Physical Layer Secrecy Enhancement for Non-orthogonal Multiple Access Cooperative Network with Artificial Noise

Van-Long Nguyen[1](✉) and Dac-Binh Ha[2]

[1] Graduate School, Duy Tan University, Da Nang, Vietnam
vanlong.itqn@gmail.com

[2] Faculty of Electrical and Electronics Engineering, Duy Tan University,
Da Nang, Vietnam
hadacbinh@duytan.edu.vn

Abstract. In this paper, the physical layer secrecy performance of non-orthogonal multiple access (NOMA) in a downlink cooperative network is studied. This considered system consists of one source, multiple legitimate user pairs and presenting an eavesdropper. In each pair, the better user forwards the information from the source to the worse user by using the decode-and-forward (DF) scheme and assuming that the eavesdropper attempts to extract the worse user's message. We propose the artificial noise - cooperative transmission scheme, namely ANCOTRAS, to improve the secrecy performance of this considered system. In order to evaluate the effectiveness of this proposed scheme, the lower bound and exact closed-form expressions of secrecy outage probability are derived by using statistical characteristics of signal-to-noise ratio (SNR) and signal-to-interference-plus-noise ratio (SINR). Moreover, we investigate the secrecy performance of this considered system according to key parameters, such as power allocation ratio, average transmit power and number of user pair to verify our proposed scheme. Finally, Monte- Carlo simulation results are provided to confirm the correctness of the analytical results.

Keywords: Non-orthogonal multiple access · Cooperative network · Decode and forward · Artificial noise · Secrecy outage probability

1 Introduction

Nowadays, wireless devices, i.e., smartphones, smart control devices, and so on, are indispensable things in human life. Due to the mobility and convenience of wireless communication devices, the wireless system and devices are booming, i.e., now toward the fifth generation network (5G). The multiple access techniques applied in 4G and earlier generation networks belong to conventional orthogonal multiple access (OMA) type, such as FDMA, TDMA, and CDMA.

T. Q. Duong et al. (Eds.): INISCOM 2019, LNICST 293, pp. 81–98, 2019.
https://doi.org/10.1007/978-3-030-30149-1_7

Due to the significantly growing number of users and wireless devices, the next generation networks, i.e., 5G networks, are required to support the demand for low latency, low-cost and diversified services at higher quality and data rate. The conventional OMA techniques can not satisfy these demands anymore due to the limited channel resource and the spectral efficiency loss. The most prominent candidate that can meet these requirements 5G is the non-orthogonal multiple access (NOMA) technique [1–5]. Due to the advantage of the power domain to serve multiple users at the same time/frequency/code, the use of NOMA can ensure a significant spectral efficiency. In addition, compared with conventional OMA, NOMA offers better user fairness. The cooperative relaying technique can improve the performance and extend the coverage of wireless networks [6,7]. Naturally, this technique can be applied in NOMA networks and attracts a number of researchers to focus on this topic [8–12]. The work [8] proposed a cooperative NOMA transmission scheme that fully exploits prior information available in NOMA systems, in which the users with better channel conditions decode the messages of the others. Prior information is used as relays to improve the reception reliability for users with poor connections. The authors of [9] investigated the NOMA cooperative relaying system and proposed the best relay selection (BRS) scheme. The result has shown that the NOMA-based BRS obtains more rate gain than the conventional BRS when a number of relays becomes large. The works of [10,11] studied the NOMA cooperative relaying system with energy harvesting. Another communication protocol for cooperative NOMA system was proposed in [12]. The authors concluded that this proposed protocol can overcome the problem of the direct link between the paired users unavailable due to weak transmission conditions.

In the information age, security of information is the most essential issue to ensure that confidential information cannot be used by illegitimate users. However, due to the broadcast nature of wireless communications, the information transmission between transceivers can be eavesdropped by wiretappers which are difficult to detect. Although there are a number of solutions to solve this problem, such as RSA (Rivest Shamir Adleman) and DES (Data Encryption Standard), most of them are applied at higher layers, i.e., application or network layers. Moreover, the conditions at such higher layers assume that the link between the transmitter and receiver (physical layer) is error-free and that eavesdroppers have restricted computational power and lack efficient algorithms [13]. In order to enhance the security of wireless networks, the physical layer secrecy (PLS) is proposed to achieve secure transmission by exploiting the dynamic characteristics of the transmission channels [14–18]. This approach can be applied to NOMA relaying networks to improve the secrecy ability of NOMA communication networks. However, the employment of successive interference cancellation (SIC) in NOMA technique makes the secrecy performance analysis of the physical layer secrecy of NOMA different from that of conventional OMA technique. Recently, there are a number of works focusing on the physical layer secrecy of NOMA relaying being networks published [19–23]. The PLS of a downlink NOMA system was investigated in [19], in which users' quality of service (QoS) requirements to perform NOMA and all channels are assumed to undergo Nakagami-m fading. The results have shown that better secrecy performance of overall communication process can be obtained when there is not much difference in the level of priority between legitimate users. The work in [20] presented the secrecy performance analysis of a two-user downlink NOMA system. The authors considered two schemes those are single-input and single-output and multiple-input and single-output systems with different transmit antenna selection (TAS). The exact and approximated closedform expressions of the secrecy outage performance (SOP) for different TAS schemes were derived. The results have shown that when increasing the transmit power, the SOP for the far user with fixed power allocation scheme degraded as the transmit power beyond the threshold and then reaches a floor as the interference from the near user increases. The authors in [21] investigated the PLS of simple NOMA model of large-scale networks through the SOP. In this model, stochastic geometry approaches were used to model the locations of NOMA users and eavesdroppers. In [22], the artifical noise is generated at the base station that can improve the security of a beamforming-aided multiple-antenna system. The secrecy beamforming scheme for multiple-input single-output non-orthogonal multiple access (MISO-NOMA) systems is proposed. In this proposed scheme, the artificial noise is used to protect the confidential information of two NOMA assisted legitimate users, such that the system secrecy performance improved. The authors of [23] studied the PLS for cooperative NOMA systems, in which the amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. They concluded that AF and DF schemes almost achieve the same secrecy performance and this secrecy performance is independent of the channel conditions between the relay and the poor user.

Unlike the above works, in this work, we consider the PLS of a downlink NOMA cooperative relay communication system combining with artifical noise. In other words, we study the PLS performance of the NOMA system in which the base station (BS) simultaneously transmits information to user pairs based on power-domain, and then users with better channel conditions (better user) relay information to the worse user assuming that the eavesdropper only tries to listen to the worse users information. In order to ensure the PLS performance, artificial noise is used in BS to confuse the eavesdropper. Given the considered networks, our work provides the following contributions:

1. The artificial noise with cooperative transmission scheme, namely ANCOTRAS, is proposed.
2. The lower bound and exact closed-form expressions of secrecy outage probability for each user and overall system are derived.
3. By means of secrecy outage probability expressions, we carry out evaluating the PLS performance.
4. The behavior of the considered system is assessed with respect to different key parameters, such as power allocation ratio, average transmit power and number of user pair.

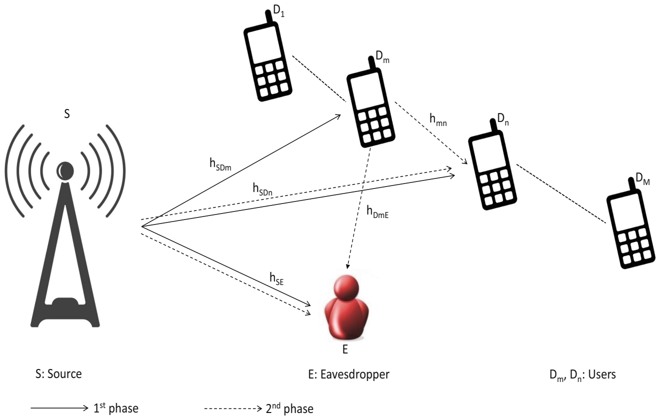

Fig. 1. System model for secured cooperative NOMA

The rest of this paper is organized as follows. The system model is presented in Sect. 2. Secrecy performance of the considered system is analyzed in Sect. 3. The numerical results are shown in Sect. 4. Finally, Sect. 5 draws the conclusion of our paper

2 Network and Channel Models

A cooperative communication system for downlink NOMA is considered as the Fig. 1. One source S, i.e., base station, intends to transmit information to M mobile users denoted as D_i, $(i = 1 \leq m < n \leq M)$ in the presence of an eavesdropper E. In this considered system, we can divided M users into multiple pairs, such as $\{D_m, D_n\}, m < n$, to perform NOMA [8] and these two paired users help to forward information signals to each other. It means that the m^{th} user and the n^{th} user are paired to perform cooperative NOMA. The better user D_m forward the information of the worse user D_n after use applying successive interference cancellation (SIC) to detect the D_m's signal.

The two-phase ANCOTRAS protocol of this considered system is proposed as follows

- In the first phase: S transmits information signal $x = \sqrt{a_m}s_m + \sqrt{a_n}s_n$ with power P_S to user pair $\{D_m, D_n\}$ in the time of αT $(0 < \alpha < 1, T$ is block time), where s_m and s_n are the message for the m^{th} user D_m and the n^{th} user D_n, respectively; a_m and a_n are the power allocation coefficients that satisfy the conditions: $0 < a_m < a_n$ and $a_m + a_n = 1$ by following the NOMA scheme.
- In the second phase: Applying NOMA, D_m uses SIC to detect message s_n and subtracts this component from the received signal to obtain its own message s_m, then decodes and forwards s_n to D_n in the time of $(1 - \alpha T)$. By this time, the S cooperates with D_m to broadcast an artificial noise to confuse

the eavesdropper. Finally, D_n combines two received signals, i.e., the direct signal from the S and the relaying signal from D_m, to decode its own message by using selection combining (SC) technique.

Meanwhile, the eavesdropper tries to extract the poor user's message s_n from the links $S - D_n$ and $D_m - D_n$.

Without loss of generality, assume that all the channel gains between S and users follow the order of $|h_{SD_1}|^2 \leq |h_{SD_2}|^2 \leq ... \leq |h_{SD_m}|^2 \leq |h_{SD_n}|^2 \leq ... \leq |h_{SD_M}|^2$ are decoded as the ordered channel gains of the m^{th} user and the n^{th} user. Denote that $|h_{mn}|^2$ is the channel gains of the links between the m^{th} user and the n^{th} user; $|h_{SE}|^2$ and $|h_{DmE}|^2$ are channel gains of the links of $S-E$ and $D_m - E$, respectively. We assume that all the nodes are single-antenna devices and operate in a half-duplex mode. All wireless links are assumed to undergo independent frequency non-selective Rayleigh block fading and additive white Gaussian noise (AWGN) with zero mean and the same variance σ^2. We denote $d_{SD_m}, d_{SD_n}, d_{mn}, d_{SE}, d_{DmE}$ as the Euclidean distances of $S-D_m, S-D_n, D_m-D_n, S-E, D_m-E$, respectively and θ denote the path-loss exponent.

2.1 The First Phase

In this phase, the source S broadcasts information to the users. The received signals at D_m and at D_n are

$$y_{SD_m} = \sqrt{\frac{P_S}{d^{\theta}_{SD_m}}}(\sqrt{a_m}s_m + \sqrt{a_n}s_n)h_{SD_m} + n_{SD_m}, \tag{1}$$

$$y_{SD_n} = \sqrt{\frac{P_S}{d^{\theta}_{SD_n}}}(\sqrt{a_m}s_m + \sqrt{a_n}s_n)h_{SD_n} + n_{SD_n}, \tag{2}$$

respectively, where n_{SD_m} and n_{SD_n} are the AWGN with zero mean and variance σ^2.

Let $X_1 \triangleq |h_{SD_m}|^2, Y_1 \triangleq |h_{SD_n}|^2, X_2 \triangleq |h_{mn}|^2, Z_1 \triangleq |h_{SE}|^2$, and $Z_2 \triangleq |h_{DmE}|^2$. The instantaneous SINR at the n^{th} user to detect s_n transmitted from S can be given by

$$\gamma_{SD_n} = \frac{a_n\bar{\gamma}|h_{SD_n}|^2}{a_m\bar{\gamma}|h_{SD_n}|^2 + d^{\theta}_{SD_n}} = \frac{b_2 Y_1}{b_1 Y_1 + 1}, \tag{3}$$

where $\bar{\gamma} = \frac{P_S}{\sigma^2}$ is denoted as the average transmit SNR of $S - D_n$ link, $b_1 = \frac{a_m\bar{\gamma}}{d^{\theta}_{SD_n}}, b_2 = \frac{a_n\bar{\gamma}}{d^{\theta}_{SD_n}}$.

Similarly, the instantaneous SINR at the m^{th} user to detect s_n transmitted from S can be written as

$$\gamma^{s_n}_{SD_m} = \frac{a_m\bar{\gamma}|h_{SD_m}|^2}{a_n\bar{\gamma}|h_{SD_m}|^2 + d^{\theta}_{SD_m}} = \frac{b_4 X_1}{b_3 X_1 + 1}, \tag{4}$$

where $b_3 = \frac{a_m\bar{\gamma}}{d^{\theta}_{SD_m}}, b_4 = \frac{a_n\bar{\gamma}}{d^{\theta}_{SD_m}}$.

At the same time, the received signal at E is given as follows

$$y_{SE} = \sqrt{\frac{P_S}{d_{SE}^{\theta}}}(\sqrt{a_m}s_m + \sqrt{a_n}s_n)h_{SE} + n_{SE}, \tag{5}$$

where n_{SE} is the AWGN with zero mean and variance σ_E^2. Due to assuming that the eavesdropper only tries to detect s_n, therefore the instantaneous SINR at E is given by

$$\gamma_{SE} = \frac{a_n\bar{\gamma}_E|h_{SE}|^2}{a_m\bar{\gamma}_E|h_{SE}|^2 + d_{SE}^{\theta}} = \frac{b_6 Z_1}{b_5 Z_1 + 1}, \tag{6}$$

where $b_5 = \frac{a_m\bar{\gamma}_E}{d_{SE}^{\theta}}, b_6 = \frac{a_n\bar{\gamma}_E}{d_{SE}^{\theta}}$.

2.2 The Second Phase

In this phase, D_m uses the power P_{Dm} to forward s_n to D_n and S simultaneously uses the power P_S to broadcast an AN to users and eavesdrooper. The instantaneous SINR at D_n in the second phase is as follows

$$\gamma_{mn} = U_1 = \frac{c_1 X_2}{c_3 Y_1 + 1}, \tag{7}$$

where $c_1 = \frac{\bar{\gamma}_{Dm}}{d_{mn}^{\theta}}$, $c_3 = \frac{\bar{\gamma}}{d_{SDn}^{\theta}}$, $\bar{\gamma}_{Dm} = \frac{P_{Dm}}{\sigma^2}$.

Similarly, the instantaneous SINR at E in this phase is given by

$$\gamma_{DmE} = U_2 = \frac{c_2 Z_2}{c_4 Z_1 + 1}, \tag{8}$$

where $c_2 = \frac{\bar{\gamma}_{DmE}}{d_{DmE}^{\theta}}$, $c_4 = \frac{\bar{\gamma}_E}{d_{SE}^{\theta}}$, $\bar{\gamma}_{DmE} = \frac{P_{Dm}}{\sigma_E^2}$.

Considering i.i.d. Rayleigh channels, the channel gains $|h_{SDm}|^2, |h_{SDn}|^2$, $|h_{SE}|^2$ and $|h_{mn}|^2$ follow exponential distributions with parameters $\lambda_{SDm}, \lambda_{SDn}$, λ_{SE} and λ_{mn}, respectively. In order statistics, the probability density function (PDF) and the cumulative distribution function (CDF) of U, where $U \in \{X_1, Y_1\}$, are respectively given by [24]

$$f_U(x) = \frac{M!}{(M-i)!(i-1)!}\frac{1}{\lambda_{SDi}}\sum_{k=0}^{i-1} C_k^{i-1}(-1)^k e^{\frac{-x(M-i+k+1)}{\lambda_{SDi}}} \tag{9}$$

$$F_U(x) = \frac{M!}{(M-i)!(i-1)!}\sum_{k=0}^{i-1} C_k^{i-1}(-1)^k \frac{1}{M-i+k+1}\left[1 - e^{\frac{-x(M-i+k+1)}{\lambda_{SDi}}}\right] \tag{10}$$

where $i \in \{m, n\}$.

The PDF and CDF of V, where $V \in (X_2, Z_1, Z_2)$ are respectively expressed as

$$f_V(x) = \frac{1}{\lambda}e^{-\frac{x}{\lambda}} \tag{11}$$

$$F_V(x) = 1 - e^{-\frac{x}{\lambda}} \tag{12}$$

where $\lambda \in \{\lambda_{mn}, \lambda_{SE}, \lambda_{DmE}\}$.

For further calculation, we derive CDFs and PDFs of $\gamma_{SD_m}^{s_n}, \gamma_{SD_n}, \gamma_{SE}$, $\gamma_{mn}, \gamma_{D_mE}$. From above results, we calculate the CDF of γ_{SDn} as follows

$$\begin{aligned} F_{\gamma_{SDm}^{s_n}}(x) &= Pr\left(\frac{b_4X_1}{b_3X_1+1} < x\right) \overset{(a)}{=} F_{X_1}\left(\frac{x}{b_4 - b_3x}\right) \\ &= \frac{M!}{(M-m)!(m-1)!}\sum_{k=0}^{m-1} C_k^{m-1}(-1)^k \\ &\times \frac{1}{M-m+k+1}\left[1 - e^{\frac{-(M-m+k+1)x}{\lambda_{SDm}}}\right], \end{aligned} \tag{13}$$

$$\begin{aligned} F_{\gamma_{SDn}}(x) &= Pr\left(\frac{b_2Y_1}{b_1Y_1+1} < x\right) \overset{(b)}{=} F_{Y_1}\left(\frac{x}{b_2 - b_1x}\right) \\ &= \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k \\ &\times \frac{1}{M-n+k+1}\left[1 - e^{\frac{-(M-n+k+1)x}{\lambda_{SDn}}}\right]. \end{aligned} \tag{14}$$

Note that step (a) and (b) are obtained by assuming the following condition holds $x < \frac{b_2}{b_1}$, $x < \frac{b_4}{b_3}$, respectively.

Similarly, we respectively derive the CDF and PDF of γ_{SE} as follows

$$\begin{aligned} F_{\gamma_{SE}}(x) &= Pr\left(\frac{b_6Z_1}{b_5Z_1+1} < x\right) \overset{(c)}{=} F_{Z_1}\left(\frac{x}{b_6 - b_5x}\right) \\ &= 1 - e^{-\frac{x}{\lambda_{SE}(b_6 - b_5x)}}, \end{aligned} \tag{15}$$

$$f_{\gamma_{SE}}(x) = \frac{b_6}{\lambda_{SE}(b_6 - b_5x)^2} e^{-\frac{x}{\lambda_{SE}(b_6 - b_5x)}}. \tag{16}$$

Note that step (c) is obtained by assuming the following condition holds $x < \frac{b_6}{b_5}$.

The CDF of the γ_{mn} is calculated as follows

$$\begin{aligned} F_{\gamma_{mn}}(x) &= \Pr\left(\frac{c_1X_2}{c_3Y_1+1} < x\right) \\ &= \int_0^\infty F_{X_2}\left(\frac{x(c_3y+1)}{c_1}\right) f_{Y_1}(y)dy \\ &= 1 - \frac{M!}{(M-n)!(n-1)!}\frac{1}{\lambda_{SDn}}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k \int_0^\infty e^{-\frac{x(c_3y+1)}{c_1\lambda_{mn}} - \frac{y(M-n+k+1)}{\lambda_{SDn}}} dy \\ &= 1 - \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k \\ &\times \frac{c_1\lambda_{mn}}{c_3\lambda_{SDn}x + c_1\lambda_{mn}(M-n+k+1)} e^{-\frac{x}{c_1\lambda_{mn}}}. \end{aligned} \tag{17}$$

Similarly the CDF of the γ_{D_mE} is given by

$$\begin{aligned}F_{\gamma_{D_mE}}(x) &= \Pr\left(\frac{c_2Z_2}{c_4Z_1+1} < x\right)\\ &= \int_0^{\infty} F_{Z_2}\left(\frac{x(c_4y+1)}{c_2}\right) f_{Z_1}(y)dy\\ &= 1 - \frac{1}{\lambda_{SE}}\int_0^{\infty} e^{-\frac{x(c_4y+1)}{c_2\lambda_{DmE}}-\frac{y}{\lambda_{SE}}}dy\\ &= 1 - \frac{c_2\lambda_{DmE}}{c_4\lambda_{SE}x+c_2\lambda_{DmE}}e^{-\frac{x}{c_2\lambda_{DmE}}}. \end{aligned} \tag{18}$$

The PDF of the γ_{D_mE} is expressed as follows

$$f_{\gamma_{D_mE}}(x) = \left(\frac{c_2c_4\lambda_{DmE}\lambda_{SE}}{(c_4\lambda_{SE}x+c_2\lambda_{DmE})^2} + \frac{1}{(c_4\lambda_{SE}x+c_2\lambda_{DmE})}\right)e^{-\frac{x}{c_2\lambda_{DmE}}}. \tag{19}$$

3 Secrecy Performance Analysis

In this section, secrecy performance is analized in terms of secrecy outage probability. Secrecy outage probability (SOP) is an important performance metric that is usually used to characterize the secrecy performance of a wireless communication system. Here, we analyze the secrecy performance in terms of SOP at S and at D_m with assuming that E tries to extract the message of D_n.

3.1 Preliminaries

The instantaneous capacities of legitimate channel and eavesdropper channel can be respectively defined by

$$C_M = B\log(1+\gamma_M), \tag{20}$$

$$C_N = B\log(1+\gamma_N), \tag{21}$$

where B is bandwith (Hertz), $\gamma_M \in \{\gamma_{SD_m}, \gamma_{SD_n}, \gamma_{mn}\}$, $\gamma_N \in \{\gamma_{SE}, \gamma_{D_mE}\}$.

The instantaneous secrecy capacity for $S-D_m$, $S-D_n$ and D_mD_n are given by

$$\begin{aligned}C_{S_1} &= \left[C_{\gamma_{SD_m}^{s_n}} - C_{\gamma_{SE}}\right]^+\\ &= \begin{cases}\alpha\log_2\left(\frac{1+\gamma_{SD_m}^{s_n}}{1+\gamma_{SE}}\right), & \gamma_{SD_m}^{s_n} > \gamma_{SE}\\ 0, & \gamma_{SD_m}^{s_n} \le \gamma_{SE}\end{cases}, \end{aligned} \tag{22}$$

$$\begin{aligned}C_{S_2} &= \left[C_{\gamma_{SD_n}} - C_{\gamma_{SE}}\right]^+\\ &= \begin{cases}\alpha\log_2\left(\frac{1+\gamma_{SD_n}}{1+\gamma_{SE}}\right), & \gamma_{SD_n} > \gamma_{SE}\\ 0, & \gamma_{SD_n} \le \gamma_{SE}\end{cases}, \end{aligned} \tag{23}$$

$$C_{S_3} = \left[C_{\gamma_{mn}} - C_{\gamma_{D_m E}}\right]^+ = \begin{cases} (1-\alpha)\log_2\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_m E}}\right), & \gamma_{mn} > \gamma_{D_m E} \\ 0, & \gamma_{mn} \le \gamma_{D_m E} \end{cases} \tag{24}$$

respectively. Here, for simplicity we assume $B = 1\,\text{Hz}$.

SOP is defined as the probability that the instantaneous secrecy capacity falls below a predetermined secrecy rate threshold $R_S > 0$, given by $SOP = Pr(C_S < R_S)$. Notice that, in this considered system we only consider the case of the eavesdropper attempting to hear the message of D_n at S and at D_m. In the next subsection, we present the calculation the SOPs at S and at D_m.

3.2 Secrecy Outage Probability at *S*

The secrecy outage probability at S of $S - D_n$ link (SOP_1) can be calculated as follows

$$\begin{aligned} SOP_1 = \Pr(C_{S_1} < R_S) &= Pr\left(\frac{1+\gamma_{SD_n}}{1+\gamma_{SE}} < 2^{R_S/\alpha}\right) \\ &= 1 - Pr\left(\gamma_{SE} < \frac{1+\gamma_{SD_n} - 2^{R_S/\alpha}}{2^{R_S/\alpha}}\right). \end{aligned} \tag{25}$$

Because Eq. (25) is intractable to obtain the closed-form expression, here we only obtain the lower bound of SOP_1.

From the Eq. (3), we have $\gamma_{SD_n} < \frac{a_n}{a_m}$, therefore the lower bound of SOP_1 is calculated as follows

$$\begin{aligned} SOP_1 > SOP_{1_{lower}} &= 1 - CDF_{\gamma_{SE}}\left(\frac{1+\frac{a_n}{a_m}}{2^{R_S/\alpha}} - 1\right) \\ &= e^{-\frac{\beta}{\lambda_{SE}(b_6 - b_5\beta)}}, \end{aligned} \tag{26}$$

where $\beta = \frac{1+\frac{a_n}{a_m}}{2^{R_S/\alpha}} - 1$.

Similarly, for SOP at S of $S - D_m$ link ($SOP_2 = \Pr(C_{S_2} < R_S)$), the lower bound $SOP_{2_{lower}}$ is the same as $SOP_{1_{lower}}$:

$$SOP_2 > SOP_{2_{lower}} = e^{-\frac{\beta}{\lambda_{SE}(b_6 - b_5\beta)}}. \tag{27}$$

3.3 Secrecy Outage Probability at D_m

In this scenario, the secrecy outage event occurs when D_m cannot detect s_n or D_m can detect s_n but the secrecy capacity is below the secrecy threshold. Therefore, the secrecy outage probability at the D_m is calculated as follows

$$\begin{aligned} SOP_3 &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_3} < R_S) \\ &= \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right) \\ &+ \left[1 - \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right)\right] \Pr\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_m E}} < 2^{\frac{R_S}{1-\alpha}}\right). \end{aligned} \tag{28}$$

Proposition 1. *Under Rayleigh fading, the SOP of the link $D_m - D_n$ with AN is given by*

$$SOP_3 = \varPhi_1 + (1 - \varPhi_1)(1 - \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k(\varPhi_2 + \varPhi_3)), \quad (29)$$

where

$$\varPhi_1 = \begin{cases} \frac{M!}{(M-m)!(m-1)!}\sum\limits_{k=0}^{m-1}(-1)^k C_k^{m-1}\frac{1}{M-m+k+1}\left[1 - e^{-\frac{\gamma_t(M-m+k+1)}{(b_4-b_3\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m}, \\ 1, & \gamma_t > \frac{a_n}{a_m}, \end{cases}$$

$$\varPhi_2 = c_1c_2c_4\lambda_{DmE}\lambda_{SE}\lambda_{mn}e^{-\frac{2^{\frac{R_S}{(1-\alpha)}}-1}{c_1\lambda_{mn}}}\left[\frac{ce^{\frac{d\mu}{c}}\varGamma(0,\frac{d\mu}{c})}{(ad-bc)^2} - \frac{ce^{\frac{b\mu}{a}}\varGamma(0,\frac{b\mu}{a})}{(ad-bc)^2} + \frac{\mu e^{\frac{b\mu}{a}}\varGamma(-1,\frac{b\mu}{a})}{a(ad-bc)^2}\right],$$

$$\varPhi_3 = c_1\lambda_{mn}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}}\left[\frac{1}{ad-bc}e^{\frac{b}{a}\mu}\varGamma(0,\frac{b}{a}\mu) - \frac{1}{ad-bc}e^{\frac{d}{c}\mu}\varGamma(0,\frac{d}{c}\mu)\right].$$

Denoted that, $a = c_4\lambda_{SE}, b = c_2\lambda_{DmE}, c = c_3\lambda_{SDn}2^{R_S/(1-\alpha)}, d = c_3\lambda_{SDn}$ $(2^{R_S/(1-\alpha)} - 1) + c_1\lambda_{mn}(M - n + k + 1), \mu = \frac{2^{R_S/(1-\alpha)}}{c_1\lambda_{mn}} + \frac{1}{c_2\lambda_{DmE}}$.

Proof. See Appendix A.

4 Numerical Results and Discussion

In this section, we investigate the physical layer secrecy performance of ANCOTRAS protocol for this considered cooperative NOMA system by numerical results. Monte-Carlo simulation results are also provides to verify our analytical results. In this simulation, it is assumed that the power allocation coefficients of NOMA are $a_m = 0.3, a_n = 0.7$. The targeted data rates for the selected NOMA user pair are assumed to be $R_s = 0.5$ bit per channel use.

4.1 Secrecy Outage Probability at S

Figures 2 and 3 describe the result of SOP of the system at S. These figures show then when we crease d_{SE},$\bar{\gamma}$ then PLS at the S decreases. This mean that the PLS capability of this model increases. Besides, in the two results, when we increase $\bar{\gamma_E}$, the SOP at S of the system also increases.

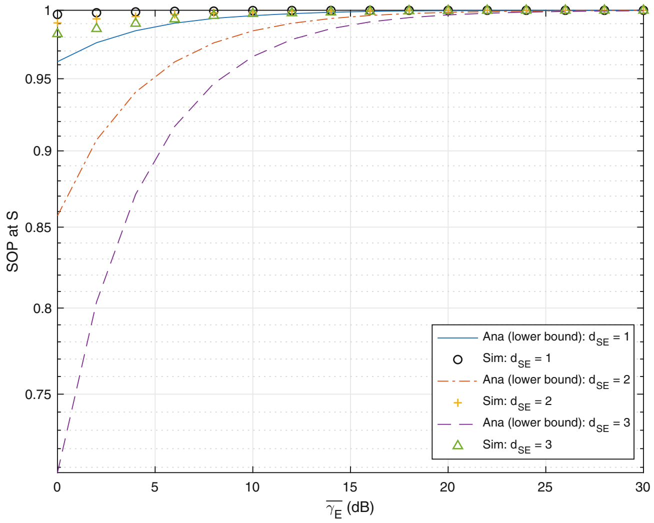

Fig. 2. The SOP at the Base Station versus $\overline{\gamma_E}$ with the change of d_{SE} and $d_{SDm} = 1$, $d_{SDn} = 2$, $\alpha = 0.3$, $M = 4$, $m = 2$, $n = 3$

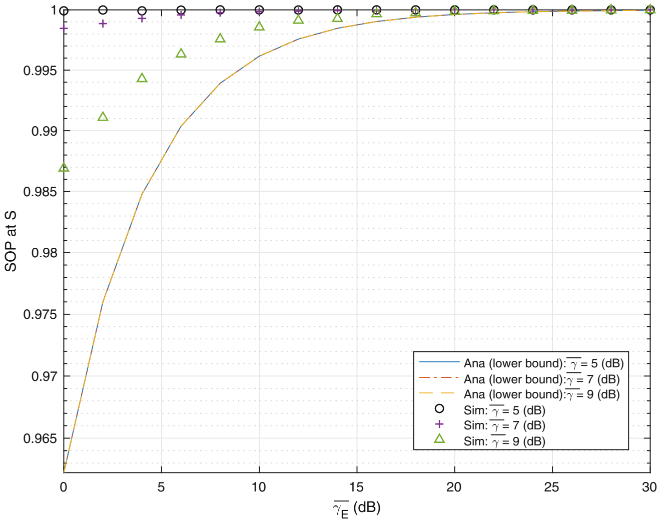

Fig. 3. The *SOP* at the Base Station versus $\bar{\gamma_E}$ with the change of $\bar{\gamma}$ and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, M = 4, m = 2, n = 3$

4.2 Secrecy Outage Probability at D_m

Figure 4, shows the results of the SOP at D_m versus $\gamma_{\bar{D}m}$. In this simulation result, we can see that when the $\gamma_{\bar{D}m}$ increases, the SOP at D_m decreases, meaning that the physical layers security performance increases. This simulation

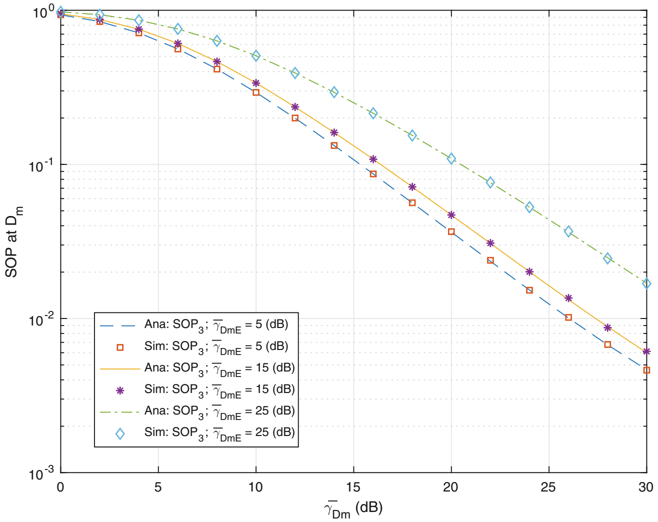

Fig. 4. The SOP at the Base Station versus $\gamma_{\bar{D}m}$ with the change of $\gamma_{D\bar{m}E}$ and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, M = 4, m = 2, n = 3$

result also shows SOP at D_m increases when we increase $\gamma_{D\bar{m}E}$. That is when the system's physical layers security performance will decrease if the average SNR of the signal from D_m to E increases. The SOP at D_m simulation result when changing AN power transmit from S to D_n is shown in Fig. 5. In this figure, we investigated the SOP at D_m versus $\gamma_{\bar{D}m}$ and $\bar{\gamma}$. Similar to Fig. 4, the simulation results show that when increasing $\gamma_{\bar{D}m}$, the SOP at D_m decreases. In particular, when $\bar{\gamma}$ increases, the SOP at D_m increases. This means that when S transmitted AN to D_n, the signal received at D_n from D_m will be affected.

When changing $\gamma_{\bar{E}}$ and $\gamma_{\bar{D}m}$, we have the simulation results as shown in Fig. 6. In this figure, we can see that, when $\gamma_{\bar{E}}$ increases, the SOP at D_m decreases, meaning that the system's physical layer security performance is improved. The reason is that when the transmitted power of AN from S to E increases, the ratio of the signal received from the D_m at E will decrease, so the ability to decode the signal from D_n of E will decrease. Thus increasing the physical layer security performance of the system. Figure 7 is the SOP at D_m simulation result versus $\bar{\gamma}$. Based on this result, we can once again confirm that using AN will help to improve the system's physical layer security performance. Specifically, when $\gamma_{\bar{E}}$ increases, the SOP at D_m decreases. However, this result also shows that, when $\bar{\gamma}$ increases, the SOP at D_m will increase.

The system has many users, Fig. 8 is the SOP at D_m simulation result when there is a change in the number of users. Based on the simulation results, we see that when the number of users increases, the SOP at D_m will decrease, meaning that the system's physical layer security performance increases.

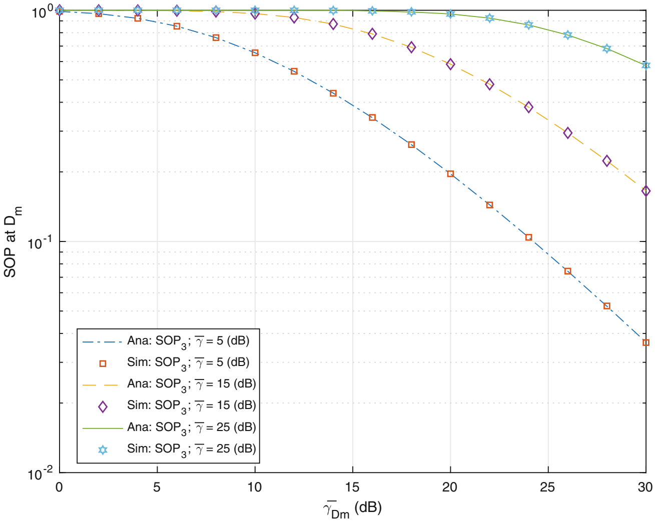

Fig. 5. The *SOP* at the Base Station versus $\gamma_{\bar{D}m}$ with the change of $\bar{\gamma}$ and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, M = 4, m = 2, n = 3$

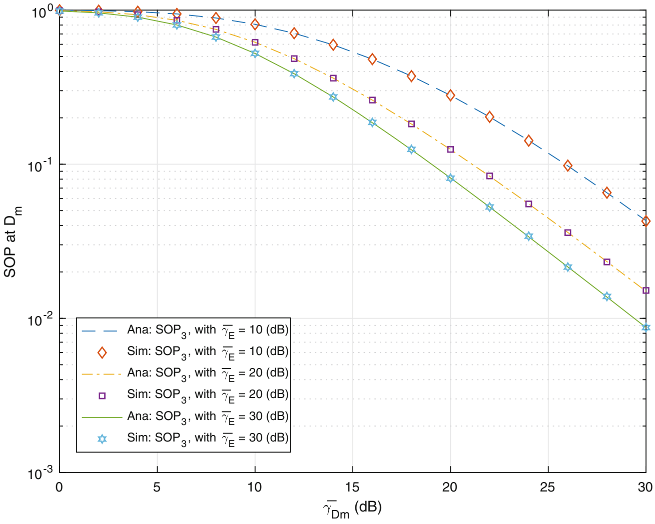

Fig. 6. The *SOP* at the Base Station versus $\gamma_{\bar{D}m}$ with the change of $\bar{\gamma_E}$ and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, M = 4, m = 2, n = 3$

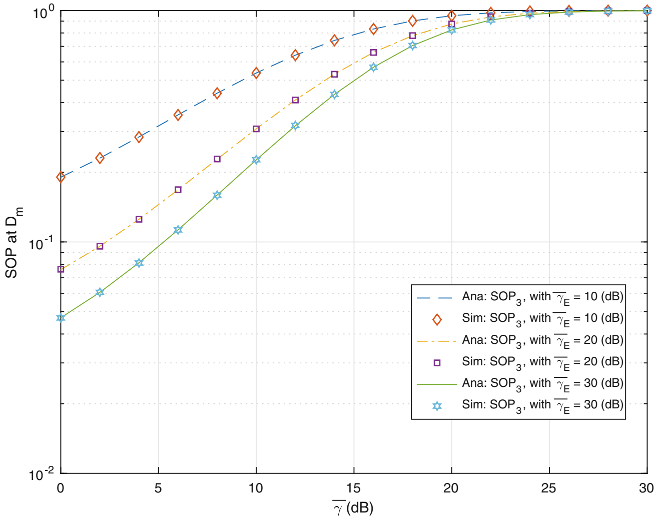

Fig. 7. The SOP at the Base Station versus $\bar{\gamma}$ with the change of $\bar{\gamma_E}$ and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, M = 4, m = 2, n = 3$

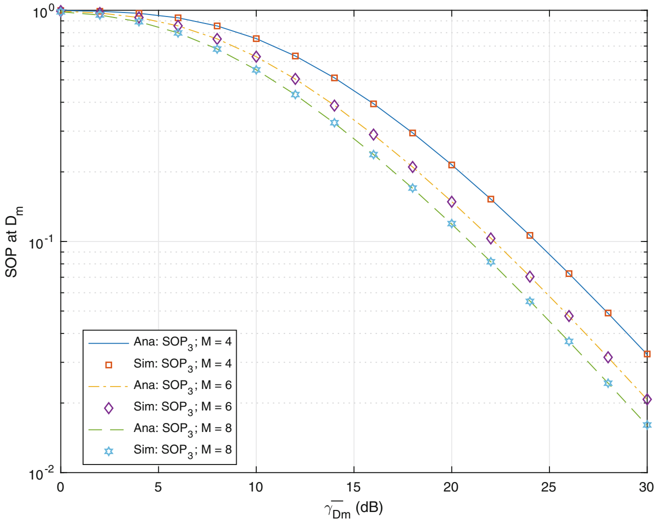

Fig. 8. The SOP at the Base Station versus $\gamma_{\bar{D}m}$ with the change of M and $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3, m = 2, n = 3$

5 Conclusion

In this paper, the secrecy performance of (NOMA) in a downlink cooperative network with simultaneous wireless information and artificial noise was examined. Specifically, we used a method to broadcast artificial noise from the base station after signaling to prevent devices from eavesdropping on exchanged messages. In addition, new analytical expressions were derived in terms of the secrecy outage probability to determine the system secrecy performance. Meanwhile, the numerical results were presented to validate the analyses. Based on the analyses and simulations, we can conclude that the security performance of the network model proposed in this paper depends on the average transmit SNR: from (1) base station to better user; worse users; eavesdropping device; (2) from good users to bad users, eavesdropping devices and (3) number of users of the system. Using artificial noise can improve the security performance of the system.

Appendix A

Here, we derive the expression of SOP at D_m in the case of with AN.

$$\begin{aligned}
SOP_3 &= \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right) + \left(1 - \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right)\right)\Pr\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_mE}} < 2^{R_S/(1-\alpha)}\right)\\
&= \varPhi_1 + (1-\varPhi_1)\int_0^\infty F_{U_1}(2^{R_S/(1-\alpha)}(1+y)-1)f_{U_2}(y)dy\\
&= \varPhi_1 + (1-\varPhi_1)\Bigg[1 - \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1}C_k^{n-1}(-1)^k\\
&\times \int_0^\infty \frac{c_1\lambda_{mn}}{c_3\lambda_{SDn}(2^{R_S/(1-\alpha)}(1+y)-1)+c_1\lambda_{mn}(M-n+k+1)}e^{-\frac{(2^{R_S/(1-\alpha)}(1+y)-1)}{c_1\lambda_{mn}}}\\
&\times \left(\frac{c_2c_4\lambda_{DmE}\lambda_{SE}}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})^2} + \frac{1}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})}\right)e^{-\frac{y}{c_2\lambda_{DmE}}}dy\Bigg]\\
&= \varPhi_1 + (1-\varPhi_1)(1 - \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1}C_k^{n-1}(-1)^k(\varPhi_2+\varPhi_3)),
\end{aligned} \tag{30}$$

where γ_t is the threshold to detect s_n and $\varPhi_1, \varPhi_2, \varPhi_3$ are calculated as follows

$$\begin{aligned}
\varPhi_1 &= F_{X_1}\left(\frac{\gamma_t}{b_4 - b_3\gamma_t}\right)\\
&= \begin{cases} \frac{M!}{(M-m)!(m-1)!}\sum\limits_{k=0}^{m-1}(-1)^kC_k^{m-1}\frac{1}{M-m+k+1}\left[1 - e^{-\frac{\gamma_t(M-m+k+1)}{(b_4-b_3\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m}\\ 1, & \gamma_t > \frac{a_n}{a_m} \end{cases}
\end{aligned}$$

$$\begin{aligned}
\Phi_2 &= \int_0^\infty \frac{c_1\lambda_{mn}}{c_3\lambda_{SDn}(2^{R_S/(1-\alpha)}(1+y)-1)+c_1\lambda_{mn}(M-n+k+1)} e^{-\frac{(2^{R_S/(1-\alpha)}(1+y)-1)}{c_1\lambda_{mn}}} \\
&\times \frac{c_2c_4\lambda_{DmE}\lambda_{SE}}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})^2} e^{-\frac{y}{c_2\lambda_{DmE}}}\,dy \\
&= c_1\lambda_{mn}c_2c_4\lambda_{DmE}\lambda_{SE}e^{-\frac{2^{R_S/(1-\alpha)}-1}{c_1\lambda_{mn}}} \int_0^\infty \frac{1}{(ay+b)^2}\frac{1}{cy+d} e^{-\left(\frac{1}{c_2\lambda_{DmE}}+\frac{2^{R_S/(1-\alpha)}}{c_1\lambda_{mn}}\right)y} dy \\
&= c_1\lambda_{mn}c_2c_4\lambda_{DmE}\lambda_{SE}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}} \left[\int_0^\infty \frac{E_1}{cy+d}e^{-\mu y}dy + \int_0^\infty \frac{E_2}{ay+b}e^{-\mu y}dy\right. \\
&\left.+ \int_0^\infty \frac{E_3}{(ay+b)^2}e^{-\mu y}dy\right] \\
&= c_1\lambda_{mn}c_2c_4\lambda_{DmE}\lambda_{SE}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}} \left[\frac{E_1}{c}e^{\frac{d}{c}\mu}\Gamma(0,\frac{d}{c}\mu) + \frac{E_2}{a}e^{\frac{b}{a}\mu}\Gamma(0,\frac{b}{a}\mu)\right. \\
&\left.+ \frac{E_3}{a^2}\mu e^{\frac{b}{a}\mu}\Gamma(-1,\frac{b}{a}\mu)\right]. \qquad (31)
\end{aligned}$$

$$\begin{aligned}
\Phi_3 &= \int_0^\infty \frac{c_1\lambda_{mn}}{c_3\lambda_{SDn}(2^{R_s}(1+y)-1)+c_1\lambda_{mn}} e^{-\frac{(2^{R_s}(1+y)-1)}{c_1\lambda_{mn}}} \\
&\times \frac{1}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})} e^{-\frac{y}{c_2\lambda_{DmE}}}\,dy \\
&= c_1\lambda_{mn}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}} \int_0^\infty \frac{1}{ay+b}\frac{1}{cy+d} e^{-\left(\frac{1}{c_2\lambda_{DmE}}+\frac{2^{R_s}}{c_1\lambda_{mn}}\right)y} dy \\
&= c_1\lambda_{mn}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}} \left[\int_0^\infty \frac{F_1}{cy+d}e^{-\mu y}dy + \int_0^\infty \frac{F_2}{ay+b}e^{-\mu y}dy\right] \\
&= c_1\lambda_{mn}e^{-\frac{2^{R_s}-1}{c_1\lambda_{mn}}} \left[\frac{F_1}{c}e^{\frac{d}{c}\mu}\Gamma(0,\frac{d}{c}\mu) + \frac{F_2}{a}e^{\frac{b}{a}\mu}\Gamma(0,\frac{b}{a}\mu)\right]
\end{aligned}$$

Denoted that $a = c_4\lambda_{SE}, b = c_2\lambda_{DmE}, c = c_3\lambda_{SDn}2^{R_S/(1-\alpha)}, d = c_3\lambda_{SDn}(2^{R_S/(1-\alpha)} - 1) + c_1\lambda_{mn}(M - n + k + 1), \mu = \frac{2^{R_S/(1-\alpha)}}{c_1\lambda_{mn}} + \frac{1}{c_2\lambda_{DmE}}, E_1 = \frac{c^2}{(ad-bc)^2}, E_2 = -\frac{ac}{(ad-bc)^2}, E_3 = \frac{a}{(ad-bc)}, F_1 = -\frac{c}{ad-bc}, F_2 = \frac{a}{ad-bc}$.

Substituting Φ_1, Φ_2, Φ_3 into (30), we obtain the closed-form expression of SOP for the link $D_m - D_n$ in the case of using AN. This concludes the proof.

References

1. Ding, Z., Yang, Z., Fan, P., Poor, H.V.: On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users. IEEE Signal Process. Lett. **21**(12), 1501–1505 (2014)
2. Dai, L., Wang, B., Yuan, Y., Han, S., Chih-Lin, I., Wang, Z.: Nonorthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. IEEE Commun. Mag. **53**(9), 74–81 (2015)
3. Shimojo, T., Umesh, A., Fujishima, D., Minokuchi, A.: Special articles on 5G technologies toward 2020 deployment. NTT DOCOMO Tech. J. **17**(4), 50–59 (2016)

4. Islam, S.M.R., Avazov, N., Dobre, O.A., Kwak, K.S.: Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges. IEEE Commun. Surv. Tutorials **19**(2), 721–742 (2017)
5. Lee, S., Duong, T.Q., da Costa, D.B., Ha, D.B., Nguyen, S.Q.: Underlay cognitive radio networks with cooperative non-orthogonal multiple access. IET Commun. **12**(3), 359–366 (2018)
6. Suraweera, H.A., Karagiannidis, G.K., Smith, P.J.: Performance analysis of the dual-hop asymmetric fading channel. IEEE Trans. Wirel. Commun. **8**(6), 2783–2788 (2009)
7. Kim, K.J., Duong, T.Q., Poor, H.V.: Performance analysis of cyclic prefixed single-carrier cognitive amplify-and-forward relay systems. IEEE Trans. Wirel. Commun. **12**(1), 195–205 (2013)
8. Ding, Z., Peng, M., Poor, H.V.: Cooperative non-orthogonal multiple access in 5G systems. IEEE Commun. Lett. **19**(8), 1462–1465 (2015)
9. Kim, J.B., Song, M.S., Lee, I.H.: Achievable rate of best relay selection for non-orthogonal multiple access-based cooperative relaying systems. In: International Conference on Information and Communication Technology Convergence (ICTC), Jeju, pp. 960–962. IEEE, South Korea (2016)
10. Liu, Y., Ding, Z., Elkashlan, M., Poor, H.V.: Cooperative nonorthogonal multiple access with simultaneous wireless information and power transfer. IEEE J. Sel. Areas Commun. **34**(4), 936–953 (2016)
11. Ha, D.B., Nguyen, Q.S.: Outage performance of energy harvesting DF relaying NOMA networks. Mob. Netw. Appl. **23**(6), 1572–1585 (2017)
12. Tran, D.D., Tran, H.V., Ha, D.B., Kaddoum, G.: Cooperation in NOMA networks under limited user-to-user communications: solution and analysis. In: IEEE Wireless Communications and Networking Conference (WCNC), 15–18 April 2018, Barcelona, Spain (2018)
13. Ha, D.B., Duong, T.Q., Tran, D.D., Zepernick, H.J., Vu, T.T.: Physical layer secrecy performance over Rayleigh/Rician fading channels. In: The 2014 International Conference on Advanced Technologies for Communications (ATC 2014), 15–17 October 2014, pp. 113–118, Hanoi, Vietnam (2013)
14. Wyner, A.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
15. Bloch, M., Barros, J., Rodrigues, M.R., McLaughlin, S.W.: Wireless information-theoretic security. IEEE Trans. Inf. Tech. **54**(6), 2515–2534 (2008)
16. Ng, D.W.K., Schober, R.: Resource allocation for secure communication in systems with wireless information and power transfer. In: IEEE Globecom Workshops, Atlanta, USA, pp. 1251–1257 (2013)
17. Ha, D.B., Van, P.T., Vu, T.T.: Physical layer secrecy performance analysis over Rayleigh/Nakagami fading channels. In: The World Congress on Engineering and Computer Science 2014 (WCECS2014), 22–24 October 2014, San Francisco, USA (2014)
18. Ha, D.B., Vu, T.T., Duy, T.T., Bao, V.N.Q.: Secure cognitive reactive decode-and-forward relay networks: with and without eavesdropper. Wirel. Pers. Commun. (WPC) **85**(4), 2619–2641 (2015)
19. Tran, D.D., Ha, D.B.: Secrecy performance analysis of QoS-based non-orthogonal multiple access networks over Nakagami-m fading. In: The International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom), HCMC, Vietnam (2018)
20. Lei, H., Zhang, J., Park, K.H., Xu, P., Ansari, I.S., Pan, G.: On secure noma systems with transmit antenna selection schemes. IEEE Access **5**, 17450–17464 (2017)

21. Liu, Y., Qin, Z., Elkashlan, M., Gao, Y., Hanzo, L.: Enhancing the physical layer security of nonorthogonal multiple access in large-scale networks. IEEE Trans. Wirel. Commun. **16**(3), 1656–1672 (2017)
22. Lv, L., Ding, Z., Ni, Q., Chen, J.: Secure MISO-NOMA transmission with artificial noise. IEEE Trans. Veh. Technol. **67**(7), 6700–6705 (2018)
23. Chen, J., Yang, L., Alouini, M.S.: Physical layer security for cooperative NOMA systems. IEEE Trans. Veh. Technol. **67**(5), 4645–4649 (2018)
24. Men, J., Ge, J.: Performance analysic of non-orthogonal multiple access in downlink cooperative network. IET Commun. **9**(18), 2267–2273 (2015)