to \infty$. The asymptotical SOP for cooperative NOMA is shown as

$$ASOP_{RRS} \approx \Pr\left(\lceil C_{D_2} - C_{E_2} \rceil^+ < R_{th_2} \right). \tag{40}$$

Substituting (27) into (40), the asymptotic SOP for RRS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

$$T_1 = \min\left\{1, \left[\frac{\left(\frac{E}{E+A\varepsilon_1} - \frac{C}{C+A\varepsilon_1} + \frac{D}{D+A\varepsilon_1}\right) e^{-\frac{A(\varepsilon_1-1)}{a_1}}}{\frac{a_2\mu\pi}{2N}\left(E\sum_{l=0}^{N}\sqrt{1-\phi_l^2}\varphi_1\left(\frac{\mu\phi_l+\mu}{2}\right) + C\sum_{m=0}^{N}\sqrt{1-\phi_m^2}\varphi_2\left(\frac{\mu\phi_m+\mu}{2}\right) - D\sum_{n=0}^{N}\sqrt{1-\phi_n^2}\varphi_3\left(\frac{\mu\phi_n+\mu}{2}\right)\right)}\right]^i\right\}. \quad (37)$$

scheme when $\rho \to \infty$ can be obtained by

$$ASOP_{RRS} = 1 - \frac{a_2\mu\pi}{N}\left\{\sum_{l=0}^{N}\frac{2E\sqrt{1-\phi_l^2}}{\left(2a_2 - a_1\mu\left(\phi_l+1\right)\right)^2} + \sum_{m=0}^{N}\frac{2C\sqrt{1-\phi_m^2}}{\left(2a_2 - a_1\mu\left(\phi_m+1\right)\right)^2} - \sum_{n=0}^{N}\frac{2D\sqrt{1-\phi_n^2}}{\left(2a_2 - a_1\mu\left(\phi_n+1\right)\right)^2}\right\}. \quad (41)$$

From the asymptotic expression of SOP, it can be seen that there exists secure performance floor in cooperative NOMA system, which depends on the NOMA protocol. The main cause for this situation is that the realizable data rate of far user D_2 is restricted by the power distribution coefficient, a_2/a_1. However, there is no such restriction to realize the data rate in *Eve*.

Based on (31), we observe that $\Pr(\Xi_1)$ tends to a constant. Therefore, the asymptotic SOP under SRS scheme is given by

$$ASOP_{SRS} = \left\{1 - \frac{a_2\mu\pi}{N}\left\{\sum_{l=0}^{N}\frac{2E\sqrt{1-\phi_l^2}}{\left(2a_2 - a_1\mu\left(\phi_l+1\right)\right)^2} + \sum_{m=0}^{N}\frac{2C\sqrt{1-\phi_m^2}}{\left(2a_2 - a_1\mu\left(\phi_m+1\right)\right)^2} - \sum_{n=0}^{N}\frac{2D\sqrt{1-\phi_n^2}}{\left(2a_2 - a_1\mu\left(\phi_n+1\right)\right)^2}\right\}\right\}^K. \quad (42)$$

Furthermore, taking into account the second stage, we have

$$Pr\left(\Xi_2\right) = 0, \rho \to \infty. \quad (43)$$

According to the above analysis, the asymptotic SOP under TRS scheme is similar to SRS scheme. That is to say, $ASOP_{TRS} = ASOP_{SRS}$.

By comparing asymptotic SOP under RRS scheme with SRS and TRS schemes, we find that the SRS and TRS schemes prominently improve the secrecy outage performance, and the interesting discovery is that increasing the amount of relays can further enhance the security performance.

V. NUMERICAL RESULTS

In this section, theoretical and practical simulation results are provided. The abbreviation for the bit-per-channel-use is BPCU. Combined with complexity and exactitude, we set up tradeoff parameter: $N = 30$.

Fig. 2 is drawn to describe the SOP of cooperative NOMA under RRS and SRS schemes for different power distribution coefficients with $K = 2$, $\alpha = 3$, $d_{SR} = 0.5$, $d_{RD_1} = 0.3$, $d_{RD_2} = 0.5$, $d_{SE} = 0.8$, $d_{RE} = 0.6$, $R_{th_1} = 2$ and $R_{th_2} = 0.5$, where $a_2 > a_1$ and $a_2 = 1 - a_1$. The blue circles and dash curves indicate the accurate SOP of RRS scheme for HD-based NOMA. The red squares and solid curves are the SRS strategy for cooperative NOMA, as can be seen from the accurate result obtained in (31). The curves of theoretical SOP coincide with the statistical simulation results. No matter what SNR situation is, the performance of SRS strategy is preferable to RRS strategy. Moreover, the SOP of the HD-based SRS and RRS schemes under $a_1 = 0.2$ and $a_2 = 0.8$ outperforms the SRS and RRS schemes under $a_1 = 0.3$ and $a_2 = 0.7$, respectively. Another phenomenon can be clearly obtained that HD-based NOMA RRS scheme under $a_1 = 0.2$ and $a_2 = 0.8$ is superior to SRS scheme under $a_1 = 0.3$ and $a_2 = 0.7$ in high SNR range. The reason for this situation is that the power distribution coefficient has a great influence in HD-based RS strategies. In addition, the simulation results also show that the security requirements of the nearby user D_1 have no effect on the security performance layer, which also proves the conclusion of the approximate SOP analyzed in the previous discussion.

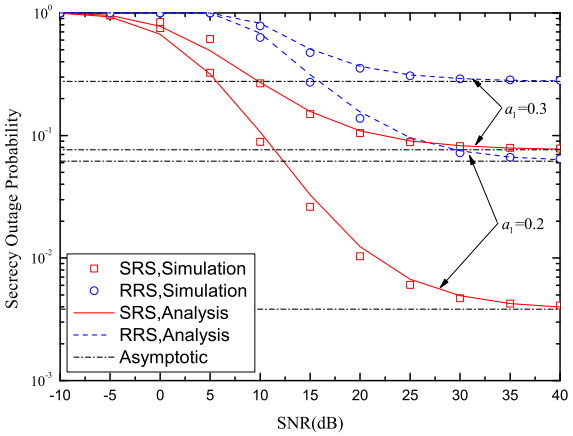

FIGURE 2. SOP versus the transmit SNR for RRS and SRS schemes with $K = 2$, $\alpha = 3$, $R_{th_1} = 2$ and $R_{th_2} = 0.5$.

Fig. 3 depicts the SOP of cooperative NOMA under RRS and TRS schemes for different power distribution coefficients. The red lines represent TRS scheme for cooperative NOMA, and are consistent with the results obtained in (39). According to the analysis results, the TRS strategy can strengthen security performance. Similarly, the SOP of TRS and RRS schemes under $a_1 = 0.2$ and $a_2 = 0.8$ outperforms the TRS and RRS schemes under $a_1 = 0.3$ and $a_2 = 0.7$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3047136, IEEE Access

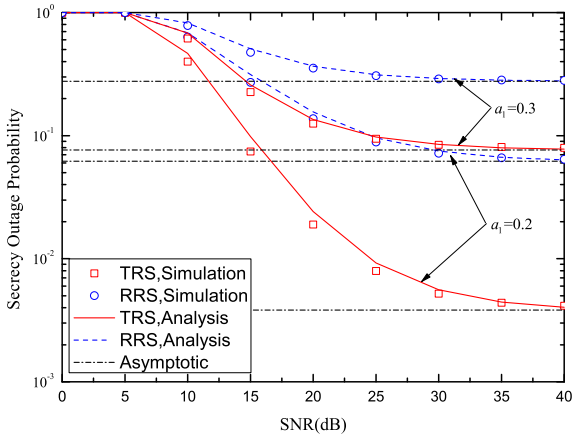

FIGURE 3. SOP versus the transmit SNR for RRS and TRS schemes with $K = 2$, $\alpha = 3$, $R_{th_1} = 2$ and $R_{th_2} = 0.5$.

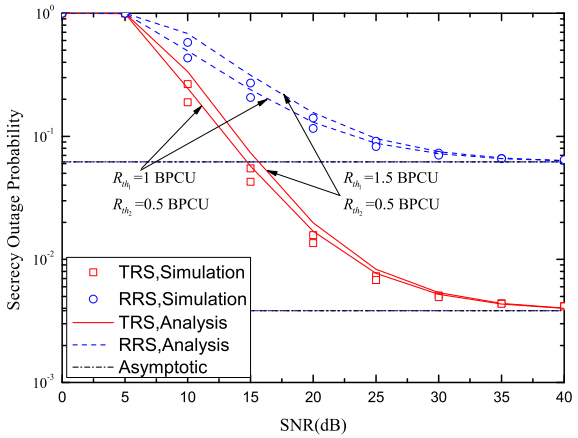

FIGURE 4. SOP versus the transmit SNR for RRS and TRS schemes for the different target rates with $a_1 = 0.2$ and $K = 2$.

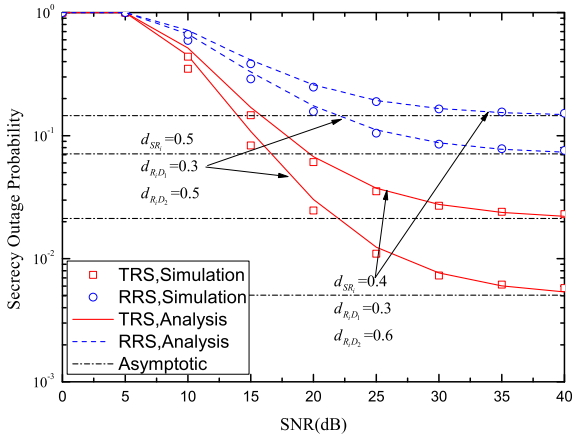

FIGURE 5. SOP versus the transmit SNR for RRS and TRS schemes for the different distances with $R_{th_1} = 1$ and $R_{th_2} = 0.3$.

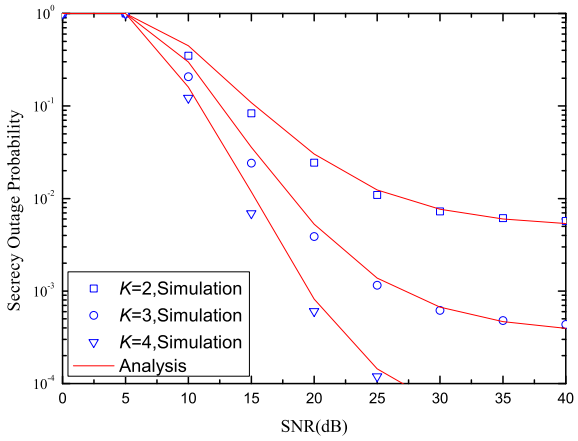

FIGURE 6. SOP versus the transmit SNR for TRS schemes with $K = 2, 3, 4$, $R_{th_1} = 1$ and $R_{th_2} = 0.3$.

respectively. Moreover, when SNR < 25 dB, the security performance of RRS scheme with $a_1 = 0.2$ is inferior to the TRS scheme with $a_1 = 0.3$. When SNR > 25 dB, the security performance of RRS scheme with $a_1 = 0.2$ begins to improve and surpasses the security performance of TRS scheme with $a_1 = 0.3$. Therefore, power distribution coefficient has a great influence on the security performance. It is also worth noting that the SOP is saturated in high SNR, and the target confidentiality rate of legal user D_2 can determine the lower performance. The primary cause for this phenomenon is that the NOMA protocol limits the available data rate for weak user D_2.

In Fig. 4, we compare the SOP using RRS and TRS strategies with different target transmission rates. An interesting observation is that transforming the NOMA user's target rate can affect the security outage behaviors for HD-based RRS and TRS schemes. As the target rate value reduces, the two kinds of schemes provide better outage performance, but the advantage fades away in high SNR range. Even if an effective RS scheme is implemented, there also exists secrecy performance floor. This is because the application of these two schemes does not eliminate the limitations (e.g., a_2/a_1) imposed by the NOMA protocol.

In Fig. 5, the SOP of cooperative NOMA under RRS and TRS schemes for different distances with $K = 2$, $a_1 = 0.2$, $a_2 = 0.8$, $\alpha = 3$, $d_{SE} = 0.6$, $d_{RE} = 0.4$, $R_{th_1} = 1$ and $R_{th_2} = 0.3$. This paper normalizes the distances for d_{SR} and d_{RD_2}, where $d_{RD_1} < d_{RD_2}$ and $d_{RD_1} + d_{RD_2} = 1$, because D_1 is the nearby user, whereas D_2 is the far user. It is observed that the security performance of TRS scheme is superior to RRS scheme when changing the distance. Compared with RRS scheme, there are more obvious variations for TRS scheme with different distances on security performance. Therefore, the distance from *BS* to R_i and from R_i to D_j has a significant impact on the secure outage performance for HD-based systems. Similarly, the SOP of cooperative NOMA can be influenced by d_{SE} and d_{RE}.

Fig. 6 paints the SOP employing TRS scheme when the number of relays is $K = 2, 3, 4$. The results show that the quantity of relays in this model has great effect on the performance of HD-based TRS schemes. When the number

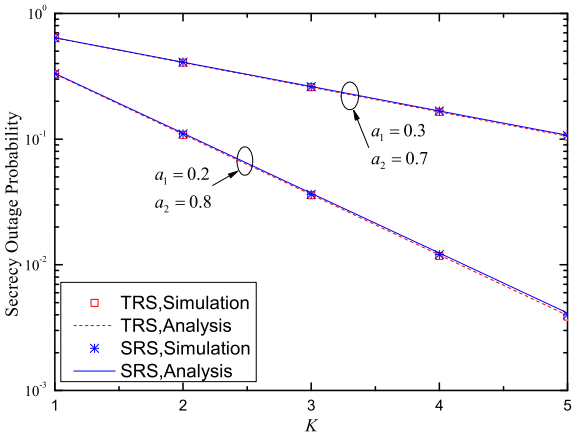

FIGURE 7. SOP versus K for SRS and TRS schemes with $R_{th_1} = 1$ and $R_{th_2} = 0.5$.

of relays increases, the RS schemes can achieve the lower outage probability. The reason is that the number of relays is positively correlated with diversity gain, thus it can improve the reliability of the cooperative networks.

Fig. 7 shows the SOP for both SRS and TRS schemes with respect to the number of relays K in high SNR region. It is observed that the analytic curves are precisely consistent with the simulated results. It can be concluded that the SOP using RS schemes reduces as the quantity of relays K increases. The security performance is improved due to the application of the efficient RS schemes that take advantage of the diversity of relaying networks. Moreover, from the analysis in section IV and expressions (31), (39), the SOP of both SRS and TRS schemes is coincident on account of $p_1^{out} = 0$ in strong SNR. Another conclusion is that the SOP of the RS schemes becomes smaller when the increasing of a_2/a_1 distinctly.

VI. CONCLUSION

This paper has studied the security performance for cooperative HD-based NOMA IoT systems over Rayleigh-distributed under the influence of different relay selection methods. The closed-form formulae of SOP for two users are derived. Further analysis shows that the SRS/TRS scheme can achieve the best secure performance, and RRS strategy may increase the SOP compared with SRS/TRS strategy. The security performance can be enhanced by augmenting the quantity of relays. Whereas, it is pointed out that due to the adoption of NOMA system, each RS scheme exists secrecy performance floor that cannot be deleted by RS schemes and power allocation strategy.

REFERENCES

[1] X. Chen, L. Guo, X. Li, C. Dong, J. Lin, and P. T. Mathiopoulos, "Secrecy Rate Optimization for Cooperative Cognitive Radio Networks Aided by a Wireless Energy Harvesting Jammer," *IEEE Access*, vol. 6, pp. 34 127–34 134, 2018.

[2] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M. Alouini, "Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[3] A. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] 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. Surv. Tutorials*, vol. 21, no. 3, pp. 2734–2771, thirdquarter 2019.

[5] J. Lee, "Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[6] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[7] L. Qing, H. Guangyao, and F. Xiaomei, "Physical Layer Security in Multi-Hop AF Relay Network Based on Compressed Sensing," *IEEE Commun. Lett.s*, vol. 22, no. 9, pp. 1882–1885, Sep. 2018.

[8] A. Pandey, S. Yadav, T. Do, and R. Kharel, "Secrecy Performance of Cooperative Cognitive AF Relaying Networks with Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," *IEEE Trans. Veh. Technol.*, pp. 1–1, Oct. 2020.

[9] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. Piscataway, New Jersey: IEEE, Sep. 2013, pp. 611–615.

[10] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Jul. 2017.

[11] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. Kwak, "Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 721–742, Oct. 2017.

[12] X. Li, Q. Wang, M. Liu, J. Li, H. Peng, J. Piran, and L. Li, "Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks with Hardware Impairments and Channel Estimation Errors," *IEEE Internet Things J.*, pp. 1–1, Oct. 2020.

[13] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin, 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.

[14] T. Nakamura, A. Benjebbour, Y. Kishiyama, S. Suyama, and T. Imai, "5G Radio Access: Requirements, Concept and Experimental Trials," *IEICE Trans. Commun.*, vol. E98.B, no. 8, pp. 1397–1406, Jun. 2015.

[15] D. Do, T. Nguyen, K. M. Rabie, X. Li, and B. M. Lee, "Throughput Analysis of Multipair Two-Way Replaying Networks With NOMA and Imperfect CSI," *IEEE Access*, vol. 8, pp. 128 942–128 953, 2020.

[16] 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.

[17] H. Lei, J. Zhang, K. Park, P. Xu, Z. Zhang, G. Pan, and M. 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.

[18] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy Analysis of Ambient Backscatter NOMA Systems Under I/Q Imbalance," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 286–12 290, Oct. 2020.

[19] K. Jiang, T. Jing, Y. Huo, F. Zhang, and Z. Li, "SIC-Based Secrecy Performance in Uplink NOMA Multi-Eavesdropper Wiretap Channels," *IEEE Access*, vol. 6, pp. 19 664–19 680, 2018.

[20] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Nov. 2004.

[21] J. Choi, "Non-Orthogonal Multiple Access in Downlink Coordinated Two-Point Systems," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 313–316, Jan. 2014.

[22] J. Kim and I. Lee, "Non-Orthogonal Multiple Access in Coordinated Direct and Relay Transmission," *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 2037–2040, Aug. 2015.

[23] Q. Li, P. Ren, and D. Xu, "Security Enhancement and QoS Provisioning for NOMA-Based Cooperative D2D Networks," *IEEE Access*, vol. 7, pp. 129 387–129 401, 2019.

[24] J. Men, J. Ge, and C. Zhang, "Performance Analysis for Downlink Relaying Aided Non-Orthogonal Multiple Access Networks With Imperfect CSI Over Nakagami-m Fading," *IEEE Access*, vol. 5, pp. 998–1004, 2017.

[25] 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.

[26] J. Chen, L. Yang, and M. Alouini, "Physical Layer Security for Cooperative NOMA Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[27] N. Dahi and N. Hamdi, "Relaying in Non-Orthogonal Multiple Access Systems with Simultaneous Wireless Information and Power Transfer," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. Piscataway, New Jersey: IEEE, Jun. 2018, pp. 164–168.

[28] Y. Zhang, H. 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.

[29] B. Zheng, M. Wen, C. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[30] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[31] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M. Alouini, "On Secrecy Outage of Relay Selection in Underlay Cognitive Radio Networks Over Nakagami-m Fading Channels," *IEEE Trans. Cognit. Commun. Networking*, vol. 3, no. 4, pp. 614–627, Dec. 2017.

[32] J. Zhao, Z. Ding, P. Fan, Z. Yang, and G. K. Karagiannidis, "Dual Relay Selection for Cooperative NOMA With Distributed Space Time Coding," *IEEE Access*, vol. 6, pp. 20 440–20 450, 2018.

[33] 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.

[34] X. Li, H. Mengyan, Y. Liu, V. G. Menon, A. Paul, and Z. Ding, "I/Q Imbalance Aware Nonlinear Wireless-Powered Relaying of B5G Networks: Security and Reliability Analysis," *IEEE Trans. Network Sci. Eng.*, pp. 1–1, Sep. 2020.

[35] 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.

[36] H. Zhang, H. Lei, I. S. Ansari, G. Pan, and K. A. Qaraqe, "Security Performance Analysis of DF Cooperative Relay Networks over Nakagami-m Fading Channels," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 5, pp. 2416–2432, May 2017.

[37] Y. Liu, Z. Qin, M. Elkashlan, A. Nallanathan, and J. A. McCann, "Non-Orthogonal Multiple Access in Large-Scale Heterogeneous Networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2667–2680, Dec. 2017.

[38] J. G. Proakis, *Digital communications*, 4th ed. Boston: McGraw-Hill, 2001.

[39] G. Liu, Z. Wang, J. Hu, Z. Ding, and P. Fan, "Cooperative NOMA Broadcasting/Multicasting for Low-Latency and High-Reliability 5G Cellular V2X Communications," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7828–7838, Oct. 2019.

[40] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y. Yao, "Secrecy Outage Probability Analysis of Friendly Jammer Selection Aided Multiuser Scheduling for Wireless Networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, May 2019.

HUI LI received the B.Sc. degree in communication engineering with the School of Information Engineering in 1999. He then received the M. Sc. and Ph. D. degrees from communication and information system in 2004 and information and communication engineering in 2008 in Nanjing University of Science and Technology. He is also a visiting scholar at Charles Darwin University, Australia, in 2013 and North Carolina A & T State University in 2014. He is currently a Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo China. His research interests include wireless communication, intelligent signal processing.

YAPING CHEN received the B.Sc. degree in electronic information science and technology with the School of Physics and Electronic Information Engineering, Henan Polytechnic University in 2019. She is currently pursuing the M.Sc. degree in communication and information systems with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo China. Her research interests include physical layer security (PLS) and cooperative communication.

MINGFU ZHU received the B.Sc. degree from Tianjin University, in 2000, the M.Sc. degree from East China Normal University, in 2004, and the Ph.D. degree from the University of California, Los Angeles(UCLA), in 2007. From 2011 to 2013, he was working with Mayyard Photoelectric Technology Co., Ltd., Ningbo, China, as the executive director. Since 2013, he has founded and served as the chairman of Hebi National Optoelectronics Technology Co., Ltd., Hebi, China. He is currently the chairman of Henan Chuangzhi Technology Co., Ltd. and general manager of Henan Chuitian Technology Co., Ltd., Hebi, China.

His research focuses on chip packaging and intelligent light development and manufacturing. With innovative ideas, intelligent lights are used to build IOL, integrate IOL into IoT, and upgrade to 5G IoT. By building scientific research platforms and manufacturing bases, 5G industry ecosystem is built to interact with upstream and downstream enterprises. The main awards and achievements of Mr. Zhu include the excellent builder for the socialist cause with Chinese characteristics, special government allowance under the State Council and leading talents in Science and Technology Innovation of National "Ten Thousand Talents Plan" and so on. He has served as a member of Henan CPPCC and a vice president of Henan Euro-American Alumni Association. He is also a president of Henan Alumni Association of Tianjin University and a director of Henan Mechanical Engineering Society.

JIANGFENG SUN received the M.S. degree in communication and information system from Zhengzhou University in 2009 and will get a doctor's degree from Beijing University of Posts and Telecommunications. He is currently a Lecturer with the School of College of Computer Science and Technology, Henan Polytechnic University. He has several papers published in journal and conferences, His current research interests include physical layer security, cooperative communications and the performance analysis of fading channels.

DINH-THUAN DO received the B.S. degree, M. Eng. degree, and Ph.D. degree from Vietnam National University (VNU-HCMC) in 2003, 2007, and 2013 respectively, all in Communications Engineering. He was a visiting Ph.D. student with Communications Engineering Institute, National Tsing Hua University, Taiwan from 2009 to 2010. Prior to joining Ton Duc Thang University, he was senior engineer at the VinaPhone Mobile Network from 2003 to 2009. Dr. Thuan was recipient of Golden Globe Award from Vietnam Ministry of Science and Technology in 2015 (Top 10 most excellent scientist nationwide). His name and his achievements will be reported in special book entitle "Young talents in Vietnam 2015-2020". His research interest includes signal processing in wireless communications network, NOMA, full-duplex transmission and energy harvesting. His publications include over 80 SCIE/SCI-indexed journal papers, over 45 SCOPUS-indexed journal papers and over 50 international conference papers. He is sole author in 1 textbook and 1 book chapter. He is currently serving as Editor of Computer Communications (Elservier), Associate Editor of EURASIP Journal on Wireless Communications and Networking (Springer), and Editor of KSII Transactions on Internet and Information Systems.

VARUN G. MENON (Senior Member, IEEE) is currently an Associate Professor with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, India. His research interests include the Internet of Things, fog computing and networking, underwater acoustic sensor networks, cyber psychology, hijacked journals, ad-hoc networks, and wireless sensor networks. He is a Distinguished Speaker of ACM Distinguished Speaker. He is currently a Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE SENSORS JOURNAL, the IEEE Internet of Things Magazine, and the Journal of Supercomputing. He is an Associate Editor of IET Quantum Communications. He is also an Editorial Board Member of the IEEE Future Directions: Technology Policy and Ethics.

SHYNU P. G. received his PhD degree in Computer Science from Vellore Institute of Technology, Vellore, India and Masters in Engineering in Computer Science and Engineering from College of Engineering, Anna University, Chennai, India. He is currently working as Associate Professor in the School of Information Technology and Engineering, VIT University, Vellore, India. He has published over 30 research papers in refereed international conferences and journals. His research interests include Deep Learning, Cloud Security and Privacy, Ad-hoc Networks and Big Data.