EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems

Research Article EAI.EU

Enhancing Physical Layer Security for Cooperative Non-Orthogonal Multiple Access Networks with Artificial Noise

Van-Long Nguyen[1,*], Dac-Binh Ha[2], Duc-Dung Tran[2], Yoonill Lee[3]

[1]Graduate School, Duy Tan University, Da Nang, Vietnam
[2]Faculty of Electrical and Electronics Engineering, Duy Tan University, Da Nang, Vietnam
[3]Department of Engineering Technology, Purdue University Northwest, Indiana, USA

Abstract

This paper does the study on the performance of the physical layer secrecy of nonorthogonal multiple access (NOMA) in downlink cooperative. The given system includes one source, multiple legitimate user pairs in the form of an eavesdropper. By applying the decode-and-forward (DF) scheme, a good user will take the information from the source to send it to the bad user in every pair, we assume that the eavesdropper will spend effort to decode the message from the bad user. To enhance the secrecy performance of given system, the artificial noise cooperative transmission scheme named ANCOTRAS is suggested. To assess the performance of the suggested scheme, we obtained the lower bound and exact closed-form expressions of secrecy outage probability by implementing statistical characteristics of signal-to-noise ratio (SNR) and signalto-interference-plus-noise ratio (SINR). Furthermore, the secrecy performance of given system is studied basing on key parameters (including the power allocation ratio), average transmit power and amount of user pair for verifying the suggested scheme. At the end, the accuracy of final analytical outcome is reassured by using the Monte-Carlo simulation results.

Received on 14 July 2019; accepted on 25 July 2019; published on 30 August 2019

Keywords: non-orthogonal multiple access, cooperative network, decode and forward, artificial noise, secrecy outage probability

Copyright © 2019 Van-Long Nguyen *et al.*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/eai.13-7-2018.159945

1. Introduction

In the recent years, the portable devices with wireless features and integrated smart operation system such as smartphones, smart watches or smart home devices became an integral part of human society, all thanks to their flexibility and multi-function. It also leads us to the compromising booming of fifth-generation network (5G) as a replacement for 4G. The reason for this changes are because the growing number of wireless devices also go hand in hand with the need for low cost and low latency networks, which the 4G and earlier generation networks, using tradition orthogonal multiple access (OMA) such as FDMA, TDMA, and CDMA, cannot meet because of the limited channel resource and the spectral efficiency loss. To adapt to the requirements of 5G network, the non-orthogonal multiple access (NOMA) technique is the most promising one requirements[1–5]. With the ability in serving multiple users in the same period of time, frequency or code, NOMA can make sure that the spectral efficiency can be maintained. Besides, the equality of user can be increased in NOMA in comparison with OMA. Furthermore, the cooperative relaying technique which can be applied to NOMA networks can enhance the effectiveness and widen the covered area of the wireless networks [6, 7] and it also can attract the attention of other researchers on this topic[8–12]. In specific, a cooperative NOMA transmission scheme is suggested in the work [8] to

[*]Corresponding author. Email: vanlong.itqn@gmail.com

explore the previous information in NOMA system, in which the better channel condition helps the users decode the message from others. For user having poor connection, the given information takes the form of the relays to increase the reception reliability. The NOMA cooperative relaying system is studied in the work [9] which also suggested the most suitable relay selection (BRS) scheme. In the outcome, it could be seen that in the case of increasing number of relays, the NOMA-based BRS acquired more rate gain than the traditional BRS. The [10, 11] study is NOMA cooperative relaying system with energy harvesting and [12] provided another communication protocol for cooperative NOMA system. In them, the writer give the conclusion that in the weak transmission conditions their protocols can deal with the lack of direct link between the paired users.

Moving to the eavesdropping issue, while the information security is becoming more and more vital in the information age because the value of our confidential information in using for illegal activities, our information become more vulnerable than ever before because of the broadcast nature of wireless communications. The activities of eavesdropping by wiretappers are hard to be discovered and convicted while information transmission between transceivers can be eavesdropped with not many efforts. Although there are some provided solutions such as RSA and DES but most of them are used at the higher layers such as application or network layers. In addition to it, they are also limited in error-free condition of the link between the transmitter and receiver and the ability of eavesdroppers are assumed in the low computing power level and lacking of efficient algorithms [13]. In the given situation, the physical layer secrecy (PLS) is suggested to accomplish the secure transmission to improve the security level of wireless networks by using the dynamic characteristics of the wireless channels [14–18]. The secrecy ability of NOMA network can be increased by applying this approach. But the involvement of successive interference cancellation (SIC) in NOMA technique can differentiate it from conventional OMA technique. In the recent time, the physical layer secrecy (PLS) of NOMA relaying networks [19–23] attracted a lot of works. For example, the [19] investigated the PLS of a downlink NOMA system with the assuming that the required users quality of service (QoS) to deploy NOMA and all channels undergo Nakagami-*m* fading. From the outcome, it's can be seen that, the secrecy performance of the overall communication process can be improved when the difference in the level of priority between legitimate users is low. The [20] analyzed the secrecy performance of a two-user downlink NOMA system. The researcher included two single-input single-output and multiple-input single-output systems which is different in transmit antenna selection (TAS). The secrecy outage probability (SOP) for different TAS schemes is also expressed in precise and estimated closed form. The outcome is that the SOP for the far user with fixed power allocation scheme drop when the transmit power increase, as the transmit power beyond the threshold, and, after that, it touch the floor with the rising of the interference from the near user. In [21], the authors studied the PLS of large-scale NOMA networks through the SOP. In this article, the locations of NOMA users and eavesdroppers were mapped by using stochastic geometry approaches. And the authors in [22] produced the artificial noise (AN) at the base station to increase the security of a beamforming-aided multiple-antenna system. They suggested The secrecy beamforming scheme for multiple-input single-output non-orthogonal multiple access (MISO-NOMA) system, in which, confidential information of two NOMA assisted legal users was protected by using AN, so the system secrecy performance is enhanced. In [23], the PLS for cooperative NOMA systems including amplify-and-forward (AF) and decode-and-forward (DF) protocols is considered. The conclusion showed that AF and DF schemes reach approximately similar secrecy performance and this secrecy performance is separated from the channel conditions between the relay and the poor user.

Different from the works above, our work focusses on the PLS of downlink NOMA cooperative relay communication system in combination with AN to increase the PLS performance. To be specific, our major subject is the PLS performance of the NOMA system, in that system, the base station (BS) simultaneously delivers information to user pairs based on power-domain, then, the information will be forwarded from the better user (user with better channel condition) to the worse user (users with poor channel conditions), assuming that only the worse users are eavesdropped. AN is applied in the BS to blur the eavesdropper to improve the performance of PLS. Our article contributes the ideas below:

1. Suggesting AN with cooperative transmission scheme (ANCOTRAS).

2. Deriving the lower bound and exact closed-form expressions of secrecy outage probability for each user and overall system.

3. Evaluating the PLS performance using tools of secrecy outage probability expressions.

4. Studying the above system behavior in distinct key parameters, including power allocation ratio, average transmit power and the number of user pairs.

5. Comparing between the PLS performance of ANCOTRAS scheme and non-AN scheme to identify the advantages of integrated AN NOMA cooperative system.

The rest of this paper is organized as follows. The system model is presented in Section II. Secrecy performance of the considered system is analyzed in Section III. The numerical results are shown in Section IV. Finally, Section V draws the conclusion of our paper.

2. Network and Channel Models

The Fig. 1 illustrated a A cooperative communication system for downlink NOMA. In which, the information is intended to be transmitted to M mobile user's represented as $D_i(i = 1 \leq m < n \leq M)$, by the source S i.e., base station, with the under the presence of an eavesdropper E. In this system, it is ok to split the M users to multiple pairs, such as $\{D_m, D_n\}, m < n$, to perform NOMA [8], and in the information signal will be exchanged (by forwarding information) between two paired users. This means m^{th} user and the n^{th} user are paired to deploy cooperative NOMA. Using the applying successive interference cancellation (SIC) to cancel the interference and detect the D_m's signal the better user, then, forward the information of the worse user D_n.

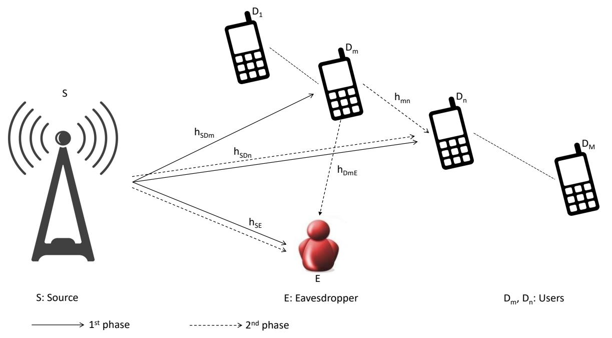

Figure 1. System model for secure cooperative NOMA

The two-phase ANCOTRAS protocol of the given system is suggested as below:

- In phase 1, S transmits information signal $x = \sqrt{a_m}s_m + \sqrt{a_n}s_n$ with power P_S to user pair $\{D_m, D_n\}$ within the time αT $(0 < \alpha < 1, T$ is block time), where s_m and s_n are the messages 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 satisfied the conditions: $0 < a_m < a_n$ and $a_m + a_n = 1$ by following the NOMA scheme.
- Next, phase 2, applying NOMA, at the beginning D_m uses SIC to detects message s_n and then subtracts this component from the received signal by using SIC to obtain its own message s_m. Then, in it, re-encodes s_n and forwards the outcome to D_n within the time of $(1 - \alpha T)$. At this moment, the S collaborates with D_m to broadcast an AN to blur the eavesdropper. At the end, D_n unites two received signals including the direct signal from the S and the relaying signal from D_m, to decode its own message with selection combining (SC) technique.

At the same time, the poor user's message is under the extracting efforts of the eavesdropper, from the links $S - D_n$ and $D_m - D_n$.

Without loss of generality, assuming 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 denoted 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. Phase 1

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

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

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

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

$$\gamma_{SD_n} = \frac{a_n\bar{\gamma}|h_{SD_n}|^2}{a_m\bar{\gamma}|h_{SD_n}|^2 + d_{SD_n}^{\theta}} = \frac{b_2Y_1}{b_1Y_1 + 1}, \tag{3}$$

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

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

$$\gamma_{SD_m}^{s_n} = \frac{a_m\bar{\gamma}|h_{SD_m}|^2}{a_n\bar{\gamma}|h_{SD_m}|^2 + d_{SD_m}^{\theta}} = \frac{b_4X_1}{b_3X_1 + 1}, \tag{4}$$

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

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. Phase 2

In phase 2, D_m uses the power P_{Dm} to forward s_n to D_n and S and, at the same time, uses the power P_S to broadcast an AN to users and eavesdropper. 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 $c_1 = \frac{\bar{\gamma}_{D_m}}{d_{mn}^{\theta}}$, $c_3 = \frac{\bar{\gamma}}{d_{SDn}^{\theta}}$, $\bar{\gamma}_{D_m} = \frac{P_{D_m}}{\sigma^2}$.

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

To identify the advantages of ANCOTRAS protocol, a study on the case of non-AN also is done. In this, the instantaneous SNR at D_n in the phase 2 is as follows:

$$\gamma'_{mn} = \frac{P_{D_m} |h_{mn}|^2}{\sigma^2 d_{mn}^{\theta}} = c_1 X_2, \tag{9}$$

Similarly, the instantaneous SNR at E in the last phase is given by

$$\gamma'_{DmE} = \frac{P_{Dm} |h_{DmE}|^2}{\sigma^2 d_{DmE}^{\theta}} = c_2 Z_2, \tag{10}$$

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 λ_{SDm}, λ_{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]

$$f_U(x) = \frac{M!}{(M-i)!(i-1)!} \frac{1}{\lambda_{SDi}} \sum_{k=0}^{i-1} C_k^{i-1} (-1)^k e^{\frac{-x(M-i+k+1)}{\lambda_{SDi}}} \tag{11}$$

$$\begin{aligned} F_U(x) &= \frac{M!}{(M-i)!(i-1)!} \sum_{k=0}^{i-1} C_k^{i-1} (-1)^k \\ &\times \frac{1}{M-i+k+1} \left[1 - e^{\frac{-x(M-i+k+1)}{\lambda_{SDi}}} \right]. \end{aligned} \tag{12}$$

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

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

$$f_V(x) = \frac{1}{\lambda} e^{-\frac{x}{\lambda}} \tag{13}$$

$$F_V(x) = 1 - e^{-\frac{x}{\lambda}} \tag{14}$$

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

Adding more calculation, we derive CDFs and PDFs of $\gamma_{SD_m}^{s_n}$, γ_{SD_n}, γ_{SE}, γ_{mn}, $\gamma_{D_m E}$. Drawn from above outcomes, The CDF of γ_{SDn} are calculated as below:

$$\begin{aligned} F_{\gamma_{SDm}^{s_n}}(x) &= Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < x \right) \overset{(a)}{=} F_{X_1}\left(\frac{x}{b_4 - b_3 x} \right) \\ &= \frac{M!}{(M-m)!(m-1)!} \sum_{k=0}^{m-1} C_k^{m-1} (-1)^k \\ &\times \frac{1}{M-m+k+1} \left[1 - e^{\frac{-(M-m+k+1)x}{\lambda_{SDm}}} \right], \end{aligned} \tag{15}$$

$$\begin{aligned} F_{\gamma_{SD_n}}(x) &= Pr\left(\frac{b_2 Y_1}{b_1 Y_1 + 1} < x \right) \overset{(b)}{=} F_{Y_1}\left(\frac{x}{b_2 - b_1 x} \right) \\ &= \frac{M!}{(M-n)!(n-1)!} \sum_{k=0}^{n-1} C_k^{n-1} (-1)^k \\ &\times \frac{1}{M-n+k+1} \left[1 - e^{\frac{-(M-n+k+1)x}{\lambda_{SDn}}} \right]. \end{aligned} \tag{16}$$

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

Equally, the CDF and PDF of γ_{SE} are derived respectively as belows:

$$\begin{aligned} F_{\gamma_{SE}}(x) &= Pr\left(\frac{b_6 Z_1}{b_5 Z_1 + 1} < x \right) \overset{(c)}{=} F_{Z_1}\left(\frac{x}{b_6 - b_5 x} \right) \\ &= 1 - e^{-\frac{x}{\lambda_{SE}(b_6 - b_5 x)}}, \end{aligned} \tag{17}$$

$$f_{\gamma_{SE}}(x) = \frac{b_6}{\lambda_{SE}(b_6 - b_5 x)^2} e^{-\frac{x}{\lambda_{SE}(b_6 - b_5 x)}}. \tag{18}$$

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

$$\begin{aligned} F_{\gamma_{mn}}(x) &= \Pr\left(\frac{c_1 X_2}{c_3 Y_1 + 1} < x\right) \\ &= \int_0^\infty F_{X_2}\left(\frac{x(c_3 y + 1)}{c_1}\right) f_{Y_1}(y)dy \\ &= 1 - \frac{M!}{(M-n)!(n-1)!}\frac{1}{\lambda_{SDn}}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k \\ &\times \int_0^\infty e^{-\frac{x(c_3 y+1)}{c_1\lambda_{mn}} - \frac{y(M-n+k+1)}{\lambda_{SDn}}} dy \\ &= 1 - \frac{M!}{(M-n)!(n-1)!} oversetn-1\sum_{k=0} C_k^{n-1}(-1)^k \\ &\times \frac{c_1\lambda_{mn}}{c_3\lambda_{SDn}x + c_1\lambda_{mn}(M-n+k+1)} e^{-\frac{x}{c_1\lambda_{mn}}}. \quad (19) \end{aligned}$$

Similarly the CDF of the $\gamma_{D_m E}$ is given by

$$\begin{aligned} F_{\gamma_{D_m E}}(x) &= \Pr\left(\frac{c_2 Z_2}{c_4 Z_1 + 1} < x\right) \\ &= \int_0^\infty F_{Z_2}\left(\frac{x(c_4 y + 1)}{c_2}\right) f_{Z_1}(y)dy \\ &= 1 - \frac{1}{\lambda_{SE}}\int_0^\infty e^{-\frac{x(c_4 y+1)}{c_2\lambda_{DmE}} - \frac{y}{\lambda_{SE}}} dy \\ &= 1 - \frac{c_2\lambda_{DmE}}{c_4\lambda_{SE}x + c_2\lambda_{DmE}} e^{-\frac{x}{c_2\lambda_{DmE}}}. \quad (20) \end{aligned}$$

The PDF of the $\gamma_{D_m E}$ is expreesed as follows:

$$\begin{aligned} f_{\gamma_{D_m E}}(x) &= \left(\frac{c_2 c_4 \lambda_{DmE}\lambda_{SE}}{(c_4\lambda_{SE}x + c_2\lambda_{DmE})^2} + \frac{1}{(c_4\lambda_{SE}x + c_2\lambda_{DmE})}\right) \\ &\times e^{-\frac{x}{c_2\lambda_{DmE}}}. \quad (21) \end{aligned}$$

3. Analyzing Secrecy Performance

This part analyzed secrecy performance is analyzed in term of secrecy outage probability (SOP). SOP is an crucial performance metric which is applied to describe the secrecy performance of a wireless communication system. In this paper, the secrecy performance is investigated in terms of SOP at S and at D_m with the assumption that E wants to take out the message of D_n.

3.1. Preliminaries

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

$$C_M = B\log(1 + \gamma_M), \quad (22)$$

$$C_N = B\log(1 + \gamma_N), \quad (23)$$

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

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

$$\begin{aligned} C_{S_1} &= \left[C_{\gamma^{s_n}_{SD_m}} - C_{\gamma_{SE}}\right]^+ \\ &= \begin{cases} \alpha\log_2\left(\frac{1+\gamma^{s_n}_{SD_m}}{1+\gamma_{SE}}\right), & \gamma^{s_n}_{SD_m} > \gamma_{SE} \\ 0, & \gamma^{s_n}_{SD_m} \le \gamma_{SE} \end{cases}, \quad (24) \\ C_{S_2} &= \left[C_{\gamma_{SD_n}} - C_{\gamma_{SE}}\right]^+ \\ &= \begin{cases} \alpha\log_2\left(\frac{1+\gamma_{SD_n}}{1+\gamma_{SE}}\right), & \gamma_{SD_n} > \gamma_{SE} \\ 0, & \gamma_{SD_n} \le \gamma_{SE} \end{cases}, \quad (25) \\ C_{S_3} &= \left[C_{\gamma_{mn}} - C_{\gamma_{D_m E}}\right]^+ \\ &= \begin{cases} (1-\alpha)\log_2\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_m E}}\right), & \gamma_{mn} > \gamma_{D_m E} \\ 0, & \gamma_{mn} \le \gamma_{D_m E} \end{cases} (26) \\ C_{S_4} &= \left[C_{\gamma'_{mn}} - C_{\gamma'_{D_m E}}\right]^+ \\ &= \begin{cases} (1-\alpha)\log_2\left(\frac{1+\gamma'_{mn}}{1+\gamma'_{D_m E}}\right), & \gamma'_{mn} > \gamma'_{D_m E} \\ 0, & \gamma'_{mn} \le \gamma'_{D_m E} \end{cases} (27) \end{aligned}$$

respectively. Here, for simplicity we assume $B = 1Hz$.

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 tries to hear the message of D_n at S and at D_m. In the next subsection, we present the calculation of the SOPs at S and at D_m.

3.2. Secrecy outgage probability at S

The SOP at S of $S - D_n$ link (SOP_1) can be calculated as follows:

$$\begin{aligned} SOP_1 &= \Pr(C_{S_1} < R_S) = Pr\left(\frac{1+\gamma_{SD_n}}{1+\gamma_{SE}} < 2^{R_S/\alpha}\right) \\ &= 1 - Pr\left(\gamma_{SE} < \frac{1+\gamma_{SD_n} - 2^{R_S/\alpha}}{2^{R_S/\alpha}}\right). \quad (28) \end{aligned}$$

Because the equation (28) is intractable to obtain the closed-form expression, only the lower bound of SOP_1 is obtained here.

From the equation (3), $\gamma_{SD_n} < \frac{a_n}{a_m}$ can be seen, so the lower bound of SOP_1 should be as follows:

$$\begin{aligned} SOP_1 > SOP_{1_{lower}} &= 1 - CDF_{\gamma_{SE}}\left(\frac{1+\frac{a_n}{a_m}}{2^{R_S/\alpha}} - 1\right) \\ &= e^{-\frac{\beta}{\lambda_{SE}(b_6 - b_5\beta)}}, \quad (29) \end{aligned}$$

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 $SOP_{1_{lower}}$:

$$SOP_2 > SOP_{2_{lower}} = e^{-\frac{\beta}{\lambda_{SE}(b_6 - b_5\beta)}}. \tag{30}$$

3.3. Secrecy outgage probability at D_m

In this situation, the secrecy outage event happens when s_n canâĂŹt be noticed by D_m or D_m can detect s_n but the secrecy capacity is under the secrecy threshold. As a result, the SOP at the D_m can be calculated as below:

- SOP at D_m with AN.

$$\begin{aligned} SOP_3 &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_3} < R_S) \\ &= \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right) \\ &+ \left[1 - \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right)\right] \\ &\times \Pr\left(\frac{1 + \gamma_{mn}}{1 + \gamma_{D_m E}} < 2^{\frac{R_S}{1-\alpha}}\right). \end{aligned} \tag{31}$$

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

$$\begin{aligned} SOP_3 &= \Phi_1 + (1 - \Phi_1)(1 - \frac{M!}{(M-n)!(n-1)!} \\ &\times \sum_{k=0}^{n-1} C_k^{n-1} (-1)^k (\Phi_2 + \Phi_3)), \end{aligned} \tag{32}$$

where

$$\Phi_1 = \begin{cases} \frac{M!}{(M-m)!(m-1)!} \sum\limits_{k=0}^{m-1} (-1)^k C_k^{m-1} \frac{1}{M-m+k+1} \\ \times\left[1 - e^{-\frac{\gamma_t (M-m+k+1)}{(b_4 - b_3\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m}, \\ 1, & \gamma_t > \frac{a_n}{a_m}, \end{cases}$$

$$\begin{aligned} \Phi_2 &= c_1 c_2 c_4 \lambda_{DmE} \lambda_{SE} \lambda_{mn} e^{-\frac{2^{\frac{R_S}{(1-\alpha)}} - 1}{c_1 \lambda_{mn}}} \\ &\times \left[\frac{c e^{\frac{d\mu}{c}} \Gamma(0, \frac{d\mu}{c})}{(ad - bc)^2} - \frac{c e^{\frac{b\mu}{a}} \Gamma(0, \frac{b\mu}{a})}{(ad - bc)^2} + \frac{\mu e^{\frac{b\mu}{a}} \Gamma(-1, \frac{b\mu}{a})}{a(ad - bc)^2}\right], \end{aligned}$$

$$\begin{aligned} \Phi_3 &= c_1 \lambda_{mn} e^{-\frac{2^{R_S} - 1}{c_1 \lambda_{mn}}} \left[\frac{1}{ad - bc} e^{\frac{b}{a}\mu} \Gamma(0, \frac{b}{a}\mu)\right. \\ &- \left.\frac{1}{ad - bc} e^{\frac{d}{c}\mu} \Gamma(0, \frac{d}{c}\mu)\right]. \end{aligned}$$

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

Proof. See Appendix A. □

- SOP at D_m without AN.

$$\begin{aligned} SOP_4 &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_4} < R_S) \\ &= \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right) \\ &+ \left[1 - \Pr\left(\frac{b_4 X_1}{b_3 X_1 + 1} < \gamma_t\right)\right] \\ &\times \Pr\left(\frac{1 + c_1 X_2}{1 + c_2 Z_2} < 2^{\frac{R_S}{1-\alpha}}\right). \end{aligned} \tag{33}$$

Proposition 2. Under Rayleigh fading, the SOP of the link $D_m - D_n$ without AN is given by

$$SOP_4 = \Phi_1 + (1 - \Phi_1)\Phi_4, \tag{34}$$

where

$$\Phi_4 = 1 - \frac{c_1 \lambda_{mn}}{2^{R_S/(1-\alpha)} c_2 \lambda_{DmE} + c_1 \lambda_{mn}} e^{-\frac{2^{R_S/(1-\alpha)} - 1}{c_1 \lambda_{mn}}}.$$

Proof. See Appendix B. □

3.4. Secrecy outgage probability of overall system

As a result of D_n applying selection combining scheme, the instantaneous secrecy can be calculated as belows:

$$C_{S_5} = \begin{cases} C_{S_1}, & \gamma_{SD_m}^{s_n} < \gamma_t, \\ \max\{C_{S_1}, \min\{C_{S_2}, C_{S_3}\}\}, & \gamma_{SD_m}^{s_n} > \gamma_t, \end{cases} \tag{35}$$

The SOP of overall system is given by

$$\begin{aligned} SOP_5 &= \Pr(C_{S_5} < R_S) \\ &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) SOP_1 \\ &+ \Pr(\gamma_{SD_m}^{s_n} > \gamma_t \\ &, \max\{C_{S_1}, \min\{C_{S_2}, C_{S_3}\}\} < R_S). \end{aligned} \tag{36}$$

Proposition 3. Under Rayleigh fading, the SOP of overall system with AN is given by

$$\begin{aligned} SOP_5 &= F_{\gamma_{SDm}^{s_n}}(\gamma_t).SOP_1 + SOP_1.SOP_2.SOP_3 \\ &\times \left[1 - F_{\gamma_{SDm}^{s_n}}(\gamma_t)\right] > F_{\gamma_{SDm}^{s_n}}(\gamma_t).SOP_{1lower} \\ &+ SOP_{1lower}.SOP_{2lower}.SOP_{3lower} \\ &\times \left[1 - F_{\gamma_{SDm}^{s_n}}(\gamma_t)\right] \end{aligned} \tag{37}$$

Proof. See Appendix C. □

Similarly, SOP of the overall system without AN is given by

$$\begin{aligned} SOP_6 &= F_{\gamma_{SDm}^{s_n}}(\gamma_t).SOP_1 + SOP_1.SOP_2.SOP_4 \\ &\times \left[1 - F_{\gamma_{SDm}^{s_n}}(\gamma_t)\right] > F_{\gamma_{SDm}^{s_n}}(\gamma_t).SOP_{1lower} \\ &+ SOP_{1lower}.SOP_{2lower}.SOP_{4lower} \\ &\times \left[1 - F_{\gamma_{SDm}^{s_n}}(\gamma_t)\right] \end{aligned} \tag{38}$$

4. Nummerical results and disscussion

In this section, the PLS performance of ANCOTRAS protocol for this considered cooperative NOMA system is analyzed by numerical results. And our analytical results is also verified using Monte-Carlo simulation results.

4.1. Secrecy outage probability at S

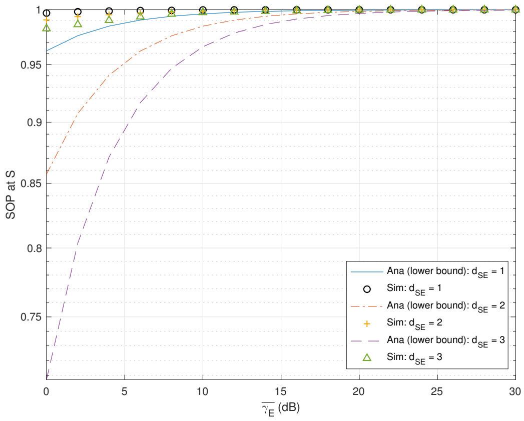

Figure 2. The SOP at the Base Station with a distance change from S to E; $d_{SDm} = 1, d_{SDn} = 2, \alpha = 0.3$

The outcomes of SOP of the system at S is illustrated in Figs. 2 and Figs. 3. These figures displayed that the average transmits SNR from S to user D_n ($\bar{\gamma}$) then the SOP at the S reduces when the distance from S to the eavesdropper $E(d_{SE})$ is increased. That means there are increase in the PLS capability of this model. Besides, in these two results, when we increase the average transmit SNR from S to the E ($\bar{\gamma}_E$), the SOP at S of the system also increases.

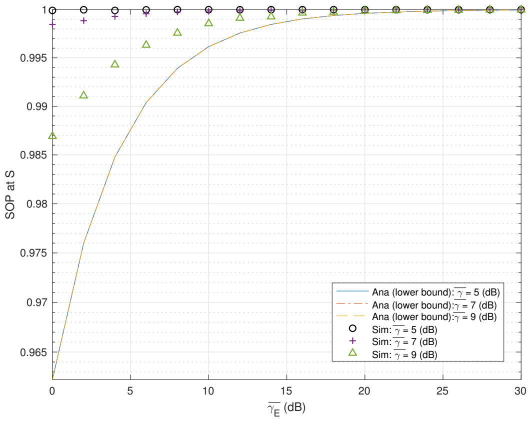

Figure 3. The SOP at the Base Station with a distance change of $\bar{\gamma}$; $d_{SDm} = 1, d_{SDn} = 2, d_{SE} = 1, \alpha = 0.3, R_s = 0.5$

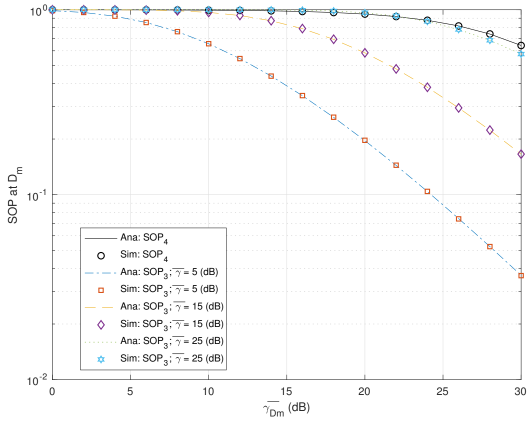

Figure 4. The SOP at the D_m with the change of $\bar{\gamma}; d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

4.2. Secrecy outage probability at D_m

Figs. 4 and Figs. 5 depict the results of the SOP of the system at D_m. In these two results, the secrecy performance is analyzed in consistent with the changes of the parameters belows: $\bar{\gamma}, \gamma_{\bar{D}m}$ and $\bar{\gamma_E}$. In these figures, We can see that the SOP at D_m reduces when $\gamma_{\bar{D}m}$ (the average transmit SNR from D_m to D_n) increase. From Figs. 4, we can see that the secrecy performance can be improved if we use AN from S to D_n ($\bar{\gamma}$ at second phase). Similarily, in Figs. 5 it is clear that the average transmit SNR of AN is increased from S to E ($\bar{\gamma}_E$), the secrecy performance is improved. However, introducing AN when the average transmit SNR is low ($\bar{\gamma}_E = 10$ dB), the security performance of the system will not be improved compared to the case of not using AN. To be more specific, in this case, we should use $\bar{\gamma}_E$ greater than or equal to 20 dB. We did a survey of the secrecy performance along with the average transmit SNR parameters: from D_m to D_n ($\gamma_{\bar{D}m}$) and to E ($\gamma_{\bar{D}mE}$). The survey results in Figs. 6 showed that the SOP at D_m of the system reduce along with the increase in $\gamma_{\bar{D}m}$ and reduce in $\gamma_{\bar{D}mE}$. This result settles once again that using AN the will increases the PLS performance of the system. Seeing the changes in the figures of users (M), which using AN, in figs. 7, it is showed that the SOP at the D_m of system decreases when M increases. Using he formula of SOP_3, the conclusion is that, C_{S_3} increases when M increase so SOP_3 decreases. Particularly, the simulation results in figs. 7 showed that with 3 sequential M values: 4,6 and 8, SOP_4 do not experience major change. So it can be seen that when the system according to the changes of M and $\gamma_{\bar{D}m}$ is

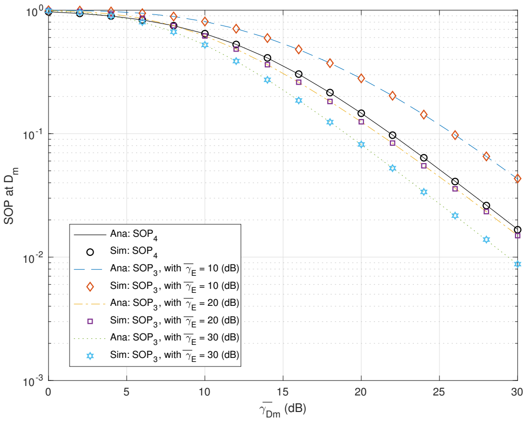

Figure 5. The SOP at the D_m with the change of $\bar{\gamma_E}; d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

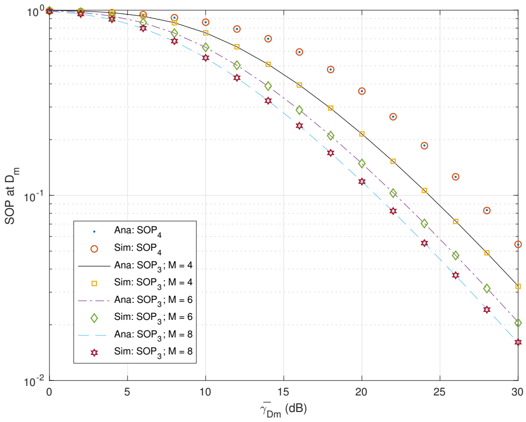

Figure 7. The SOP at the D_m with the change of M; $d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

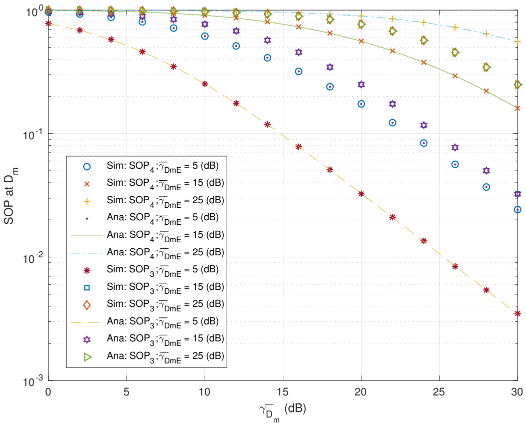

Figure 6. The SOP at the D_m with the change of $\gamma_{\bar{D}mE}; d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

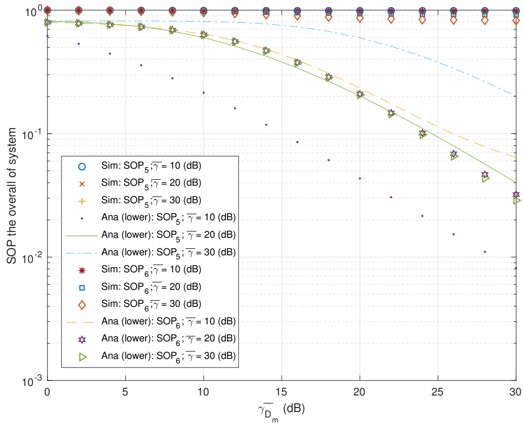

Figure 8. The SOP of overall with the change of $\gamma_{\bar{D}m}$; $d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

examined, in without AN case, then M does not have any affection to the PLS performance of the system.

4.3. Secrecy outage probability overall system

Fig. 8 illustrates the SOP of the overall system. The result displays that the higher the average transmit SNR from D_m to D_n ($\gamma_{\bar{D}m}$) is the lower SOP of the overall system is observed. It means that secrecy performance will rise. On another side, it can be seen that when the average transmit SNR from S to D_n ($\bar{\gamma}$) rise, then SOP of the overall system with reduce, but, if $\bar{\gamma}$ is big enough (particularly when $\bar{\gamma} \geq 20$ (dB) in this figure) then SOP of the overall system with AN will rise. In phase 2, $\bar{\gamma}$ is the average transmit SNR of the AN, so if $\bar{\gamma}$ is greater than a appropriate value (particularly when $\bar{\gamma} \geq 10$ (dB) in this figure) the security performance of the system with AN will reduce.

We can see the SOP of the overall system with AN reduced when increasing the average transmit SNR from S to E ($\bar{\gamma_E}$) in Fig. 9. In this figure, the increase of $\bar{\gamma_E}$ go hand in hand with the decrease of SOP. However, $\bar{\gamma_E}$ have to be at suitable (particularly when $\bar{\gamma_E} \geq 10$ (dB) in this figure), the security performance of the system with AN better than that the security performance of the system without AN.

5. Conclusion

In this work, we inspected the secrecy performance of a downlink cooperative NOMA network with artificial noise. Particularly, in this paper, the method of broadcasting artificial noise from the base station is used to interfere the eavesdroppers and we also improved the information security. Besides, new analytical expressions were carried out in terms of the secrecy outage probability to regulate the system secrecy performance. In the meantime,we used the numerical results to confirm the examines. Basing on the analytical and simulation results, it can be settled that the security level of the network model which is suggested in this paper relies on the distance: from 1) base station to the better user; worse users; eavesdropping device and from 2) better users to worse users, eavesdropping devices. Using artificial noise can improve the security performance of the system. As long as appropriate values are used, the securecy performance of the system with AN is better than that without AN. APPENDIX A:

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

$$\begin{aligned}
SOP_3 &= \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right) + \left(1 - \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right)\right)\\
&\times \Pr\left(\frac{1+\gamma_{mn}}{1+\gamma_{D_mE}} < 2^{R_S/(1-\alpha)}\right)\\
&= \Phi_1 + (1-\Phi_1)\\
&\times \int_0^\infty F_{U_1}(2^{R_S/(1-\alpha)}(1+y)-1) f_{U_2}(y)dy\\
&= \Phi_1 + (1-\Phi_1)\Bigg[1 - \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k\\
&\times \int_0^\infty (c_1\lambda_{mn})\left(e^{-\frac{(2^{R_S/(1-\alpha)}(1+y)-1)}{c_1\lambda_{mn}}}\right)\\
&/ \quad (c_3\lambda_{SDn}(2^{R_S/(1-\alpha)}(1+y)-1)\\
&+ \quad c_1\lambda_{mn}(M-n+k+1))\\
&\times \left(\frac{c_2c_4\lambda_{DmE}\lambda_{SE}}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})^2} + \frac{1}{(c_4\lambda_{SE}y+c_2\lambda_{DmE})}\right)\\
&\times e^{-\frac{y}{c_2\lambda_{DmE}}}dy\Bigg]\\
&= \Phi_1 + (1-\Phi_1)(1 - \frac{M!}{(M-n)!(n-1)!}\\
&\times \sum_{k=0}^{n-1} C_k^{n-1}(-1)^k(\Phi_2+\Phi_3)),
\end{aligned} \tag{39}$$

where γ_t is the threshold to detect s_n and Φ_1, Φ_2, Φ_3 are calculated as follows

$$\begin{aligned}
\Phi_1 &= F_{X_1}\left(\frac{\gamma_t}{b_4 - b_3\gamma_t}\right)\\
&= \begin{cases} \frac{M!}{(M-m)!(m-1)!}\sum\limits_{k=0}^{m-1}(-1)^k C_k^{m-1}\frac{1}{M-m+k+1} & \\ \qquad \times\left[1 - e^{-\frac{\gamma_t(M-m+k+1)}{(b_4-b_3\gamma_t)\lambda_{SDm}}}\right], & \gamma_t < \frac{a_n}{a_m}\\ \qquad 1, & \gamma_t > \frac{a_n}{a_m} \end{cases}
\end{aligned}$$

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

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

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 (39), 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.

$$\begin{aligned}
SOP_4 &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t) + \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_4} < R_S)\\
&= \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right) + \left[1 - \Pr\left(\frac{b_4X_1}{b_3X_1+1} < \gamma_t\right)\right]\\
&\times \Pr\left(\frac{1+c_1X_2}{1+c_2Z_2} < 2^{\frac{R_S}{1-\alpha}}\right)\\
&= \Phi_1 + (1-\Phi_1)\Phi_4,
\end{aligned} \tag{40}$$

where

$$\begin{aligned}\Phi_4 &= \Pr\left(X_2 < \frac{2^{R_S/(1-\alpha)}(1+c_2 Z_2)-1}{c_1}\right)\\ &= \int_0^\infty F_{X_2}\left(\frac{2^{R_S/(1-\alpha)}(1+c_2 z)-1}{c_1}\right) f_{Z_2}(z)dz\\ &= 1-\frac{1}{\lambda_{DmE}}\int_0^\infty e^{-\frac{2^{R_S/(1-\alpha)}(1+c_2 z)-1}{c_1\lambda_{mn}}-\frac{z}{\lambda_{DmE}}}dz\\ &= 1-\frac{c_1\lambda_{mn}}{2^{R_S/(1-\alpha)}c_2\lambda_{DmE}+c_1\lambda_{mn}}e^{-\frac{2^{R_S/(1-\alpha)}-1}{c_1\lambda_{mn}}}.\end{aligned}$$

Substituting Φ_1, Φ_4 into (40), we obtain the closed-form expression of SOP for the link $D_m - D_n$ in the case of without using AN. This concludes the proof.

APPENDIX C:

$$\begin{aligned}SOP_5 &= \Pr(\gamma_{SD_m}^{s_n} < \gamma_t)SOP_1\\ &+ \Pr(\gamma_{SD_m}^{s_n} > \gamma_t, \max\{C_{S_1}, \min\{C_{S_2}, C_{S_3}\}\} < R_S)\\ &= \underbrace{F_{\gamma_{SD_m}^{s_n}}(\gamma_t)SOP_1}_{I_1}\\ &+ \underbrace{\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_1} < R_S, \min\{C_{S_2}, C_{S_3}\} < R_S)}_{I_2}.\end{aligned}$$

$$\begin{aligned}I_1 &> F_{\gamma_{SD_m}^{s_n}}(\gamma_t).SOP_{1lower} = \frac{M!}{(M-n)!(n-1)!}\sum_{k=0}^{n-1} C_k^{n-1}(-1)^k\\ &\times \frac{1}{M-n+k+1}\left[1-e^{\frac{-(M-n+k+1)\gamma_t}{\lambda_{SDn}}}\right]e^{-\frac{\beta}{\lambda_{SE}(b_6-b_5\beta)}}.\end{aligned} \quad (41)$$

$$\begin{aligned}I_2 &= SOP_1.\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, \min\{C_{S_2}, C_{S_3}\} < R_S)\\ &= SOP_1.\left[1-\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, \min\{C_{S_2}, C_{S_3}\} > R_S)\right]\\ &= SOP_1.\left[1-\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_2} > R_S, C_{S_3} > R_S)\right]\\ &= SOP_1.\left[1-\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_2} > R_S).SOP_3\right]\\ &= SOP_1.\{1-\left[1-\Pr(\gamma_{SD_m}^{s_n} > \gamma_t, C_{S_2} < R_S)\right].SOP_3\}\end{aligned} \quad (42)$$

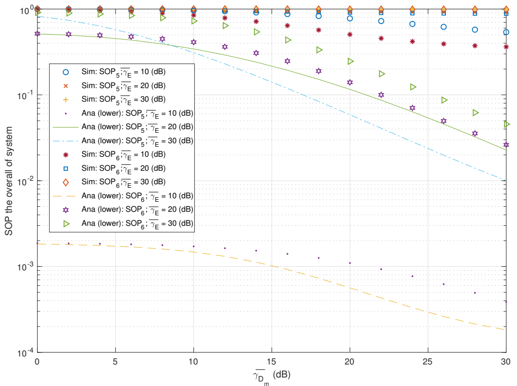

Figure 9. The SOP of overall with the change of $\bar{\gamma_E}$; $d_{SDm} = 1, d_{SDn} = 2, d_{mn} = 1, d_{DmE} = 1, \alpha = 0.3$

References

[1] Ding, Z., Yang, Z., Fan, P. and Poor, H.V.(2014) *On the performance of non-orthogonal multiple access in 5g systems with randomly deployed user*, IEEE signal. Process. Lett. 21(12): 1501-1505.

[2] Dai, L., Wang, B., Yuan, Y., Han, S., Lin I, C. and Wang, Z (2015) *Nonorthogonal multiple access for 5g: Solutions, challenges, opportunities, and future research trends*, IEEE Communications Magazine 53(9): 74-81.

[3] Shimojo, T., Umesh, A., Fujishima, D. and Minokuchi, A. (2018) *Performance analysis of energy-harvesting-aware multi-relay networks in Nakagami-m fading*, EURASIP Journal on Wireless Communications and Networking, 2018:63.

[4] Islam, S.M.R., Avazov, N., Dobre, O.A. and sup Kwak, K. (2017) *Power- domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges*, IEEE Communications Surveys and Tutorials 19(2): 721-741.

[5] Lee, S., Duong, T.Q., Da Costa, D.B., Ha, D.B. and Nguyen, S.Q. (2018) *Un- derlay cognitive radio networks with cooperative non-orthogonal multiple access*, IET Communications 12(3):359-366.

[6] Suraweera, H.A., Karagiannidis, G.K. and Smith, P.J. (2009) *Performance analysis of the dual-hop asymmetric fading channel*, IEEE Trans. Wireless Com- mun. 8(6): 2783-2788.

[7] Kim, K.J., Duong, T.Q. and Poor, H.V. (2013) *erformance analysis of cyclic prefixed single-carrier cognitive amplify-and-forward relay systems*,IEEE Trans- actions on Wireless Communications 12(1): 195-205.

[8] Ding, Z., Peng, M. and Poor, H.V. (2015) *Cooperative non-orthogonal multiple access in 5G systems*,IEEE Communications Letters 19(8): 1462-1465.

[9] Kim, J.B., Song, M.S. and Lee, I.H. (2016) *Achievable rate of best relay se- lection for non-orthogonal multiple access-based cooperative relaying systems*,In International Conference on Information and Communication Technology Convergence (ICTC) (Jeju, South Korea: IEEE): 960-962.

[10] Liu, Y., Ding, Z., Elkashlan, M. and Poor, H.V. (2016) *Cooperative nonorthogonal multiple access with simultaneous wireless information and power transfer*,IEEE Journal on Selected Areas in Communications 34(4): 936-953.

[11] Ha, D.B. and Nguyen, Q.S. (2017) *Outage performance of energy harvesting DF relaying NOMA networks*, Mobile Networks and Applications.

[12] Tran,D.D.,Tran,H.V.,Ha,D.B.andKaddoum,G. (15-18/4/2018,Barcelona, Spain) *Cooperation in NOMA networks under limited user-to-user communica- tions: Solution and analysis*, In IEEE Wireless Communications and Networking Conference (WCNC).

[13] Ha, D.B., Duong, T.Q., Tran, D.D., Zepernick, H.J. and Vu, T.T. (Hanoi, Vietnam, Oct. 15-17, 2014) *Physical layer secrecy performance over Rayleigh/Rician fading channels*, In The 2014 International Conference on Advanced Technologies for Communications (ATC'14): 113-118.

[14] Wyner, A. (1975) *The wire-tap channel*, Bell System Technical Journal 54(8): 1355-1387.

[15] Bloch, M., Barros, J., Rodrigues, M.R. and McLaughlin, S.W. (2008) *Wire- less information-theoretic security*, IEEE Trans. Inf. Tech. 54(6): 2515-2534.

[16] Ng, D.W.K. and Schober, R. (2013) *Resource allocation for secure communica- tion in systems with wireless information and power transfer*, In IEEE Globecom Workshops (Atlanta, USA): 1251-1257.

[17] Ha, D.B., Van, P.T. and Vu, T.T. (San Francisco, USA, 22-24 October, 2014) *Physical layer secrecy performance analysis over Rayleigh/Nakagami fad- ing channels*, In The World Congress on Engineering and Computer Science 2014 (WCECS2014).

[18] Ha, D.B., Vu, T.T., Duy, T.T. and Bao, V.N.Q. (2015) *Secure cognitive reac- tive decode-and-forward relay networks: With and without eavesdropper*, Wireless Personal Communications (WPC) 85(4): 2619-2641.

[19] Tran, D.D. and Ha, D.B. (2018) *Secrecy performance analysis of QoS-based non-orthogonal multiple access networks over nakagami-m fading*, In The Interna- tional Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom) (HCMC, Vietnam).

[20] Lei, H., Zhang, J., Park, K.H., Xu, P., Ansari, I.S. and Pan, G. (2017) *On secure noma systems with transmit antenna selection schemes*, IEEE Access 5: 17450-17464.

[21] Liu, Y., Qin, Z., Elkashlan, M., Gao, Y. and Hanzo, L. (2017) *Enhancing the physical layer security of nonorthogonal multiple access in large-scale networks*, IEEE Transactions on Wireless Communications 16(3): 1656-1672.

[22] Lv, L., Ding, Z., Ni, Q. and Chen, J. (2017) *Secure MISO-NOMA transmission with artificial noise*, IEEE Transactions on Vehicular Technology 67(7): 6700-6705.

[23] Chen, J., Yang, L. and Alouini, M.S. (2018) *Physical layer security for cooper- ative NOMA systems*, IEEE Transactions on Vehicular Technology 67(5): 4645-4649.

[24] Men, J. and Ge, J. (2015) *Performance analysic of non-orthogonal multiple access in downlink cooperative network*, IET Communications 9(18): 2267-2273.