Wireless Networks (2022) 28:3157–3172
https://doi.org/10.1007/s11276-022-03024-7

ORIGINAL PAPER

Analysis of secrecy outage performance for full duplex NOMA relay systems with appearance of multiple eavesdroppers

Nguyen Le Cuong[1] · Tran Manh Hoang[2] · Nguyen Thu Phuong[3] · Pham Thanh Hiep[3]

Accepted: 31 May 2022 / Published online: 28 June 2022

Abstract

Full-duplex (FD) relay systems including a transmit antenna selection and a non-orthogonal multiple access (NOMA) methods are analyzed under presence of multiple eavesdroppers. A channel state information of both the considered system and eavesdroppers is assumed to be outdated and eavesdroppers eavesdrop information signals independently. A closed-form of secure outage probability (SOP), secrecy throughput of every user is derived to evaluate the secrecy performance, and the mathematical analysis approach is verified by the Monte-Carlo simulation. Furthermore, the Golden-Section Search algorithm is proposed to find the maximum of the secrecy throughput of the considered FD-NOMA system. Numerical results indicate that there exists the SOP floor in the considered system and it is constrained by the channel gain of near user. Moreover, there is the optimal signal to interference plus noise ratio value which minimizes the SOP of the system regardless of the number of eavesdroppers. In comparison with half-duplex NOMA model, the SOP of FD-NOMA model is better.

Keywords Full-duplex NOMA relay systems · Secrecy outage probability · Self interference cancellation · Multiple non-colluding eavesdroppers

1 Introduction

Nowadays, a non orthogonal multiple access (NOMA), as well known is a promising technique to improve significantly a spectral efficiency for the fifth generation (5G) and beyond (5GB) mobile networks [1–3]. It is to meet the requirement of connection for large multiple users systems and growing demand for the amount of data traffic. The number of devices and connections in wireless networks, as well as the spectrum demand continuously increase. To detect the signals of multiple users with different power levels or codes, a successive interference cancellation (SIC) method is applied to all users [4, 5].

Also, a full-duplex (FD) communication can improve the spectral efficiency by receiving and transmitting simultaneously via the same bandwidth [6–8], furthermore to mitigate the self-interference of the FD model, analog and digital domains cancellation methods are employed. According to a report in [9, 10], the capability mitigation of the self-interference cancellation (IC) can be up to 110 dB. On the other hand, the multi-antenna deployment has improved the system performance, while transmit antenna selection (TAS) can reduce the cost, power consumption and hardware complexity [11]. Combination of TAS and FD can improve the secure performance, because the TAS enhances a signal to noise ratio (SNR) in legitimate channels and the FD provides a higher data rate transmission.

Presently, some works evaluated the performance of FD cooperative NOMA systems as in [12–14]. In these works, the authors derived a closed-form expression of outage probability (OP) and ergodic capacity (EC) of the proposed system. The hybrid half-duplex (HD)/FD cooperative NOMA system was carried out in [15], the optimal power allocation in the sense of maximum EC and minimum OP was derived. The above mentioned works considered simple models and without investigating the secure

✉ Pham Thanh Hiep
phamthanhhiep@gmail.com

1 Electric Power University, Hanoi 100000, Vietnam

2 University of Telecommunications, Nhatrang, Vietnam

3 Le Quy Don Technical University, Hanoi, Vietnam

performance of the system. Meanwhile, wireless networks are especially vulnerable to eavesdrop due to broadcasting signals on wireless channels. Generally, traditional security approaches employ symmetric and asymmetric cryptographic algorithms to achieve secure communications.

Recently, physical layer security (PLS) has attracted attention as a simple method to guarantee secure communications in wireless networks. The basic idea of PLS is that it utilizes physical characteristics of wireless channels to protect the source message against eavesdroppers. The common metric used to evaluate the PLS of wireless communication networks is secrecy capacity, which is defined as the maximal achievable rate at which messages can be reliably sent from a source to a receiver without being decoded by any eavesdropper. In other words, communication data can be theoretically secured without using any traditional cryptographic mechanisms if the condition of legitimate propagation channel is better than that of eavesdroppers [16–18]. The history of PLS can be traced back to Shannon's information theoretic secrecy analysis [16], and then was developed into the work of Wyner on the wiretap channel [17], where two legitimate users communicate over the main channel and an eavesdropper accesses to signals from the illegitimate channel. In [18], Csiszar and Kornor proved that there exist channel codes that guarantee the security of wireless communication networks. Since the 1949s, the PLS of wireless communication systems has been studied. It is studied continuously until now [19–22]. Presently, PLS is still a major problem in the overall structure of wireless networks. Especially, for multi-user systems, where intertwinements between legitimate users may have occurred, the PLS has attracted more attention.

The study on PLS for NOMA systems has been presented in many literatures [23–26], where each work considered a different aspect. The work in [23] investigated a secrecy outage probability (SOP) of far and near users, where signals are transmitted by a base station via the FD relay and the direct link. In this scenario, the authors considered the case of the presence of only one eavesdropper. To improve the secure performance of NOMA systems, the authors in [24] use a jammer to an eavesdropper appearance in the uplink channel, as such the configuration of the system consists of multi-user, one BS and one eavesdropper. This is the simplified scenario investigated with external eavesdropper in communication links from users to the BS. The impact of imperfect CSI on PLS of NOMA system is considered by the authors in [25], this word proposed an algorithm to optimize the power allocation for the transmitter in the sense of minimum OP and SOP. The work carried out in this scenario is that the authors only considered the secrecy of NOMA downlink signals with the appearance of one eavesdropper. Similar to investigation of SOP for the NOMA downlink in [25], the authors in [27] considered the secrecy performance of NOMA downlink with two users. The decoding capability of eavesdroppers is investigated in two case, i.e., perfect and imperfect received signals.

Based on the summarization mentioned above, we know that these works considered the system with an HD model and one eavesdropper, most of them refer to the case of point-to-point communication. Therefore, we are going to propose an idea that close to the work in [26]. In this model, the authors proposed a system, where the best relay with HD model forwards signals to two users by the NOMA scheme, and another relay is selected as a jammer to one eavesdropper. A major problem with this scheme is the interference between relays, cancellation of interference of each relay is very difficult and lets hardware complexity increase.

To the best of our knowledge, the system with the TAS algorithm at the source, the NOMA scheme at FD relay and multiple eavesdroppers, is not taken into consideration in any literature. Motivated by the general problem of securing propagation over wireless channels, in this paper, we mainly focus on the SOP of the TAS-FD-NOMA system with multiple eavesdroppers. The effect of channel state information (CSI) on the TAS scheme is discussed when the CSI between the desired devices is assumed to be outdated, whereas the CSI between the relay and eavesdroppers is unknown. Because the relay doesn't know the CSI, several techniques to improve the secrecy performance such as artificial noise, beamforming and jamming are unsuitable to use in our work.

The contributions of this paper are summarized as follows:

- We propose and analyze the SOP of FD-NOMA system with multiple eavesdroppers overhearing the information of two users. To improve the secure performance, the source is equipped with multiple antennas and the TAS scheme. To investigate the proposed system in a practical scenario, the non-colluding multiple eavesdroppers are considered, it can be found in Internet of Things (IoT) and future wireless networks [28].
- We analyze the security of FD-NOMA relay system by deriving the closed-form expression of SOP, and provide insights of the SOP over Rayleigh fading channel propagation condition, the outdated CSI for TAS scheme and the imperfect CSI at eavesdroppers. The theoretical analysis is validated via simulations.
- Instead of consideration of the secrecy capacity, we investigate the secrecy throughput of the FD-NOMA system. We propose to utilize the Golden-Section Search algorithm to find the maximum of the secrecy throughput. Two lemmas are proved to explain

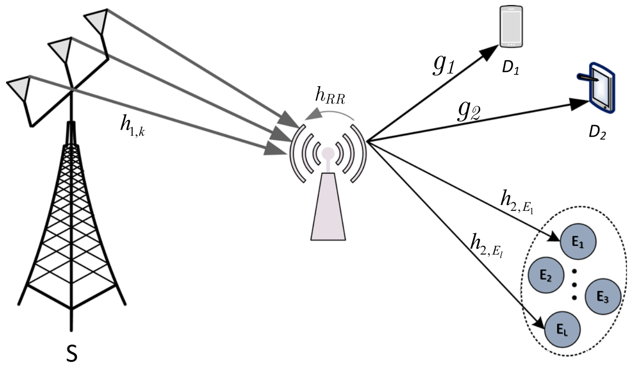


Fig. 1 System model of the considered FD-NOMA relay system with multiple non-colluding eavesdroppers

the property of our work, and they also can be applied for investigating another work.

- We propose the FD model at the relay to improve the data rate of legitimate channel, and then the FD model is compared with the HD model based on the SOP performance of the proposed system.
- The performance of the proposed system is investigated based on the number of antennas of the source, the self interference cancellation coefficients at the full-duplex devices and the transmission power.

The rest of the paper is organized as follows. Section 2 describes the system model, and Sect. 3 presents the detailed analysis of the considered FD-NOMA relay system. The main results and their implications are discussed in detail in Sect. 5. Finally, Sect. 6 concludes the paper.

2 FD-NOMA relay systems with multiple non-colluding eavesdroppers

2.1 System model

In this paper, the downlink FD-NOMA relay system as illustrated in Fig. 1 is investigated. The source (S) is equipped with K antennas, and transmits its data to two legitimate end-users (D_i) with the assistance of the relay R which utilizes the decode-and-forward (DF) scheme in the FD model. As the same with the work in [26], we assume that the direct link is unavailable due to long distance, blockage and shadowing. Furthermore, only two end-users are considered because the degradation of system performance is proportional to the number of users due to applying SIC [29]. The system also includes overhearing attacks of multi-malicious eavesdroppers, $\mathrm{E}_l, l \in \{1, 2, \ldots, L\}$.[1] The relay node is equipped with two antennas for the active FD mechanism. The advantage of this mechanism is self-interference cancellation at the antenna domain, because of natural isolation which arises from the sheer physical distance between transmit and receive antennas, and rational installation guarantee obstacles between transmit and receive antennas to block the line-of-sight signal. Whereas, due to the limitation of the size, users and eavesdroppers have only one antenna, which is the same configuration in [24–26].

All the channels are assumed to follow the Rayleigh fading block model. Let's $h_{1,k} \sim \mathcal{CN}(0, \Omega_{\mathrm{SR}})$ and $h_{2,E_l} \sim \mathcal{CN}(0, \Omega_{\mathrm{RE}})$ denote the channel fading (including large-scale and small-scale) coefficient of propagation channel from antennas of the S to the relay and from the relay to eavesdroppers, respectively. Moreover, $\tilde{g}_i$ represents the channel fading coefficient of channel between the best relay and the i^{th} user, i.e. $g_i = \tilde{g}_i\sqrt{d_i^{-\alpha}}$, then $g_i \sim athcalCN(0, \Omega_{\mathrm{RD}_i})$, where $i \in \{1, 2\}$ and $\Omega_{\mathrm{RD}_i} = \mathbb{E}\{|g_i|^2\}$, d_i is the distance between the best relay and D_i, and α is the path-loss coefficient. Without loss of generality, it is assumed that the channel gains are sorted according to an ascending order $|g_2|^2 < |g_1|^2$.

On the other hand, we also denote $h_{\mathrm{RR}} \sim \mathcal{CN}(0, \Omega_{\mathrm{RR}})$ as the channel fading coefficient between the transmit antenna and the receiver antenna of the relay, thus $|h_{\mathrm{RR}}|^2$ is exponentially distributed with $\mathbb{E}\{|h_{\mathrm{RR}}|^2\} = \Omega_{\mathrm{RR}}$, which is closely related to the strength of the loop-back interference.

The additive white Gaussian noise (AWGN) at each receiver is represented by $w_{\mathcal{A}} \sim \mathcal{CN}(0, \sigma^2_{\mathcal{A}})$, $\mathcal{A} \in \{\mathrm{R}, \mathrm{E}, D_i\}$, in which $\sigma^2_{\mathcal{A}}$ is the noise variance. In this paper, we assume that the CSI is perfect at the receiver. In contrast, the feedback CSI from the R to the S is outdated, and channels estimation at eavesdroppers is imperfect due to the R doesn't know the channel from itself to eavesdroppers.[2] Thus, the estimated channel of R-E_l can be represented via actual and estimation error channels as

$$h_{2,E_l} = \hat{h}_{2,E_l} + \epsilon_{E_l}, \tag{1}$$

where, $\epsilon_{E_l} \sim \mathcal{CN}(0, \sigma^2_{\mathrm{E}_l})$ and $\hat{h}_{2,E_l} \sim \mathcal{CN}(0, \hat{\Omega}_{\mathrm{RE}})$ denote the coefficient of the estimation error and actual channels between R-E_l, respectively. According to [30, 31], $\hat{\Omega}_{\mathrm{RE}} = \Omega_{\mathrm{RE}} - \sigma^2_{\mathrm{E}_l}$ is the normalized channel gain of $\hat{h}_{2,E_l}$, which is statistically independent of ϵ_{E_l}. On the other hand, we

[1] It is noticed that even when the $\mathrm{S}-\mathrm{E}_l$ or $\mathrm{S}-\mathrm{D}_i$ link is available, E_l and D_i can't retrieve the confidential information. The reason is, they receive different signals from the S and the R_b in the same time, and hence they can't distinguish the confidential information from interference.

[2] In a practical system, the transmission node obtains the CSI by the uplink channel from users to the source using channel estimation methods, while eavesdroppers don't know training pilots. Moreover, the signal constellation mapping is unavailable at the eavesdroppers node, it is only available at the legitimate node.

assumed that ρ_{E_l}, $0 \le \rho_{E_l} \le 1$ is the correlation coefficient of channel estimation error, which indicates the difference between the actual and estimated channel. Moreover, the normalized variance of the estimation error is $\sigma^2_{E_l} = \rho_{E_l}\Omega_{RE}$, thus, we have $\hat{\Omega}_{RE} = (1-\rho_{E_l})\Omega_{RE}$.

The transmit antenna selection (TAS) scheme can reduce the power consumption and complexity of wireless systems because only one RF chain is used, hence the TAS is applied to the S.[3] The operation of the TAS scheme can be summarized as follows. First, the S sends the pilot sequence one-by-one to the R for the channel estimation. After that the R selects a transmit antenna associated with the best instantaneous SNR, and gives feedback with the index of the selected antenna to the S. This feedback information can be presented by a binary vector with the number of bits $b = \log_2 N$.

2.2 Calculation of transmission rate

Due to the time-varying characteristics of S – R channel, its coherent time may be altered when the feedback delay is larger than the transmission block period *T*. Consequently, the feedback information of CSI for the selected antenna is outdated at the S. Mathematically, we have signal to noise ratio (SNR) of TAS scheme as

$$\gamma_{SR} = \arg \max_{k=1\div K} \gamma_{1,k}. \tag{2}$$

Let's denote $\rho_{1,k}$ as the correlation coefficients between the actual channel, $\hat{h}_{1,k}$, and the estimated channel, $h_{1,k}$. For simplicity, we assume that the correlation coefficients $\rho_{1,k}$, $k = 1, \cdots, K$ is the same, i.e., $\rho_{1,k} = \rho$, with $k = 1, 2, \cdots, K$. By using Markov chain, the relationship of $h_{1,k}$ and $\hat{h}_{1,k}$ can be modeled by the correlation coefficient ρ as

$$h_{1,k} = \rho\hat{h}_{1,k} + \sqrt{1-\rho^2}e_{1,k}, \tag{3}$$

where $e_{1,k}$ is an error term due to outdated changes and is modeled by a circular symmetric complex Gaussian random variable, i.e., $e_{1,k} \sim \mathcal{CN}(\mu, \sigma^2)$. The coefficient ρ, $0 \le \rho \le 1$, depends only on the time delay and can be considered as the measurement of the channel fluctuation rate. To reduce the complexity of mathematical equations, we denote $X = \arg\max_{k=1\div K} |h_{1,k}|^2$ in the following analysis.

Remark 1 According to [32], a probability density function (PDF) of SNR of $S-R$ link with the TAS scheme in the case of outdated CSI is given by

$$f_X(x) = \sum_{k=1}^{K} \binom{K}{k} \frac{(-1)^{k-1}k}{\Omega_{SR}\Delta(\rho)} \exp\left(-\frac{kx}{\Omega_{SR}\Delta(\rho)}\right), \tag{4}$$

where $\Delta(\rho) = 1 + (k-1)(1-\rho^2)$.

From (4), a cumulative distribution function (CDF) of X is expressed as follows.

$$F_X(x) = \sum_{k=1}^{K} \binom{K}{k} (-1)^{k-1} \left[1 - \exp\left(-\frac{kx}{\Omega_{SR}\Delta(\rho)}\right)\right]. \tag{5}$$

Based on the property of CDF, i.e., $F_X(\infty) = 1$, then when $x \to \infty$ in (5), $\sum_{k=1}^{K} \binom{K}{k} (-1)^{k-1} = 1$. Thus, we can rewrite (5) as

$$F_X(x) = 1 - \sum_{k=1}^{K} \binom{K}{k} (-1)^{k-1} \exp\left(-\frac{kx}{\Omega_{SR}\Delta(\rho)}\right). \tag{6}$$

Proof of Remark 1 is depicted in [32].

The PDF in (4) and the CDF in (6) are probability functions which model the statistical channel gain between S - R link with the outdated CSI. From these equations, we can recognize that when the CSI is outdated, the variance of channel fading amplitude increases, and then the received SINR is decreased.

We assume that the relay processes the received signal within one time slot, thus the signal which is transmitted at the relay is the received signal from the source in the previous slot. The signal of D_1 and D_2 is respectively denoted by x_1 and x_2, then the received signal at the relay in the FD model is represented by

$$y_R = h_{SR}(\sqrt{a_1 P_S}x_1 + \sqrt{a_2 P_S}x_2) + \sqrt{\eta P_R}x_R h_{RR} + w_R, \tag{7}$$

where $h_{SR} = \arg\max_{k=1\div K} h_{1,k}$ is the channel fading coefficient from the selected antenna of S to the R. a_1 and a_2 denote the power allocation coefficients for the x_1 and x_2 signals, respectively with $a_1 + a_2 = 1$. Following the principle of NOMA, to achieve the boundary of the user capacity, let $a_2 > a_1$.[4]

The coefficient of residual self interference cancellation (RSIC) is denoted by η, it represents the remaining self-interference after cancellation process, and depends on the quality of designing FD self interference mitigation. To notice that the component $\sqrt{\eta P_R}x_R h_{RR}$ will be subtracted by the self-interference cancellation techniques such as antenna isolation, analog and digital domain suppression.

Furthermore, according to the NOMA principle, the relay R performs a successive interference cancellation (SIC) for the x_2, and then detect the x_1. That is, the R decodes the signal x_2 while treating the x_1 as interference,

[3] Instead of TAS scheme, the other schemes such as selecting several antennas, varying the number of antennas or constructing beamforming at the S to improve the secrecy performance are considered in our future works.

[4] Power allocation depends on the targeted point on the capacity region of the users scheduled in one cluster [33].

then removes the x_2 from the received signal and decodes the x_1. Thus SINR at the R of x_1 and x_2 in the case of perfect SIC[5] is given as

$$\gamma_{\mathrm{R}}^{x_1} = \frac{a_1 P_{\mathrm{S}} |h_{\mathrm{SR}}|^2}{\eta P_{\mathrm{R}} |h_{\mathrm{RR}}|^2 + \sigma_{\mathrm{R}}^2}, \tag{8}$$

$$\gamma_{\mathrm{R}}^{x_2} = \frac{a_2 P_{\mathrm{S}} |h_{\mathrm{SR}}|^2}{a_1 P_{\mathrm{S}} |h_{\mathrm{SR}}|^2 + \eta P_{\mathrm{R}} |h_{\mathrm{RR}}|^2 + \sigma_{\mathrm{R}}^2}. \tag{9}$$

After successfully decoding, the R re-encodes the x_1 and x_2, $\sqrt{a_1 P_{\mathrm{R}}} x_1 + \sqrt{a_2 P_{\mathrm{R}}} x_2$, to transmit to the D_1 and D_2 in the next time slot. Thus, the received signal at the D_1 and D_2 is given as

$$y_{\mathrm{D}_1} = g_1 (\sqrt{a_1 P_{\mathrm{R}}} x_1 + \sqrt{a_2 P_{\mathrm{R}}} x_2) + w_{\mathrm{D}_1}, \tag{10}$$

$$y_{\mathrm{D}_2} = g_2 (\sqrt{a_1 P_{\mathrm{R}}} x_1 + \sqrt{a_2 P_{\mathrm{R}}} x_2) + w_{\mathrm{D}_2}. \tag{11}$$

Similar to the SIC method at the R, the D_1 firstly detects and subtracts the x_2 based on the SIC structure, and then decodes the x_1, while the D_2 decodes its own signal with considering the x_1 as interference. Thus, the SINR at the D_1 and D_2 is given as

$$\gamma_{\mathrm{D}_1}^{x_2} = \frac{a_2 P_{\mathrm{R}} |g_1|^2}{a_1 P_{\mathrm{R}} |g_1|^2 + \sigma_{\mathrm{D}_1}^2}, \tag{12}$$

$$\gamma_{\mathrm{D}_1}^{x_1} = \frac{a_1 P_{\mathrm{R}} |g_1|^2}{\sigma_{\mathrm{D}_1}^2}, \tag{13}$$

$$\gamma_{\mathrm{D}_2}^{x_2} = \frac{a_2 P_{\mathrm{R}} |g_2|^2}{a_1 P_{\mathrm{R}} |g_2|^2 + \sigma_{\mathrm{D}_2}^2}. \tag{14}$$

Due to the broadcast property of the signals in wireless environment, the received signal of the eavesdropper E_l is given as follows.

$$y_{\mathrm{E}_l} = h_{2,\mathrm{E}_l} (\sqrt{a_1 P_{\mathrm{R}}} x_1 + \sqrt{a_2 P_{\mathrm{R}}} x_2) + w_{\mathrm{E}_l}. \tag{15}$$

In the case of non-colluding, every eavesdropper processes the received signal independently, overhearing is successful if one of them can detect the signal. Therefore, the channel of the best one in the set of eavesdroppers is taken into account, that means the channel gain between the R and eavesdroppers is the best one in all of eavesdroppers, $h_{2,\mathrm{E}} = \max_{l=1 \div L} h_{2,\mathrm{E}_l}$. Similar to [34–36], we consider the worst-case, i.e., the eavesdropper can detect the signal powerfully, it can detect the x_1 (or the x_2) without being interfered by the x_2 (or the x_1), and then the maximal SNR of received signals at eavesdroppers is given as

$$\gamma_{\mathrm{E}}^{x_i} = \frac{a_i P_{\mathrm{R}}}{\sigma_{\mathrm{E}_l}^2} |h_{2,\mathrm{E}}|^2, \quad i \in \{1, 2\}. \tag{16}$$

Since the DF protocol is applied to the R, the end-to-end transmission rate of x_1 and x_2 over legitimate channels equals the lowest rate of all transmitted hops from the S to the end-user. Consequently, it can be calculated by the minimum SINR of all related nodes as follows.

$$\mathrm{C}^{x_1} = \log_2 \left(1 + \min\{\gamma_{\mathrm{R}}^{x_1}, \gamma_{\mathrm{D}_1}^{x_1}\}\right), \tag{17}$$

$$\mathrm{C}^{x_2} = \log_2 \left(1 + \min\{\gamma_{\mathrm{R}}^{x_2}, \underbrace{\gamma_{\mathrm{D}_1}^{x_2}}_{\mathrm{SIC}}, \gamma_{\mathrm{D}_2}^{x_2}\}\right). \tag{18}$$

On the other hands, the rate of x_1 and x_2 over wiretap channels is given as

$$\mathrm{C}_{\mathrm{E}}^{x_i} = \log_2 \left(1 + \gamma_{\mathrm{E}}^{x_i}\right), i \in \{1, 2\}. \tag{19}$$

To notice that the secrecy capacity is denoted as the gap of capacity between legitimate and eavesdropping channels [19, 23], i.e., $\mathrm{C}^{\mathrm{sec}} = [\mathrm{C}^{x_i} - \mathrm{C}_{\mathrm{E}}^{x_i}]^+$. In order to evaluate the secrecy capacity $\mathrm{C}^{\mathrm{sec}}$, we estimate the instantaneous capacity of legitimate and eavesdropping channels, it is described in detail in Sect. 4.

3 Performance analysis of SOP

In this section, we provide the closed-form expressions of the SOP from the S to the D_i of the system. The SOP is defined by the probability that the end-to-end secrecy capacity is lower than the given positive secure transmission rate [26].

$$\mathrm{SOP}^{x_i} = \Pr\left([\mathrm{C}^{x_i} - \mathrm{C}_{\mathrm{E}}^{x_i}]^+ < r_i\right), \tag{20}$$

where $[x]^+ = \max\{0, x\}$, where, C^{x_i} and $\mathrm{C}_{\mathrm{E}}^{x_i}$ given in (17), (18) and (19) are, respectively. $r_i = r_b - r_e$ is also called the transmission rate of confidential data, r_b denotes the codeword rate of the legitimate channel while r_e is the equivocation rate of the eavesdropping channel. It indicates that, smaller r_i leads to smaller SOP, smaller r_b and higher r_e.

As evaluation in [23, 37], the received signals x_1 and x_2 at eavesdroppers are different, thus we investigate the SOP of x_1 and x_2 separately.

3.1 Secrecy outage probability of x_1

The SOP of x_1 is defined as the probability that the instantaneous secrecy capacity of x_1, i.e. $[\mathrm{C}^{x_1} - \mathrm{C}_{\mathrm{E}}^{x_1}]^+$, is below the predefined threshold value of secure transmission rate, r_1. The SOP of x_1 is given as in Proposition 1.

[5] The target of this paper is investigating the impact of the channel conditions and non-colluding of eavesdroppers on the SOP of the system. The imperfect SIC is the practical scenario, however we are going to consider it in future works.

Proposition 1 *The SOP of x_1 in the TAS - FD - NOMA relay system under the condition of outdated CSI at the S and imperfect CSI at the eavesdropper is given as*

$$\mathrm{SOP}^{x_1} = 1 - \sum_{k=1}^{K}\sum_{l=1}^{L}(-1)^{k+l-2}\binom{K}{k}\binom{L}{l}\frac{lP_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}{\beta P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\frac{\exp\left(\frac{(1-\gamma_{\mathrm{th}})}{a_1\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}}+\frac{1-\gamma_{\mathrm{th}}}{a_1P_{\mathrm{R}}\Omega_{\mathrm{RD}_1}}\right)}{\mathcal{A}_2+\mathcal{A}_3+\mathcal{A}_4}, \tag{21}$$

where

$$\gamma_{\mathrm{th}} = 2^{r_1}, beta = \Omega_{\mathrm{RR}}k\eta P_{\mathrm{R}}(\gamma_{\mathrm{th}}-1) + a_1\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}},$$
$$\mathcal{A}_2 = \frac{\gamma_{\mathrm{th}}\Omega_{\mathrm{RR}}k\eta P_{\mathrm{R}}}{\beta}, \mathcal{A}_3 = \frac{k\gamma_{\mathrm{th}}}{a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}+\frac{\gamma_{\mathrm{th}}}{a_1P_{\mathrm{R}}\Omega_{\mathrm{RD}_1}},$$
$$\mathcal{A}_4 = \frac{l}{a_1P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}.$$

From (21), we can recognize that the average channel gain between the R and eavesdroppers, $\hat{\Omega}_{\mathrm{RE}}$, the channel gain of self - interference, Ω_{RR}, and the outdated CSI, $\Delta(\rho)$, linearly influence the SOP of x_1. Moreover, the number of relay nodes, K, and the number of eavesdroppers, L, also impact on the secrecy performance. From (17) and (20) we can rewrite SOP of x_1 as

$$\begin{aligned}\mathrm{SOP}^{x_1} &= \Pr\left([\mathrm{C}^{x_1}-\mathrm{C}_{\mathrm{E}}^{x_1}]^+ < r_1\right)\\ &= \Pr\left(\log_2\left[\frac{1+\gamma_1}{1+\gamma_{\mathrm{E}_l}^{x_1}}\right] < r_1\right)\\ &= \Pr\left(\frac{1+\gamma_1}{1+\gamma_{\mathrm{E}_l}^{x_1}} < 2^{r_1}\right)\\ &= \int_0^\infty \Pr\left(\gamma_1 < 2^{r_1}(1+x)-1\right)f_{\gamma_{\mathrm{E}_l}^{x_1}}(x)dx.\end{aligned} \tag{22}$$

To obtain the closed-form for (22), we derive the CDF and PDF of γ_1 and $\gamma_{\mathrm{E}}^{x_1}$ with respect to x variable. From (16), we have the PDF of $\gamma_{\mathrm{E}}^{x_i}$ as

$$f_{\gamma_{\mathrm{E}}^{x_i}}(x) = \sum_{l=1}^{L}\binom{L}{l}\frac{(-1)^{l-1}l}{a_iP_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\exp\left(-\frac{lx}{a_iP_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\right), \tag{23}$$

where $i \in \{1,2\}$.

Let $\gamma_1 = \min\{\gamma_{\mathrm{R}}^{x_1}, \gamma_{\mathrm{D}_1}^{x_1}\}$ and $y = 2^{r_1}(1+x)-1$, and after some manipulations, the CDF of γ_1 can be given as

$$F_{\gamma_1}(x) = 1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\exp(\mathcal{A}_1)\frac{a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}{\beta}\frac{1}{1+\mathcal{A}_2x}\exp(-\mathcal{A}_3x). \tag{24}$$

The detail of proof for (24) is presented in the Appendix A. Note that in the case of small $\mathcal{A}_2$, we can approximate by Taylor expansion as $\frac{1}{1+\mathcal{A}_2x} \to \exp(-\mathcal{A}_2x)$. Replace (24) and (23) into (22), the SOP of x_1 is rewritten as follows.

$$\begin{aligned}\mathrm{SOP}^{x_1} = &1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\sum_{l=1}^{L}(-1)^{l-1}\binom{L}{l}\\ &\frac{la_1\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}}{\beta a_1P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\exp(\mathcal{A}_1)\\ &\times\int_0^\infty \exp[-x(\mathcal{A}_2+\mathcal{A}_3+\mathcal{A}_4)]dx.\end{aligned} \tag{25}$$

Using [38, eq. (3.310. 11)], we have the closed-form expression of SOP^{x_1} as shown in (21).

3.2 Secrecy outage probability of x_2

The SOP of x_2 is defined as the probability that the instantaneous secrecy capacity of x_2 is below the predefined threshold value of secure transmission rate, r_2. In the NOMA scheme, the secrecy capacity of x_2 is different from that of x_1, because the signal detection in the NOMA technique must use the SIC operation. Thus, from (9), (12) and (14), the end-to-end SINR of x_2 can be modeled as an equivalent single hop whose output SINR is presented as $\gamma_2 = \min\{\gamma_{\mathrm{R}}^{x_2}, \gamma_{\mathrm{D}_1}^{x_2}, \gamma_{\mathrm{D}_2}^{x_2}\}$, which is dominated by the weakest case. Thus we have Proposition 2 providing the SOP of x_2 as follows.

Proposition 2 *With the outdated CSI at the S and error CSI at the eavesdroppers, the SOP of x_2 in the TAS-FD-NOMA relay system is given as*

$$\begin{aligned}\mathrm{SOP}^{x_2} = &1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\sum_{l=1}^{L}(-1)^{l-1}\binom{L}{l}\\ &\times\frac{l}{a_2P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\frac{\Delta\pi}{2N}\sum_{n=1}^{N}\frac{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}(a_2-a_1\chi_u)}{\chi_u\xi+\Omega_{\mathrm{SR}}\Delta(\rho)a_2P_{\mathrm{S}}}\sqrt{1-\phi_n^2}\\ &\times\exp\left(-\frac{k\chi_u}{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}(a_2-a_1\chi_u)}-\frac{l\chi_u}{a_2P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\right)\\ &\times\exp\left(-\frac{\chi_u}{\Omega_{\mathrm{RD}_1}P_{\mathrm{R}}(a_2-a_1\chi_u)}-\frac{\chi_u}{\Omega_{\mathrm{RD}_2}P_{\mathrm{R}}(a_2-a_1\chi_u)}\right),\end{aligned} \tag{26}$$

where $\Delta = \frac{1-\gamma_{\rm th}a_1}{a_1\gamma_{\rm th}}$, $\gamma_{\rm th} = 2^{r_2}$, $\xi = (k\eta P_{\rm R}\Omega_{\rm RR} - \Omega_{\rm SR}\Delta(\rho) a_1 P_{\rm S})$ and $u = \frac{\Delta}{2}\left[\phi_n + 1\right]$ with $\phi_n = \cos\left(\frac{(2n-1)\pi}{2N}\right)$.

As the same with conclusion for Proposition 1, we also recognize clearly that the power allocation coefficient, a_1 and a_2, significantly impacts on the secrecy performance. Thus, in the NOMA scheme, the suitable power allocation coefficient should be used to improve the rate of D_i. From (18) and (20), we can rewrite the SOP of x_2 as follows.

$$\begin{aligned}\mathrm{SOP}^{x_2} &= \Pr\left([C^{x_2} - C_{\rm E}^{x_2}]^+ < r_2\right)\\ &= \Pr\left(\log_2\left[\frac{1+\gamma_2}{1+\gamma_{\rm E_l}^{x_2}}\right] < r_2\right)\\ &= \Pr\left(\frac{1+\gamma_2}{1+\gamma_{\rm E_l}^{x_2}} < 2^{r_2}\right)\\ &= \int_0^\infty \Pr\left(\gamma_2 < 2^{r_2}(1+x) - 1\right) f_{\gamma_{\rm E_l}^{x_2}}(x)dx.\end{aligned} \tag{27}$$

In oder to derive the closed-form expression for (27), firstly the CDF of γ_2 and the PDF of $\gamma_{\rm E}^{x_2}$ is proposed. From (9), (12) and (14), we have γ_2 as in (28).

$$\gamma_2 = \min\left\{\frac{a_2 P_{\rm S}|h_{\rm SR}|^2}{a_1 P_{\rm S}|h_{\rm SR}|^2 + \eta P_{\rm R}|h_{\rm RR}|^2 + \sigma_{\rm R}^2}, \frac{a_2 P_{\rm R}|g_1|^2}{a_1 P_{\rm R}|g_1|^2 + \sigma_{\rm D_1}^2}, \frac{a_2 P_{\rm R}|g_2|^2}{a_1 P_{\rm R}|g_2|^2 + \sigma_{\rm D_2}^2}\right\}, \tag{28}$$

According to (28), we have the CDF of γ_2 as given in (29) and (30), and its derivation is provided in detail in Appendix B.

$$F_{\gamma_2}(y) = 1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\frac{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1 y)}{y(k\eta P_{\rm R}\Omega_{\rm RR} - \Omega_{\rm SR}\Delta(\rho)a_1 P_{\rm S}) + \Omega_{\rm SR}\Delta(\rho)a_2 P_{\rm S}} \times \exp\left(-\frac{ky}{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1 y)}\right) \times \exp\left(-\frac{y}{\Omega_{\rm RD_1}P_{\rm R}(a_2 - a_1 y)} - \frac{y}{\Omega_{\rm RD_2}P_{\rm R}(a_2 - a_1 y)}\right), \quad \text{if } y < \frac{a_2}{a_1} \tag{29}$$

$$1, \quad \text{if } y \geq \frac{a_2}{a_1}. \tag{30}$$

Then, replace (29) and (23) into (27), we can rewrite the SOP of x_2 as follows.

$$\mathrm{SOP}^{x_2} = 1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\sum_{l=1}^{L}(-1)^{l-1}\binom{L}{l}\underbrace{\frac{l}{a_2 P_{\rm R}\hat{\Omega}_{\rm RE}}\int_0^\Delta \Psi(\chi_x)\exp\left(-\frac{lx}{a_2 P_{\rm R}\hat{\Omega}_{\rm RE}}\right)dx}_{\mathcal{W}(u)}, \tag{31}$$

where $\Delta = \frac{1-\gamma_{\rm th}a_1}{a_1\gamma_{\rm th}}$, $\chi_x = \gamma_{\rm th} + \gamma_{\rm th}x - 1$ and $\gamma_{\rm th} = 2^{r_2}$,

$$\Psi(\chi_x) = \frac{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1\chi_x)}{\chi_x\xi + \Omega_{\rm SR}\Delta(\rho)a_2 P_{\rm S}}\exp\left(-\frac{k\chi_x}{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1\chi_x)}\right) \times \exp\left(-\frac{\chi_x}{\Omega_{\rm RD_1}P_{\rm R}(a_2 - a_1\chi_x)} - \frac{\chi_x}{\Omega_{\rm RD_2}P_{\rm R}(a_2 - a_1\chi_x)}\right), \tag{32}$$

with $\xi = k\eta P_{\rm R}\Omega_{\rm RR} - \Omega_{\rm SR}\Delta(\rho)a_1 P_{\rm S}$ and $f_{\gamma_{\rm E}^{x_2}}(x)$ is presented in (23).

The integral in (31) is very difficult to obtain the closed-form expression, therefore the approximation by using Gaussian–Chebyshev quadrature [39, eq: (25.4.30)] is applied to obtain the expression of $\mathcal{W}(u)$ as

$$\mathcal{W}(u) = \frac{\Delta}{2}\sum_{n=1}^{N}\frac{\pi}{N}\frac{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1\chi_u)}{\chi_u\xi + \Omega_{\rm SR}\Delta(\rho)a_2 P_{\rm S}}\sqrt{1-\phi_n^2} \times \exp\left(-\frac{k\chi_u}{\Omega_{\rm SR}\Delta(\rho)P_{\rm S}(a_2 - a_1\chi_u)} - \frac{l\chi_u}{a_2 P_{\rm R}\hat{\Omega}_{\rm RE}}\right) \times \exp\left(-\frac{\chi_u}{\Omega_{\rm RD_1}P_{\rm R}(a_2 - a_1\chi_u)} - \frac{\chi_u}{\Omega_{\rm RD_2}P_{\rm R}(a_2 - a_1\chi_u)}\right), \tag{33}$$

where u and ϕ_n are provided in Proposition 2.

Remark 2 According to [40], we assume that the R, D_1 and D_2 perform the SIC operation perfectly, the eavesdroppers have enough capability to detect multiuser data, the secrecy outage of x_1 is independent of x_2. This means that the SOP of x_1 has no effect on the SOP of x_2. Thus the SOP for which the eavesdroppers can detect at least one of x_1 and x_2 can be given as

$$\begin{aligned}\mathrm{SOP} &= \Pr\left(\min\{[C^{x_1} - C_{\rm E}^{x_1}], [C^{x_2} - C_{\rm E}^{x_2}]\} \leq r_i\right)\\ &= 1 - \Pr\left([C^{x_1} - C_{\rm E}^{x_1}] > r_i, [C^{x_2} - C_{\rm E}^{x_2}] > r_i\right)\\ &= 1 - (1 - \mathrm{SOP}^{x_1})(1 - \mathrm{SOP}^{x_2})\\ &= \mathrm{SOP}^{x_1} + \mathrm{SOP}^{x_2} - \mathrm{SOP}^{x_1}\mathrm{SOP}^{x_2}.\end{aligned} \tag{34}$$

The *SOP* in (34) is the security outage probability of the system when eavesdroppers can overhear x_1 and/or x_2

successfully, it is represented by the SOP of x_1 and the SOP of x_2.

Remark 3 In case the eavesdropper can decode successfully the signals x_1 and x_2, they can detect both the x_1 and x_2. It means that the secure transmission rate of the strongest user is less than the certain threshold rate r_i. Thus, we have the mathematical form as follows.

$$\begin{aligned}\mathrm{SOP} &= \Pr\Big(\max\{[\mathrm{C}^{x_1}-\mathrm{C}_{\mathrm{E}}^{x_1}],[\mathrm{C}^{x_2}-\mathrm{C}_{\mathrm{E}}^{x_2}]\}<r_i\}\Big)\\ &= \Pr\Big([\mathrm{C}^{x_1}-\mathrm{C}_{\mathrm{E}}^{x_1}]<r_i,[\mathrm{C}^{x_2}-\mathrm{C}_{\mathrm{E}}^{x_2}]<r_i\}\Big)\\ &= \Pr\left(\frac{1+\gamma_1}{1+\gamma_{\mathrm{E}_l}^{x_1}}<r_i,\frac{1+\gamma_2}{1+\gamma_{\mathrm{E}_l}^{x_2}}<r_i\right)\\ &= \Pr\left(\frac{1+\gamma_1}{1+\gamma_{\mathrm{E}_l}^{x_1}}<r_i\right)\Pr\left(\frac{1+\gamma_2}{1+\gamma_{\mathrm{E}_l}^{x_2}}<r_i\right).\end{aligned} \tag{35}$$

It is rewritten via SOP^{x_1} and SOP^{x_2} by

$$\mathrm{SOP} = \mathrm{SOP}^{x_1}\mathrm{SOP}^{x_2}. \tag{36}$$

The SOP in (36) is the security outage probability of the system when eavesdroppers can overhear both the x_1 and x_2 successfully, it is a special case of the SOP in (34).

4 Performance analysis of secrecy throughput

When the codeword is long enough (i.e., its duration is larger than the channel coherence time), the ergodic capacity should be used as a performance metric. In contrast, when the codeword is short (i.e., its duration is less than the channel coherence time), the throughput should be used instead of the ergodic capacity. Assuming that the signals x_1 and x_2 are transmitted with rates of r_1 and r_2, respectively. The secrecy throughput of FD-NOMA relay system can be determined as

$$\begin{aligned}\tau(r) = &\underbrace{\sum_{i=1}^{2} r_i \Pr(\log_2(1+\gamma_{\mathrm{e2e}}^{x_i})>r_i)}_{J_1}\\ &-\underbrace{\sum_{i=1}^{2} r_i \Pr(\log_2(1+\gamma_{\mathrm{E}}^{x_i})>r_i)}_{J_2},\ i\in\{1,2\},\end{aligned} \tag{37}$$

where $\gamma_{\mathrm{e2e}}^{x_1}=\min\{\gamma_{\mathrm{R}}^{x_1},\gamma_{\mathrm{D}_1}^{x_1}\}$ and $\gamma_{\mathrm{e2e}}^{x_2}=\min\{\gamma_{\mathrm{R}}^{x_2},\gamma_{\mathrm{D}_1}^{x_2},\gamma_{\mathrm{D}_2}^{x_2}\}$.

Remark 4 Equation (37) indicates that a very high code rate r_i lets the probability of successfully decoding signals and the secrecy throughput of system be lower. In contrast, low r_i results in high probability of successfully decoding signals, however the throughput may not be high as expected because of the low r_i. According to the NOMA principle, the secrecy throughput of the considered NOMA-FD system can be rewritten as

$$\tau(r) = r_1(1-\mathrm{SOP}^{x_1}) + r_2(1-\mathrm{SOP}^{x_2}). \tag{38}$$

It is noticed that, the secrecy throughput is a function of transmission rate. Thus, the optimal transmission rate that maximizes the secrecy throughput of each NOMA user needs to be found. From (37), for a given transmission power, J_1 can be calculated as

$$\begin{aligned}J_1 = &\underbrace{r_1\Pr(\log_2(1+\gamma_{\mathrm{e2e}}^{x_1})>r_1)}_{Q_1}\\ &+\underbrace{r_2\Pr(\log_2(1+\gamma_{\mathrm{e2e}}^{x_2})>r_2)}_{Q_2}.\end{aligned} \tag{39}$$

Replacing $\gamma_{\mathrm{e2e}}^{x_1}$ and $\gamma_{\mathrm{e2e}}^{x_2}$ into (39), we have

$$Q_1 = r_1 Pr\left(\frac{a_1P_{\mathrm{S}}|h_{\mathrm{SR}}|^2}{\eta P_{\mathrm{R}}|h_{\mathrm{RR}}|^2+\sigma_{\mathrm{R}}^2}>\xi_1\right)\Pr\left(\frac{a_1P_{\mathrm{R}}|g_1|^2}{\sigma_{\mathrm{D}_1}^2}>\xi_1\right), \tag{40}$$

and

$$\begin{aligned}Q_2 =& r_2\Pr\left(\frac{a_2P_{\mathrm{S}}|h_{\mathrm{SR}}|^2}{a_1P_{\mathrm{S}}|h_{\mathrm{SR}}|^2+\eta P_{\mathrm{R}}|h_{\mathrm{RR}}|^2+\sigma_{\mathrm{R}}^2}>\xi_2\right)\\ &\Pr\left(\frac{a_2P_{\mathrm{R}}|g_1|^2}{a_1P_{\mathrm{R}}|g_1|^2+\sigma_{\mathrm{D}_1}^2}>\xi_2\right)\\ &\times\Pr\left(\frac{a_2P_{\mathrm{R}}|g_2|^2}{a_1P_{\mathrm{R}}|g_2|^2+\sigma_{\mathrm{D}_2}^2}>\xi_2\right).\end{aligned} \tag{41}$$

where $\xi_1 = 2^{r_1}-1$ and $\xi_2 = 2^{r_2}-1$.

From (40) and (41), we can find ξ_i or r_i that maximizes $Q_1(r_1)$ and $Q_1(r_2)$ with certain transmission power and average channel gain.

$$\begin{aligned}Q_1(\xi_1) = &\log_2(1+\xi_1)\sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\\ &\frac{a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}{\Omega_{\mathrm{RR}}k\xi_1\eta P_{\mathrm{R}}+a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}\\ &\times\exp\left(-\frac{\xi_1}{\Omega_{\mathrm{RD}_1}a_1P_{\mathrm{R}}}-\frac{k\xi_1}{\Omega_{\mathrm{SR}}\Delta(\rho)a_1P_{\mathrm{S}}}\right),\end{aligned} \tag{42}$$

$$Q_2(\xi_2) = \log_2(1+\xi_2)\sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k} \frac{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}(a_2-a_1\xi_2)}{\xi_2[k\eta P_{\mathrm{R}}\Omega_{\mathrm{RR}}-\Omega_{\mathrm{SR}}\Delta(\rho)a_1P_{\mathrm{S}}]+\Omega_{\mathrm{SR}}\Delta(\rho)a_2P_{\mathrm{S}}} \times \exp\Big(-\frac{k\xi_2}{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}(a_2-a_1\xi_2)} - \frac{\xi_2}{\Omega_{\mathrm{RD}_1}P_{\mathrm{R}}(a_2-a_1\xi_2)} - \frac{\xi_2}{\Omega_{\mathrm{RD}_2}P_{\mathrm{R}}(a_2-a_1\xi_2)}\Big), \tag{43}$$

These equations are rewritten as follows.

$$Q_1(\xi_1) \geq \log_2(1+\xi_1)\frac{a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)\exp(-\mu_1\xi_1)}{\xi_1\Omega_{\mathrm{RR}}1\eta P_{\mathrm{R}}+a_1P_{\mathrm{S}}\Omega_{\mathrm{SR}}\Delta(\rho)}, \tag{44}$$

$$Q_2(\xi_2) \geq \log_2(1+\xi_2)\frac{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}(a_2-a_1\xi_2)}{\xi_2\beta_1+\Omega_{\mathrm{SR}}\Delta(\rho)a_2P_{\mathrm{S}}}\exp - \Big(\frac{\mu_2\xi_2}{a_2-a_1\xi_2}\Big), \tag{45}$$

where $\mu_1 = \frac{1}{\Omega_{\mathrm{RD}_1}a_1P_{\mathrm{R}}} + \frac{1}{\Omega_{\mathrm{SR}}\Delta(\rho)a_1P_{\mathrm{S}}}$, $\mu_2 = \frac{1}{\Omega_{\mathrm{SR}}\Delta(\rho)P_{\mathrm{S}}} + \frac{1}{\Omega_{\mathrm{RD}_1}P_{\mathrm{R}}} + \frac{1}{\Omega_{\mathrm{RD}_2}P_{\mathrm{R}}}$ and $\beta_1 = \eta P_{\mathrm{R}}\Omega_{\mathrm{RR}} - \Omega_{\mathrm{SR}}\Delta(\rho)a_1P_{\mathrm{S}}$. To notice that (44) and (45) are linear with (42) and (43), respectively.

The maximal J_1 for given transmission power and average channel gains can be determined via following optimization problem

$$\xi_i^* = \arg \max_{\substack{0<\xi_1<r_{\max} \\ 0<\xi_2<a_2/a_1}} Q_i(\xi_i). \tag{46}$$

To find the feasible ξ_i values, we have the Lemmas for the property unique root as follows.

Lemma 1 *For $a,b,c>0$, the below function has one and only one maximum value in the interval $[0,r_{\max})$.*

$$f(x) = \log_2(1+x)\frac{a}{bx+c}\exp(-\mu x), 0 \leq x < r_{\max}. \tag{47}$$

If x^* is the value that maximizes $f(x)$, the function $f(x)$ monotonically increases in the interval $[0,x^*)$ and then monotonically decreases in the interval $(x^*,r_{\max})$. This means that $f(x)$ is an unimodal function in the interval $[0,r_{\max})$.

Lemma 2 *For $a,b>0$, the below function has one and only one maximum value in the interval [0, a/b).*

$$\psi(x) = \log_2(1+x)\frac{\mathcal{D}(a-bx)}{\beta_1x+\mathcal{C}}\exp(-\frac{\mu x}{a-bx}), 0 \leq x < a/b. \tag{48}$$

If x^* is the value that maximizes $\psi(x)$, the function $\psi(x)$ monotonically increases in the interval $[0,x^*)$, and then monotonically decreases in the interval $(x^*,a/b)$. This means that $\psi(x)$ is an unimodal function in the interval [0, a/b).

The proof of Lemmas 1 and 2 is given in detail in Appendix C. Moreover, the throughput of eavesdroppers can be derived as

$$J_2 = \underbrace{r_1\Pr(\log_2(1+\gamma_{\mathrm{E}}^{x_1})>r_1)}_{Q_3} + \underbrace{r_2\Pr(\log_2(1+\gamma_{\mathrm{E}}^{x_2})>r_2)}_{Q_4}. \tag{49}$$

Similar to $Q_1(\xi_1)$ and $Q_2(\xi_2)$, $Q_3(\xi_1)$ and $Q_4(\xi_2)$ are calculated as

$$Q_3(\xi_1) = \log_2(1+\xi_1)\sum_{l=1}^{L}\binom{L}{l}(-1)^{l-1}\exp\Big(-\frac{l\xi_1}{a_1P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\Big), \tag{50}$$

$$Q_4(\xi_2) = \log_2(1+\xi_2)\sum_{l=1}^{L}\binom{L}{l}(-1)^{l-1}\exp\Big(-\frac{l\xi_2}{a_2P_{\mathrm{R}}\hat{\Omega}_{\mathrm{RE}}}\Big). \tag{51}$$

Once above two Lemmas are satisfied, the throughput ξ_i^* is maximized by using the Golden-Section Search (GSS) method as shown in Algorithm 1, where $\tau(\xi_1) = Q_1(\xi_1) - Q_3(\xi_1)$ and $\tau(\xi_2) = Q_2(\xi_2) - Q_4(\xi_2)$.

Algorithm 1 Golden-Section Search Algorithm

1: Initialization: $\xi_L = 0, \xi_U = a_2/a_1, r_{\max} = 10, \phi = \frac{\sqrt{5}-1}{2}$ (Golden ratio), error tolerance $\delta = 10^{-2}$
2: $i = 1, \xi_1 = \xi_L + \frac{\xi_U-\xi_L}{\phi}, \xi_2 = \xi_U + \frac{\xi_L-\xi_U}{\phi}$,
3: **repeat**
4: **if** $\tau(\xi_1) < \tau(\xi_2)$ **then**
5: $\xi_U = \xi_2; \xi_2 = \xi_1; \tau_2 = \tau_1; \xi_1 = \xi_U + \frac{\xi_L-\xi_U}{\phi}; \tau_1 = \tau(\xi_1)$
6: **else**
7: $\xi_L = \xi_1; \xi_1 = \xi_2; \tau_1 = \tau_2; \xi_2 = \xi_L + \frac{\xi_U-\xi_L}{\phi}; \tau_2 = \tau(\xi_2)$
8: **end if**
9: $i = i+1$
10: **until** $|\xi_U - \xi_L| < \delta$ (the solution converge)
11: Optimal transmission rate $\xi^* = (\xi_U + \xi_L)/2$.

Table 1 The parameters of the system using for simulation

The parameters	Value
The number of users	$M = 2$
The number of antenna at S	$K \in [1, 2, 3]$
The number of eavesdroppers	$L \in [1, 2, 3]$
Power allocation coefficients	$a_1 = 0.3$, $a_2 = 0.7$
The average channel gains	$\Omega_{SR} = \Omega_{RD_2} = 10$ dB, $\Omega_{RD_1} = 15$dB, $\Omega_{RE} = -5$dB
The threshold data rate	$r_1 = r_2 = 0.5$ b/s/Hz
RSIC coefficient	$\eta = 0.1$
The number of terms Gaussian–Chebyshev	$N = 40$

5 Numerical results

In this section, the Monte-Carlo simulation is used to verify our derivations and evaluate the novel of the proposed model. In this system, the terminal is assumed to be stationary, thus, the path loss of the S - R and R - D links is characterized as average gain, i.e. $\Omega_{SR} = \mathbb{E}\{|h_{1,k}|^2\}$, $\Omega_{RR} = \mathbb{E}\{|h_{RR}|^2\}$, $\Omega_{RD_1} = \mathbb{E}\{|g_1|^2\}$, and $\Omega_{RD_2} = \mathbb{E}\{|g_2|^2\}$. The average SNR is defined as the ratio of the transmit power to the variance of AWGN, i.e., $\mathrm{SNR} = P_S/\sigma^2$. Except some special cases, in other scenarios, we set $\hat{\Omega}_{RE} = -5$ dB, the noise variance $\sigma_R^2 = \sigma_{D_1}^2 = \sigma_{D_2}^2 = \sigma^2 = 1$ and transmit power $P_S = P_R = P$. The Monte-Carlo simulation performs with 10×2^{14} independent trials. The other parameters are shown in Table 1, which are referred from [26].

In all figures, the Monte-Carlo simulation result is represented by marks, whereas the theoretical analysis result is plotted by a dark line. Firstly, we can observe that the simulation results match perfectly with the analysis results. It provides that our analysis is reasonable. The other notable result from all following figures is that the SOP of D_2 is firstly improved and then return into worst with high transmit SNR, it is identified with results and conclusion in [23, 26]. It is explained that, D_2 decodes its own signal by treating the signal of D_1 as interference, while D_1 performs the SIC operation to cancel the signal of D_2, and then decodes its own signal. Furthermore, due to the residual self-interference cancellation of FD technique, the SOP of D_1 is saturated in high SNR regime.

In Fig. 2, we illustrate the impact of a number of eavesdroppers on the SOP of the considered system versus SNR in dB. It can be observed from Fig. 2 that the security performance is degraded as the number of eavesdroppers increases. It's easily explained that with more eavesdroppers, the capability overhearing the information of legitimate channels is increased, i.e., the chance for one of them to overhear the desired message becomes higher. On the other hand, the SOP of each user is improved in the low SNR region, and then the SOP of D_2 is saturated, while the SOP of D_1 becomes worse. In addition, the simulation curves overlap with the corresponding analytical curves, it confirms the correctness of our theoretical analysis.

Figure 3 demonstrates the SOP versus SNR with the correlation coefficient of channel estimation error at the eavesdropper, $\rho_E = 0.2$ and correlation coefficient of the outdated CSI at the source, $\rho = 0.9$. In this figure, we recognize that the SOP is improved in terms of increasing the number of antennas. However, observation is that the gap between the curves is difference with different number of antennas at the S, K, where K increases from 1 to 2, the gap is larger when K increases from 2 to 3. The reason is, the number of antennas at the FD relay is 2, therefore the performance is improved slowly when K is larger than 2. On the other hand, we also recognize that the shape of curves in Fig. 3 is the same as them in Fig. 2, the reason is explained as above.

Figure 4 illustrates the SOP of D_1 versus the average SNR with the various value of self-interference channel gain, Ω_{RR}. From this figure we know that intensifying Ω_{RR} lets the SOP degrade. It is because the SOP is considered as the ratio of SNR between the legitimate channel and wiretapping channel. Meanwhile, the larger the Ω_{RR} is, the smaller the SNR of the legitimate channel becomes. Thus, to guarantee the secrecy performance, the performance of SIC of x_2 at the relay and the D_1 should ensure perfectly, as well as the residual self-interference at the relay node must be mitigated.

The eavesdropper is a passive system, it doesn't train the CSI in the communication process. Therefore, the eavesdropper hardly obtains the perfect CSI. Figure 5 demonstrates the SOP of D_1 with different values of correlation coefficient of channel estimation error at the eavesdropper, ρ_E. As shown in this figure, when ρ_E increases, the error of CSI for signal detection at the eavesdropper increases, thus the SOP is improved.

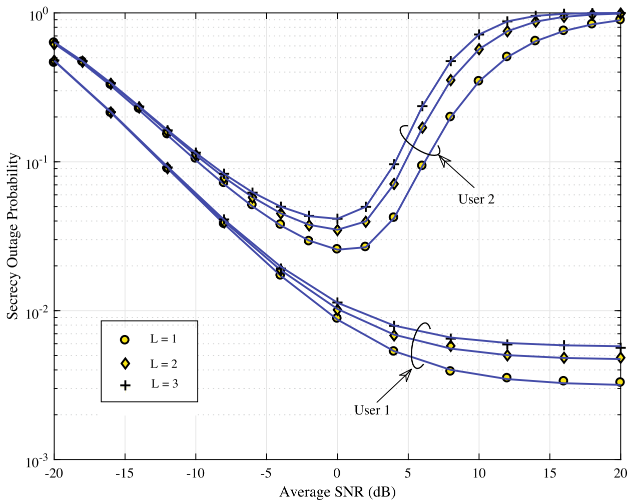


Fig. 2 The SOP for various number of L with $K = 3$, $\Omega_{\mathrm{RR}} = -20$ dB, $\rho_E = 0.2$, $\rho = 0.9$

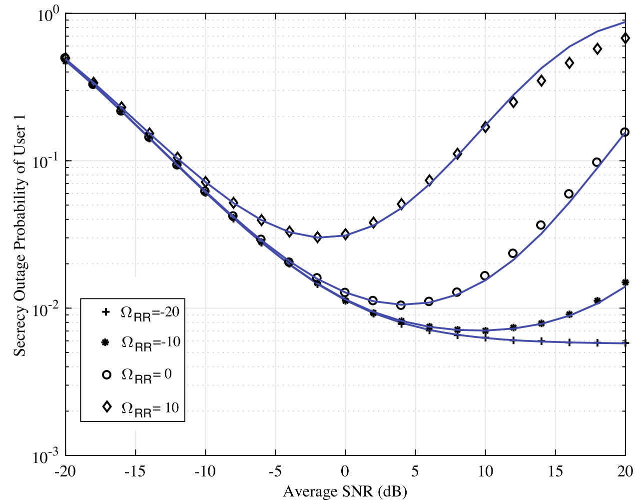


Fig. 4 Impact of the loop-back interference channel gain, Ω_{RR} on the SOP with $K = 3$ and $L = 3$, $\rho_E = 0.2$, $\rho = 0.9$

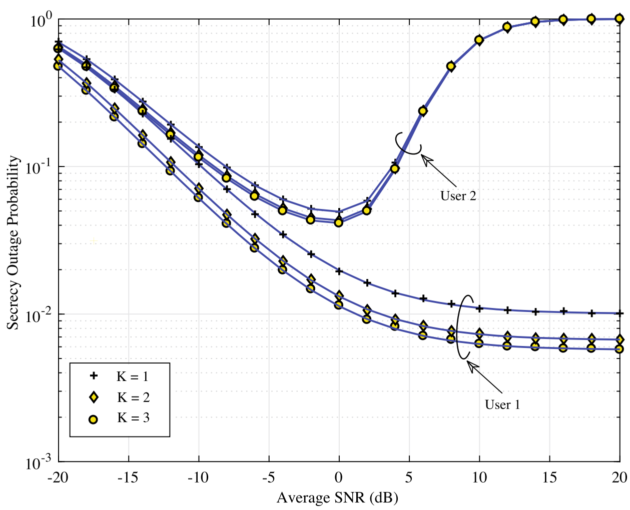


Fig. 3 SOP for various the number of K with $L = 3$, $\Omega_{\mathrm{RR}} = -20$ dB, $\rho_E = 0.2$, $\rho = 0.9$

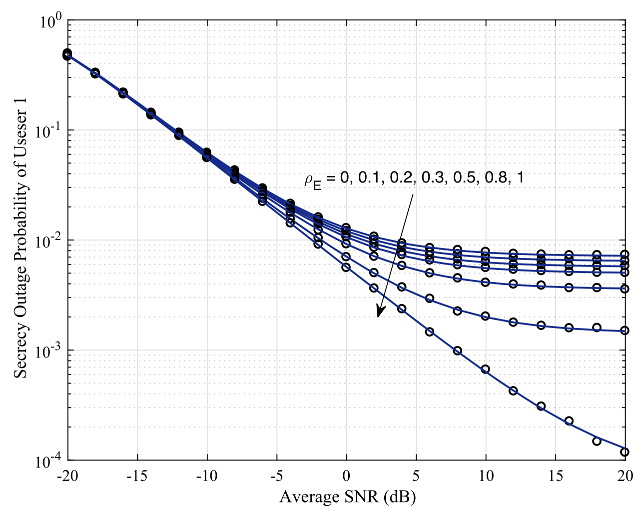


Fig. 5 The SOP for various ρ_E with $L = 3$, $K = 3$, $\Omega_{\mathrm{RR}} = -20$ dB, $\rho = 0.9$

Figure 6 demonstrates the SOP of the system versus average SNR in dB. In this result, we investigated the secrecy performance of the NOMA system, i.e., the SOP of each user and the SOP of overall system following Remark 2 and Remark 3. Also, we consider the SOP for the case of OMA technique to compare the secrecy performances of them. Firstly, we see that the theoretical result of Remark 3 is matched with the simulation in all SNR region, while the theoretical result of Remark 2 is approximate with the simulation result, especially in high SNR region. Another observation is that, the secrecy performances of the system depends mostly on the SOP of D_2. Intuitively, the user that mostly loses security dominates the overall secrecy performance of the system. Finally, we recognize that with the low SNR region, the SOP of NOMA outperforms the SOP of OMA scheme. In contrast, at the high SNR region, the SOP of the OMA scheme is better.

Figure 7 present the SOP of each user in two cases, i.e., HD and FD techniques, versus SNR in dB. Similar to the other figures, when SNR increase, the SOP of both users firstly decreases, and then increases or reaches the saturation point. Moreover, the secrecy performance of FD-NOMA system always outperform the HD-NOMA system. The reason is that the communication phase of HD and FD is performed with one and two phases, respectively. Thus, the predefined threshold value of HD and FD is respectively $\gamma_{\mathrm{th}} = 2^{2r_1}$ and $\gamma_{\mathrm{th}} = 2^{r_1}$.

The secrecy throughput of each user and sum of them are represented in Fig. 8 versus average SNR in dB. From this figure we can see that, the secrecy throughput of D_2

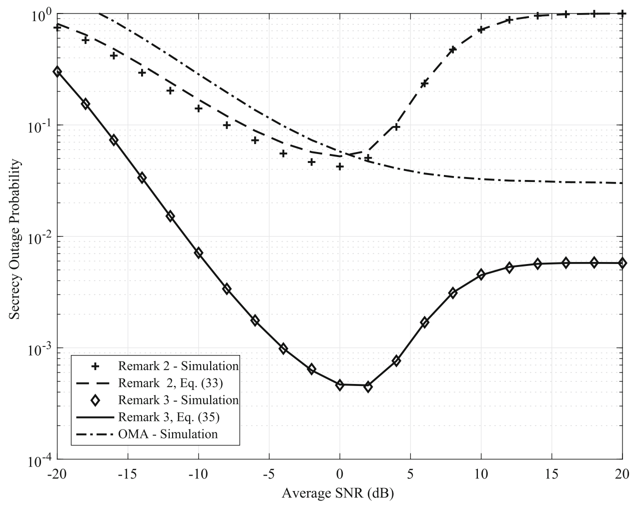


Fig. 6 Comparison of SOPs with $L = 3$, $K = 3$ and $\Omega_{RR} = -20$ dB, $\rho = 0.9$, $\rho_E = 0.2$

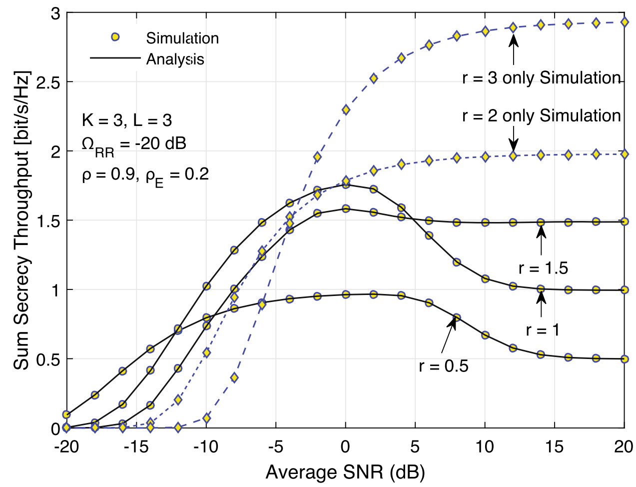


Fig. 9 Sum secrecy through versus the SNR with different transmission rates, $L = 3$, $K = 3$ and $\Omega_{RR} = -20$ dB, $\rho = 0.9$, $\rho_E = 0.2$

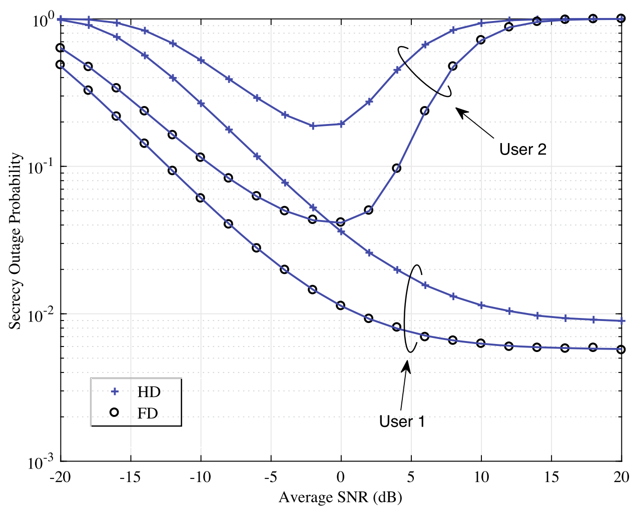


Fig. 7 Comparison of SOP of FD and HD techniques with the NOMA relay protocol with $L = 3$ and $K = 3$, $\Omega_{RR} = -20$ dB, $\rho_E = 0.2$, $\rho = 0.9$

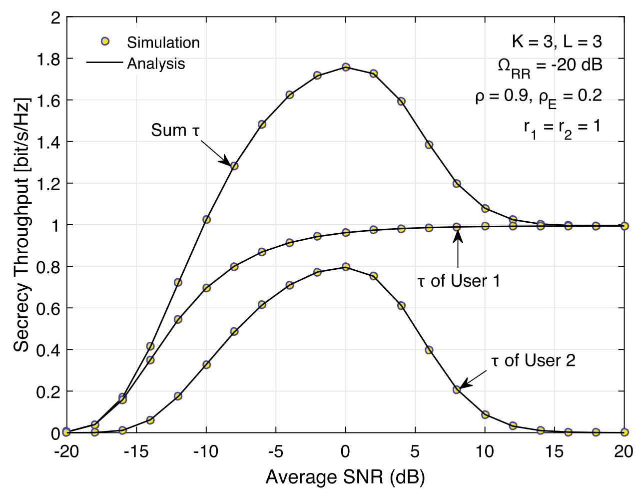


Fig. 8 System secrecy through versus the SNR $L = 3$, $K = 3$ and $\Omega_{RR} = -20$ dB, $\rho = 0.9$, $\rho_E = 0.2$

firstly increases, reaches to the maximum value at SNR = 0 dB, and then decreases when the average SNR increases. In contrast, the secrecy throughput of D_1 firstly increases, and then saturates at the high SNR regime. It is because that, the signal of D_1 interferes with the D_2, while the signal of D_2 are removed (by SIC operation) at D_1.

Figure 9 demonstrates the sum secrecy throughput of the considered FD-NOMA relay system with different transmission rates (codeword rates). The secrecy throughput is increased when the average SNR increases. However, the secrecy throughput of low r is higher than that of larger r in the low average SNR regime. Whereas, in the high average SNR regime, the secrecy throughput is improved with increasing transmission rate, i.e. the secrecy throughput of high r is larger than that of low r.

Figure 10 illustrated the secrecy throughput of the D_1, D_2 and sum of them versus the transmission rate, we set SNR = 10 dB and other parameters as shown in Fig. 10. From this figure, we can recognize that the secrecy throughput firstly increases and then decreases for any transmission rate, r_i. Moreover, the optimal value of r^* derived by the Golden-Section Search method are the same as simulation result. On the other hand, the optimal value of r^* for the maximum secrecy throughput of D_1 is different from that for the maximum secrecy throughput of D_2. The reason is similar to the result in Fig. 8.

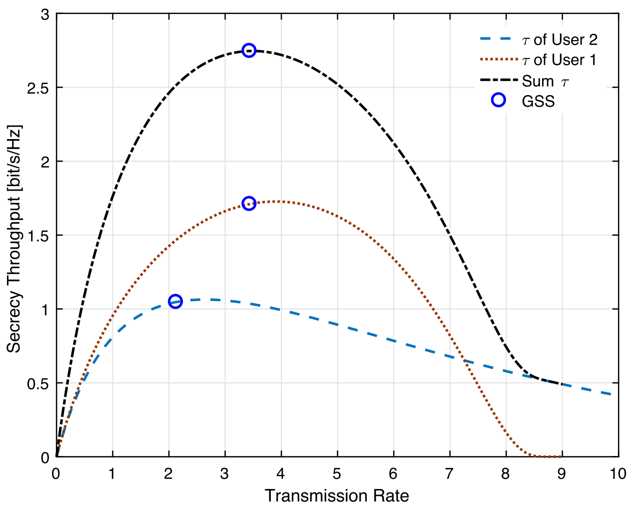


Fig. 10 Sum secrecy through versus transmission rate, SNR = 10 dB, $\Omega_{RR} = -20$ dB, $\rho = 0.9$, $\rho_E = 0.2$. The optimal r^* and maximum τ derived by the Golden-Section Search

6 Conclusion

In this paper, we have proposed and analyzed the TAS - FD - NOMA relay system with the assumption of the presentation of multiple eavesdroppers. The SOP of each user, as well as the SOP of the whole system are considered as a criterion to evaluate the secrecy performance of the system. The closed-form expressions of SOP of every user and the approximate SOP of overall system are derived under condition of outdated CSI for the TAS and channel estimation error at eavesdroppers. With the numerical and analytical results, this paper has provided valuable insight into the secure performance of FD-NOMA system, i.e. the SOP of a near user (User 1) is much higher than that of a far user (User 2), especially in high SNR region; the SOP is improved when the correlation coefficient of channel estimation error at the eavesdropper reduces and/or the correlation coefficient of the outdated CSI at the source increases. The calculation result indicates that the FD-NOMA system outperforms the HD-NOMA system in terms of the same transmission time slot. Furthermore, the secrecy throughput is investigated, and the Golden-Section Search method is applied to find the optimal value of transmission rate in order to maximize the secrecy throughput of every user and sum of them.

The TAS - FD - NOMA relay system was proposed and its SOP was evaluated, however, the number of hops as well as the number of users were restricted to two, moreover, the eavesdropper was assumed to be non-colluding. The system with more hops, more users and colluding eavesdropper will be considered in our future work.

Appendix

Appendix A

This appendix aim is to provide the proof of CDF of SINR end to end for User 1. As denoted in the previous section, $\gamma_1 = \min\{\gamma_R^{x_1}, \gamma_{D_1}^{x_1}\}$, the CDF of γ_1 can be written as

$$F_{\gamma_1}(y) = \Pr(\min\{\gamma_R^{x_1}, \gamma_{D_1}^{x_1}\} < y) \\ = 1 - \Pr(\min\{\gamma_R^{x_1}, \gamma_{D_1}^{x_1}\} > y). \tag{52}$$

From (8) and (13) we have

$$F_{\gamma_1}(y) = 1 - \Pr\left(\frac{a_1 P_S |h_{SR}|^2}{\eta P_R |h_{RR}|^2 + \sigma_R^2} > y, \frac{a_1 P_R |g_1|^2}{\sigma_{D_1}^2} > y\right) \\ = 1 - \Pr\left(\frac{a_1 P_S |h_{SR}|^2}{\eta P_R |h_{RR}|^2 + \sigma_R^2} > y\right) \Pr\left(\frac{a_1 P_R |g_1|^2}{\sigma_{D_1}^2} > y\right). \tag{53}$$

Without loss of generality, we assume that $\sigma_R^2 = \sigma_{D_1}^2 = 1$, and by using the probability condition, we can rewrite (53) as

$$F_{\gamma_1}(y) = 1 - \int_0^\infty \left[1 - F_{|h_{SR}|^2}\left(\frac{y(\eta P_R z + 1)}{a_1 P_S}\right)\right] f_Z(z) dz \left[1 - F_{|g_1|^2}\left(\frac{y}{a_1 P_R}\right)\right]. \tag{54}$$

Because the CDF of $|g_1|^2$ follows the Rayleigh distribution, $F_{|g_1|^2}(x) = 1 - \exp\left(-\frac{x}{\Omega_3 a_1 P_R}\right)$ and $Z = |h_{RR}|^2$ are modeled by Rayleigh distribution, i.e., $f_Z(z) = \frac{1}{\Omega_{RR}} \exp(-\frac{z}{\Omega_{RR}})$. From (54), we can rewrite $F_{\gamma_1}(y)$ as follows.

$$F_{\gamma_1}(y) = 1 - \sum_{k=1}^{K} (-1)^{k-1} \binom{K}{k} e^{-\frac{y}{\Omega_3 a_1 P_R}} \\ - \frac{ky}{\Omega_{SR}\Delta(\rho) a_1 P_S} \frac{1}{\Omega_{RR}} \int_0^\infty e^{-\frac{k y \eta P_R z}{\Omega_{SR}\Delta(\rho) a_1 P_S} - \frac{z}{\Omega_{RR}}} dz. \tag{55}$$

By using $\int_0^\infty \exp(-ax)dx = 1/a$ [38, eq. (3.310. 11)], we can obtain the closed-form expression of $F_{\gamma_1}(y)$.

$$F_{\gamma_1}(y) = 1 - \sum_{k=1}^{K} (-1)^{k-1} \binom{K}{k} e^{-\frac{y}{\Omega_3 a_1 P_R}} \\ - \frac{ky}{\Omega_{SR}\Delta(\rho) a_1 P_S} \frac{a_1 P_S \Omega_{SR} \Delta(\rho)}{\Omega_{RR} k y \eta P_R + a_1 P_S \Omega_{SR} \Delta(\rho)}, \tag{56}$$

where $y = 2^{r_1}(1 + x) - 1$. After some manipulation we have

$$F_{\gamma_1}(x) = 1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\exp(\mathcal{A}_1)\frac{a_1 P_S \Omega_{SR}\Delta(\rho)}{\beta+\gamma_{th}\Omega_{RR}kP_R\eta x} \times \exp\left(-\frac{k\gamma_{th}x}{a_1 P_S\Omega_{SR}\Delta(\rho)} - \frac{\gamma_{th}x}{a_1 P_R \Omega_{RD_1}}\right), = 1 - \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\exp(\mathcal{A}_1) \frac{a_1 P_S\Omega_{SR}\Delta(\rho)}{\beta}\frac{1}{1+\mathcal{A}_2 x}\exp(-\mathcal{A}_3 x), \tag{57}$$

where $\gamma_{th} = 2^{r_1}$, $\beta = \Omega_{RR}k\eta P_R(\gamma_{th}-1) + a_1\Omega_{SR}\Delta(\rho)P_S$, $\mathcal{A}_1 = \frac{k(1-\gamma_{th})}{a_1\Omega_{SR}\Delta(\rho)kP_S} + \frac{1-\gamma_{th}}{a_1 P_R\Omega_{RD_1}}$, $\mathcal{A}_2 = \frac{\gamma_{th}\Omega_{RR}k\eta P_R}{\beta}$ and $\mathcal{A}_3 = \frac{k\gamma_{th}}{a_1 P_S\Omega_{SR}\Delta(\rho)} + \frac{\gamma_{th}}{a_1 P_R\Omega_{RD_1}}$. The CDF of γ_1 is obtained and the proof is completed.

Appendix B

From (28), we know that SNR of each link is independence, thus the CDF of γ_2, i.e., $F_{\gamma_2}(y) = \Pr(\gamma_2 < y)$ is derived as

$$F_{\gamma_2}(y) = 1 - \underbrace{\Pr\left(\frac{a_2 P_S|h_{SR}|^2}{a_1 P_S|h_{SR}|^2 + \eta P_R|h_{RR}|^2 + \sigma_R^2} > y\right)}_{\mathcal{O}_1} \times \Pr\left(\frac{a_2 P_R|g_1|^2}{a_1 P_R|g_1|^2 + \sigma_{D_1}^2} > y\right)\Pr\left(\frac{a_2 P_R|g_2|^2}{a_1 P_R|g_2|^2 + \sigma_{D_2}^2} > y\right). \tag{58}$$

Using the probability condition, the first part in (58) is rewritten as

$$\mathcal{O}_1 = \int_0^\infty \Pr\left(|h_{SR}|^2 > \frac{y(\eta P_R z + 1)}{P_S(a_2 - a_1 y)}\right) f_{|h_{RR}|^2}(z)dz. \tag{59}$$

Using (6) and $f_{|h_{RR}|^2}(z)$ in Appendix A, we can get the $\mathcal{O}_1$ as

$$\mathcal{O}_1 = \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\exp\left(-\frac{ky}{\Omega_{SR}\Delta(\rho)P_S(a_2 - a_1 y)}\right) \times \frac{1}{\Omega_{RR}}\int_0^\infty \exp\left(-\frac{ky\eta P_R z}{\Omega_{SR}\Delta(\rho)P_S(a_2 - a_1 y)} - \frac{z}{\Omega_{RR}}\right)dz. \tag{60}$$

Applying [38, eq. (3.310. 11)] for integral component in (60) with respect to z variable, we obtain the closed-form of $\mathcal{O}_1$. On the other hand, the channel is modeled by Rayleigh distribution, thus $|g_1|^2$ and $|g_2|^2$ follows the exponential distribution. From the second and third probability parts in (58), and with some manipulation, we have the CDF of γ_2 as shown in (29).

Appendix C

This appendix provides the proof of Lemma 1 and Lemma 2. Firstly, we present the step-by-step to prove Lemma 1. Because the object problem is maximization and object function is convex, i.e., the problem of (46) is non convex with respect to ξ_i. Thus, we must prove the increase and decrease of function $f(x)$ in (47) via the extremum problem. We take the first derivation of $f(x)$ with respect to x as

$$\frac{df(x)}{dx} = \frac{\exp(-\mu_1 x)}{(bx+c)\ln 2}\left[\frac{a}{1+x} - \frac{ab\ln(1+x)}{bx+c} - a\ln(1+x)\right]. \tag{61}$$

For $x > 0$, we have $\frac{\exp(-\mu_1 x)}{(bx+c)\ln 2} > 0$. Thus, we can find the solutions of $f(x)$ through $g(x) = \frac{a}{1+x} - \frac{ab\ln(1+x)}{bx+c} - a\ln(1+x)$. To notice that, since there exists a neighborhood of x^* in $(0, r_{\max})$ which lets $g(x)$ change from positive to negative values, i.e., $g(x)$ reaches the maximum value at x^*. For $x = 0$, we have $g(x) = a > 0$ and $x \to r_{\max}$, thus $g(x) = \frac{a}{1+r_{\max}} - \frac{ab\ln(1+r_{\max})}{br_{\max}+c} - a\ln(1+r_{\max}) < 0$, $\forall a, b, c > 0$. On the other hand, the first derivation of $g(x)$ with respect to x is $\frac{dg(x)}{dx} = -a\left(\frac{1}{(1+x)^2} + \frac{1}{(1+x)\ln 2} + \frac{b}{(1+x)(c+bx)\ln 2} - \frac{b\ln(1+x)}{(c+bx)^2\ln 2}\right) < 0$, $0 \le x < r_{\max}$. Therefore, $\frac{df(x)}{dx} > 0$ in the interval $[0, x^*)$ and $\frac{df(x)}{dx} < 0$ in the interval $(x^*, r_{\max})$. The proof of Lemma 1 is finished.

The proof of Lemma 2 is similar to that of Lemma 1, to notice that the first derivation of $\psi(x)$ with respect to x is represented as

$$\frac{d\psi(x)}{dx} = \frac{exp\left(-\frac{\mu_2 x}{a-bx}\right)(a-bx)\mathcal{D}}{(\beta_1 x + \mathcal{C})\ln 2} \times \underbrace{\left[\frac{1}{1+x} - \frac{\ln(1+x)}{\beta_1 x + \mathcal{C}} - b\ln(1+x) + \left(-\frac{b\mu_2 x}{a-bx} - \frac{\mu_2}{a-bx}\right)\ln(1+x)\right]}_{G(x)}, \tag{62}$$

and

$$\frac{dG(x)}{dx} = -\left(\frac{1}{(1+x)} + \frac{b}{1+x} + \frac{1}{(1+x)(\beta_1 x + \mathcal{C})}\right) + \frac{\beta_1\ln(1+x)}{(\beta_1 x + \mathcal{C})^2} - \left(\frac{b\mu_2}{(a-bx)^2} + \frac{b^2\mu_2 x}{(a-bx)^2} + \frac{b\mu_2}{a-bx}\right)\ln(1+x). \tag{63}$$

In general, there is one and only one x^* in the interval (0, a/b) that $\psi(x)$ obtains a maximum value. The proof of Lemma 2 is completed, i.e., there always exist a transmission rate that maximizes the secrecy throughput of the considered FD-NOMA relay system.

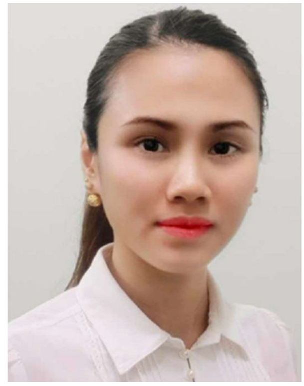
References

1. Islam, S. R., Avazov, N., Dobre, O. A., & Kwak, K.-S. (2016). Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges. *IEEE Communications Surveys and Tutorials, 19*(2), 721–742.
2. Liu, Y., Qin, Z., Elkashlan, M., Nallanathan, A., & McCann, J. A. (2017). Non-orthogonal multiple access in large-scale heterogeneous networks. *IEEE Journal on Selected Areas in Communications, 35*(12), 2667–2680.
3. Liu, Y., Ding, Z., Elkashlan, M., & Poor, H. V. (2016). Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer. *IEEE Journal on Selected Areas in Communications, 34*(4), 938–953.
4. Hoang, T. M., Tan, N. T., Hoang, N. H., & Hiep, P. T. (2018). Performance analysis of decode-and-forward partial relay selection in NOMA systems with RF energy harvesting. *Wireless Networks, 25,* 4585.
5. Zeng, M., Yadav, A., Dobre, O. A., Tsiropoulos, G. I., & Poor, H. V. (2017). Capacity comparison between MIMO-NOMA and MIMO-OMA with multiple users in a cluster. *IEEE Journal on Selected Areas in Communications, 35*(10), 2413–2424.
6. Rodriguez, L. J., Tran, N. H., & Le-Ngoc, T. (2014). Performance of full-duplex AF relaying in the presence of residual self-interference. *IEEE Journal on Selected Areas in Communications, 32*(9), 1752–1764.
7. Mohammadi, M., Suraweera, H. A., Cao, Y., Krikidis, I., & Tellambura, C. (2015). Full-duplex radio for uplink/downlink wireless access with spatially random nodes. *IEEE Transactions on Communications, 63*(12), 5250–5266.
8. Hoang, T. M., Son, V. V., Dinh, N. C., & Hiep, P. T. (2018). Optimizing duration of energy harvesting for downlink NOMA full-duplex over Nakagami-m fading channel. *AEU - International Journal of Electronics and Communications, 95,* 199–206.
9. Laughlin, L., Beach, M. A., Morris, K. A., & Haine, J. L. (2014). Optimum single antenna full duplex using hybrid junctions. *IEEE Journal on Selected Areas in Communications, 32*(9), 1653–1661.
10. Li, R., Chen, Y., Li, G. Y., & Liu, G. (2017). Full-duplex cellular networks. *IEEE Communications Magazine, 55*(4), 184–191.
11. Lei, H., Zhang, J., Park, K.-H., Xu, P., Zhang, Z., Pan, G., & Alouini, M.-S. (2018). Secrecy outage of max-min TAS scheme in MIMO-NOMA systems. *IEEE Transactions on Vehicular Technology, 67*(8), 6981–6990.
12. Zhang, X., & Wang, F. (2018). Resource allocation for wireless power transmission over full-duplex OFDMA/NOMA mobile wireless networks. *IEEE Journal on Selected Areas in Communications, 37*(2), 327–344.
13. Kim, Y.-B., Yamazaki, K., & Jung, B. C. (2019). Virtual full-duplex cooperative NOMA: Relay selection and interference cancellation. *IEEE Transactions on Wireless Communications, 18*(12), 5882–5893.
14. Li, X., Liu, M., Deng, C., Mathiopoulos, P. T., Ding, Z., & Liu, Y. (2019). Full-duplex cooperative NOMA relaying systems with I/Q imbalance and imperfect SIC. *IEEE Wireless Communications Letters, 9,* 17.
15. Liu, G., Chen, X., Ding, Z., Ma, Z., & Yu, F. R. (2017). Hybrid half-duplex/full-duplex cooperative non-orthogonal multiple access with transmit power adaptation. *IEEE Transactions on Wireless Communications, 17*(1), 506–519.
16. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28*(4), 656–715.
17. Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal, 54*(8), 1355–1387.
18. Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory, 24*(3), 339–348.
19. Zhao, H., Liu, Z., Yang, L., & Alouini, M.-S. (2019). Secrecy analysis in df relay over generalized-K fading channels. *IEEE Transactions on Wireless Communications, 67*(10), 7168–7182.
20. Cao, K., Wang, B., Ding, H., & Tian, J. (2019). Adaptive cooperative jamming for secure communication in energy harvesting relay networks. *IEEE Transactions on Wireless Communications, 8*(5), 1316–1319.
21. Guo, Q., & Feng, W. (2019). Joint relay and eavesdropper selection strategy against multiple eavesdroppers over Nakagami-m fading channels in cooperative decode-and-forward relay networks. *IEEE Access, 7,* 37–980.
22. Ding, Z., Leung, K. K., Goeckel, D. L., & Towsley, D. (2012). On the application of cooperative transmission to secrecy communications. *IEEE Journal on Selected Areas in Communications, 30*(2), 359–368.
23. Pei, X., Yu, H., Wen, M., Li, Q., & Ding, Z. (2020). Secure outage analysis for cooperative NOMA systems with antenna selection. *IEEE Transactions on Vehicular Technology, 69,* 4503.
24. Jiang, K., Zhou, W., & Sun, L. (2020). Jamming-aided secrecy performance in secure uplink NOMA system. *IEEE Access, 8,* 15072–15084.
25. Wang, D., Xu, W., Liang, W., Ding, Z., & Li, L. (2020). Security provisioning for non-orthogonal multiple access networks with limited feedback. *IEEE Wireless Communications Letters, 9,* 1226.
26. Lei, H., Yang, Z., Park, K.-H., Ansari, I. S., Guo, Y., Pan, G., & Alouini, M.-S. (2019). Secrecy outage analysis for cooperative NOMA systems with relay selection schemes. *IEEE Transactions on Communications, 67*(9), 6282–6298.
27. Lei, H., Gao, R., Park, K.-H., Ansari, I. S., Kim, K. J., & Alouini, M.-S. (2020). On secure downlink NOMA systems with outage constraint. *IEEE Transactions on Communications, 68*(12), 7824–7836.
28. Cao, K., Wang, B., Ding, H., Li, T., Tian, J., & Gong, F. (2020). Secure transmission designs for noma systems against internal and external eavesdropping. *IEEE Transactions on Information Forensics and Security, 15,* 2930–2943.
29. Bariah, L., Muhaidat, S., & Al-Dweik, A. (2018). Error probability analysis of non-orthogonal multiple access over nakagami-*m* fading channels. *IEEE Transactions on Communications, 67*(2), 1586–1599.
30. Cheng, H. V., Björnson, E., & Larsson, E. G. (2018). Performance analysis of NOMA in training-based multiuser MIMO systems. *IEEE Transactions on Communications, 17*(1), 372–385.
31. Adhikary, A., Nam, J., Ahn, J.-Y., & Caire, G. (2013). Joint spatial division and multiplexing: The large-scale array regime. *IEEE Transactions on Information Theory, 59*(10), 6441–6463.
32. Huang, Y., Al-Qahtani, F. S., Duong, T. Q., & Wang, J. (2015). Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. *IEEE Transactions on Communications, 63*(8), 2959–2971.
33. Vaezi, M., Schober, R., Ding, Z., & Poor, H. V. (2019). Non-orthogonal multiple access: Common myths and critical questions. *IEEE Wireless Communications, 26*(5), 174–180.
34. Xu, Y., Xia, J., Wu, H., & Fan, L. (2019). Q-learning based physical-layer secure game against multiagent attacks. *IEEE Access, 7*(49), 212.
35. Wang, D., Ren, P., & Cheng, J. (2017). Cooperative secure communication in two-hop buffer-aided networks. *IEEE Transactions on Wireless Communications, 66*(3), 972–985.

36. Zhang, Y., Wang, H.-M., Yang, Q., & Ding, Z. (2016). Secrecy sum rate maximization in non-orthogonal multiple access. *IEEE Communications Letters, 20*(5), 930–933.
37. Xiang, Z., Yang, W., Pan, G., Cai, Y., & Sun, X. (2019). Secure transmission in non-orthogonal multiple access networks with an untrusted relay. *IEEE Communications Letters, 8*(3), 905–908.
38. Gradshteyn, I. S., & Ryzhik, I. M. (2014). Table of integrals, series, and products.
39. Abramowitz, M., & Stegun, I. A. (1964). *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. North Chelmsford, MA, USA: Courier Corporation, vol. 55.
40. Liu, Y., Qin, Z., Elkashlan, M., Gao, Y., & Hanzo, L. (2017). Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Transactions on Communications, 16*(3), 1656–1672.

Dr. Nguyen Le Cuong received his Bachelor degree in Electronics and Telecommunications at Hanoi University of Science and Technology in 1999 and Master degree in Telecommunications at Le Quy Don University in 2006. In 2012 he received a Ph.D. degreein Electronics Engineering at Post and Telecommunications Institute of Technology (PTIT). He joined Vietnam telephone equipment company (VITECO) as Research Engineer in 1999. Now,he is a lecturer in Electric Power University, Vietnam as Head of Faculty of Electronics and Telecommunications. His research interests are information security, watermarking and signal processing.

Dr. Tran Manh Hoang received the B.S. degree in communication command from Telecommunications University, Ministry of Defense, Nha Trang, Vietnam, in 2002, the B.Eng. degree in electrical engineering from Le Quy Don Technical University, Ha Noi, Vietnam, in 2006, the M.Eng. degree in electronics engineering from Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam, in 2013 and the Ph.D degree from Le Quy Don Technical University, Hanoi, Vietnam, in 2018. He is currently a Lecturer with Telecommunications University, Nhatrang, Vietnam. His research interests include energy harvesting, non-orthogonal multiple access, and signal processing for wireless cooperative communications.



Dr. Nguyen Thu Phuong received the B.S, M.S and Ph.D. degrees from Le Quy Don Technical University, Vietnam in 2008, 2012 and 2016, respectively. She is now a lecturer at Faculty of Radio-Electronics Engineering, and a key member of Advanced Wireless Communication Group, Le Quy Don Technical University, Hanoi, Vietnam. Her research interests are in the area of emerging technologies for future wireless communications: Spatial modulation and index modulation, Non-orthogonal multiple access (NOMA), space-time processing, space-time coding and MIMO systems.

Pham Thanh Hiep received the B.E. degree in Communications Engineering from National Defense Academy, Japan, in 2005; received the M.E. and Ph.D. degree in Physics, Electrical and Computer Engineering from Yokohama National University, Japan, in 2009 and 2012, respectively. He was working as associate researcher at Yokohama National University, Yokohama, Japan from 2012 to 2015. Now, he is a lecturer at Le Quy Don Technical University, Ha Noi, Viet Nam. His research interests lie in the area of wireless information and communications technologies.