Performance of Cooperative NOMA Systems under Passive Eavesdropping

Basem M. ElHalawany*†§, Rukhsana Ruby*§, Taneli Riihonen‡, Kaishun Wu*
*College of Computer Science, Shenzhen University, China
†Benha University, Egypt
‡Tampere University of Technology, Finland
§Equal Contribution

***Abstract*—A key feature of the non-orthogonal multiple access (NOMA) technique is that users with better channel conditions have prior information about the messages of other users. The technique to exploit the prior knowledge of strong users in order to improve the performance of weak users is known as cooperative NOMA. In this paper, we study the physical layer security in such a cooperative NOMA system. In order to reduce the complexity, the considered system in this paper has two users. Through the cooperative NOMA concept, the performance of the weak user is enhanced by the strong user. Given that there is an eavesdropper in the system that can hear all transmissions, we study the secrecy rate of the strong and the weak users. More specifically, we make an attempt to derive the secrecy outage probability (SOP) of both the users. Due to the intractable nature of the exact analysis for the weak user, we provide the closed form expression for the SOP of this user in high SNR regime while keeping the exactness for the strong user. Through numerical simulations, we verify the correctness of our analytical derivations under different scenarios. Besides, we provide the insights of achieving optimal secrecy performance in such a system.**

***Index Terms*—Cooperative NOMA Systems; Physical Layer Security; Secrecy Outage Probability under Passive Eavesdropping**

I. Introduction

Non-orthogonal multiple access (NOMA) [1] is considered as a breakthrough technology of 5G systems because of its superior spectral efficiency. Generally, this technique utilizes the power domain to achieve multiple-access strategies, which is unlike the conventional orthogonal multiple access structures, such as frequency division multiple access. Via having less power level, users with better channel condition can decode their own information by applying the successive interference cancellation (SIC) technique [2]. As a result, these users know the messages intended to other weaker users, and hence they can improve the performance of the weak users by re-sending the decoded information via adopting short-range communication technologies, such as Bluetooth and Ultra Wide Band (UWB). Then, weak users can use the maximum ratio combining technique to combine all information sent to them. Essentially, in NOMA systems, a strong user can act as the relay for weak users, and hence additional relay nodes are not required to be deployed in order to obtain the benefit of cooperation concept in wireless communications.

Based on such cooperative NOMA concept, there are some works in the existing literature. For example, in [3], the outage probability and diversity order are analytically studied, in which a set of strong users help weak users via re-transmitting their information. For another such a system [4], in which near NOMA users that are close to the source act as energy harvesting relays to help far NOMA users, outage probability and system throughput are studied. Their results confirm that the opportunistic use of node locations for user selection can achieve lower outage probability and deliver superior throughput in comparison to the random selection scheme. Cooperative NOMA concept in a multi-cast system [5] is studied as well, in which the multi-cast subscribers are served as secondary users underlying a primary strong user. The performance is studied analytically in terms of primary outage probability and secondary ergodic capacity. More recently, in [6], the authors have proposed a dynamic NOMA strong user selection scheme for each weak user that can improve its reception reliability. Similar to the prior works, in this work, outage probability of the users is considered as the performance metric.

On the other hand, while employing real relays with decode-and-forward (DF) or amplify-and-forward (AF) mode and then equipping the NOMA concept, there are some works in the existing literature to study the benefits of cooperation concept. For example, a hybrid DF and AF relaying strategy was studied in [7] for such a system with multiple relays. In [8], the outage performance of a DF relaying NOMA system, which is equipped with a two-stage relay selection (TSRS) method, was analyzed. The authors in [9] studied a cooperative NOMA scenario with the help of an AF relay, and then derived an expression for the approximate outage probability. In [10], the authors have proposed a full-duplex (FD) cooperative NOMA system with dual users, where a dedicated FD relay assists the information transmission of a user with weak channel condition.

Wireless communication networks are more vulnerable to security threats due to the broadcast nature of the wireless medium. Typically, in prior works, security was ensured for wireless networks in the higher layer of the OSI model. However, due to the distributed nature of today's networks and the hassle associated with the management of different secret keys, nowadays, physical layer security techniques [11] have received tremendous attention. In this paper, on the presence of a passive eavesdropper, we study the performance of secrecy rate in a cooperative NOMA system. Till now, without considering the NOMA technique, the analysis of secrecy performance for different systems with different technologies, such as multiple-input-multiple-output (MIMO) [12], cooperative diversity [13], energy harvesting [14] and cognitive radio [15], has extensively been studied. There are a few works came out recently for NOMA-equipped networks as well. For example, physical layer security for a typical 5G NOMA system was considered in [16], in which two different structures were proposed to improve the secrecy performance for single antenna and multiple-antenna networks via the stochastic geometry concept, respectively. A new design of the NOMA technique under secrecy considerations was proposed in [17], the objective of which is to determine the optimal decoding order, transmission rates and power allocated to each user. A very close work to ours is [18], which is based on the cooperative NOMA concept. However, with the presence of an eavesdropper, the authors in this work implemented the cooperative concept via deploying one real relay either with the AF or DF mode.

In this paper, we have studied the secrecy performance of a cooperative NOMA system without deploying any real relay. The cooperation concept is achieved through the strong user of the system. Due to the decoding facility of the SIC technique, the strong user is able to decode the message of the weak user, and hence it is able to enhance the reception reliability of the weak user through re-transmitting the decoded messages. On the presence of a passive eavesdropper, in such a system with two users, we have studied their performance analytically in terms of secrecy outage probability (SOP). To the best of our knowledge, this is the first work that has studied the performance of a relay-free cooperative NOMA system under a passive eavesdropping scenario. Although we have provided the exact closed form expression of the SOP for the strong user, that for the weak user is provided in high signal-to-noise-ratio (SNR) regime due to the intractable nature of its exact analysis. Extensive numerical simulations have been conducted in order to verify the correctness of the analytical results under different scenarios. Both the analytical derivations and simulation results reveal that the optimal secrecy performance can be achieved in such a system via an appropriate power control.

The rest of the paper is organized as follows. In Section II, we elaborately describe the components and functionalities of the system, and then formulate the problem. The exact analysis of the proposed system is provided in Section III. In Section IV, we evaluate the performance of the proposed analytical model. Finally, Section V concludes the paper.

II. System Model and Problem Formulation

Let us consider a NOMA-equipped cellular system, in which there is a pico base station (BS), two users and an eavesdropper. The BS is located in the center of the cell, and a sample system model is provided in Fig. 1. The strong and weak users are denoted by UE$_n$ and UE$_m$, respectively. The maximal power level of the BS and the strong user are denoted by P_b and P_u, respectively. We assume that all nodes in the network are equipped with a single antenna and all the channels follow the conventional path loss model accompanied with small scale fading. The transmission in this network is accomplished in two phases, the description of each is given in the following.

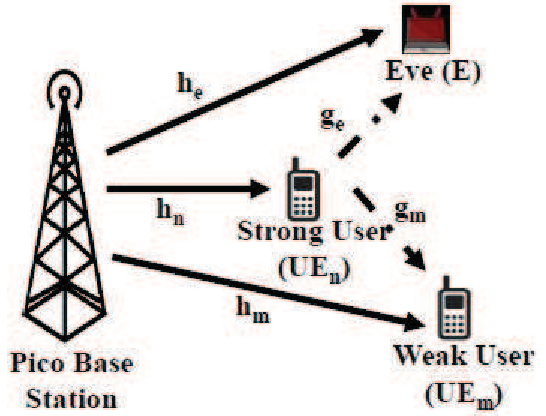


Fig. 1: A sample cooperative NOMA system under a passive eavesdropping scenario.

A. Direct Transmission Phase

In this phase, the BS broadcasts the superimposed mixture, $x_b = \sqrt{a_m}s_m + \sqrt{a_n}s_n$, where s_m and s_n are the unit power signal received by user m and user n, respectively, and a_m and a_n are their power allocation coefficients, respectively. While taking the quality-of-service (QoS) constraints of both the users into account, we assume that $a_m > a_n$ and $a_m + a_n = 1$. As a result, the received signal at user m, user n and the eavesdropper can be given by

$$y_n = \frac{h_n}{d_n^\alpha} x_b \sqrt{P_b} + \omega_n, \tag{1}$$

$$y_m = \frac{h_m}{d_m^\alpha} x_b \sqrt{P_b} + \omega_m, \text{ and} \tag{2}$$

$$y_e = \frac{h_e}{d_e^\alpha} x_b \sqrt{P_b} + \omega_e, \text{ respectively,} \tag{3}$$

where h_n, h_m and h_e are the channel gain associated with the small scale fading from the BS to user n, user m and the eavesdropper, respectively. d_n, d_m and d_e are the distance from the BS to user n, user m and the eavesdropper, respectively. ω_m, ω_n and ω_e are the additive white Gaussian noise with zero mean and variance N_0, and α is the path loss exponent. For the sake of simplicity, we assume that $\rho_b = P_b/N_0$. As a result, we obtain

$$\gamma_{sm}^n = \frac{a_m|h_n|^2}{a_n|h_n|^2 + d_n^\alpha/\rho_b}, \text{ and } \gamma_{sn}^n = \frac{a_n\rho_b|h_n|^2}{d_n^\alpha}, \tag{4}$$

$$\gamma_{sm}^m = \frac{a_m|h_m|^2}{a_n|h_m|^2 + d_m^\alpha/\rho_b}, \tag{5}$$

$$\gamma_{sm}^e = \frac{a_m|h_e|^2}{a_n|h_e|^2 + d_e^\alpha/\rho_b}, \text{ and } \gamma_{sn}^e = \frac{a_n\rho_b|h_e|^2}{d_e^\alpha}. \tag{6}$$

where γ_{sm}^n and γ_{sn}^n are the signal-to-interference-plus-noise-ratio (SINR) of user m and user n decoded by user n, respectively, γ_{sm}^{m} is the SINR of user m decoded by itself, and γ_{sm}^{e} and γ_{sn}^{e} are the SINR of user m and user n decoded by the eavesdropper, respectively.

B. Cooperative Phase

In this phase, the strong user n broadcasts the extracted weak user signal $x_u = s_{nm}$, where s_{nm} is the unit power signal received by user m. Consequently, the received signal at user m and the eavesdropper can be given by

$$y_{nm} = \frac{g_m}{d_{nm}^{\alpha}} x_u \sqrt{P_u} + \omega_{nm}, \text{ and} \tag{7}$$

$$y_{ne} = \frac{g_e}{d_{ne}^{\alpha}} x_u \sqrt{P_u} + \omega_{ne}, \text{ respectively,} \tag{8}$$

where g_m and g_e are the channel gain associated with the small scale fading from user n to user m and the eavesdropper, respectively. d_{nm} and d_{ne} are the distance from user n to user m and the eavesdropper, respectively. ω_{nm} and ω_{ne} are the additive white Gaussian noise with zero mean and variance N_0. Given that $\rho_u = P_u/N_0$, we obtain

$$\gamma_{nm}^{m} = \tfrac{\rho_u |g_m|^2}{d_{nm}^{\alpha}}, \text{ and } \quad \gamma_{nm}^{e} = \frac{\rho_u |g_e|^2}{d_{ne}^{\alpha}}, \tag{9}$$

where γ_{nm}^{m} is the SINR of user m decoded by itself, and γ_{nm}^{e} is the SINR of user m decoded by the eavesdropper. Using the maximum ratio combining technique, the combined SINR of user m decoded by itself (i.e., γ_m^m) and the eavesdropper (i.e., γ_m^e) can be given by

$$\gamma_m^m = \gamma_{sm}^{m} + \min\left(\gamma_{sm}^{n}, \gamma_{nm}^{m}\right), \text{ and} \tag{10}$$

$$\gamma_m^e = \gamma_{sm}^{e} + \min\left(\gamma_{sm}^{n}, \gamma_{nm}^{e}\right). \tag{11}$$

C. Problem Formulation

Using Shannon's capacity formula [19], the secrecy rate of user n can be given by

$$C_n = I_n^n - I_n^e, \text{ where} \tag{12}$$

$$I_n^n = \log_2\left(1 + \gamma_{sn}^{n}\right), \text{ and } I_n^e = \log_2\left(1 + \gamma_{sn}^{e}\right). \tag{13}$$

On the other hand, the secrecy rate of user m can be given by

$$C_m = \tfrac{1}{2}\left(I_m^m - I_m^e\right), \text{ where} \tag{14}$$

$$I_m^m = \log_2\left(1 + \gamma_m^m\right), \text{ and } I_m^e = \log_2\left(1 + \gamma_m^e\right). \tag{15}$$

If R_m^{th} and R_n^{th} are the threshold capacity of user m and user n, respectively, the outage probability of the system can be given by

$$\begin{aligned} \text{SOP} &= \Pr\{C_m < R_m^{th} \text{ OR } C_n < R_n^{th}\} \\ &= 1 - \Pr\{C_m \geq R_m^{th}\} \times \Pr\{C_n \geq R_n^{th}\} \\ &= 1 - P_m \times P_n. \end{aligned} \tag{16}$$

Therefore, the individual SOP of user m and user n can be given by $1 - P_m$ and $1 - P_n$, respectively.

III. Performance Analysis and Implications

In this section, we first derive the closed form expression of the SOP, and then study the analytical derivation in order to develop an optimal secure cooperative system.

A. Derivation of SOP

For the sake of analysis, we assume that $|h_m|^2$, $|h_n|^2$, $|h_e|^2$, $|g_m|^2$ and $|g_e|^2$ all follow the exponential distribution with mean λ. Now, $P_m = \Pr\{C_m \geq R_m^{th}\} = \Pr\{\frac{1+\gamma_m^m}{1+\gamma_m^e} \geq 2^{2R_m^{th}}\}$. If $C_m^{th} = 2^{2R_m^{th}}$, the expression $\frac{1+\gamma_m^m}{1+\gamma_m^e} \geq C_m^{th}$ can be written as

$$\begin{aligned} \min\left(\gamma_{sm}^{n}, \gamma_{nm}^{m}\right) \geq C_m^{th}(1 + \gamma_{sm}^{e}) + \\ C_m^{th} \min\left(\gamma_{sm}^{n}, \gamma_{nm}^{e}\right) - 1 - \gamma_{sm}^{m}. \end{aligned} \tag{17}$$

Because of the "min" function and the interference term of γ_{sm}^{n}, γ_{sm}^{e} and γ_{sm}^{m}, the closed form expression of P_m is not tractable. However, at high SNR regime, we can write $\gamma_{sm}^{n} = \gamma_{sm}^{m} = \gamma_{sm}^{e} = \frac{a_m}{a_n}$. In this case, the expression in (17) can be written as

$$\min\left(\frac{a_m}{a_n}, \gamma_{nm}^{m}\right) \geq \frac{C_m^{th} - 1}{a_n} + C_m^{th} \min\left(\frac{a_m}{a_n}, \gamma_{nm}^{e}\right). \tag{18}$$

Let $B = \frac{C_m^{th} - 1}{a_n}$, the probability of the expression in (18) is equivalent to

$$P_m = P_m^1 + P_m^2 + P_m^3 + P_m^4, \tag{19}$$

where $P_m^1 = \Pr\{\gamma_{nm}^{m} \geq \frac{a_m}{a_n} \text{ AND } \frac{a_m}{a_n} \geq C_m^{th}\gamma_{nm}^{e} + B\}$, $P_m^2 = \Pr\{\gamma_{nm}^{m} \geq \frac{a_m}{a_n} \text{ AND } \frac{a_m}{a_n} \geq C_m^{th}\frac{a_m}{a_n} + B\}$, $P_m^3 = \Pr\{\frac{a_m}{a_n} \geq \gamma_{nm}^{m} \text{ AND } \frac{a_m}{a_n} \geq C_m^{th}\gamma_{nm}^{e} + B\}$, and $P_m^4 = \Pr\{\frac{a_m}{a_n} > \gamma_{nm}^{m} \text{ AND } \gamma_{nm}^{m} \geq C_m^{th}\frac{a_m}{a_n} + B\}$. The values of P_m^2 and P_m^4 are 0 as the expressions associated with these probabilities are impossible to happen in practice. However, the simplified value of P_m^1 can be written as

$$P_m^1 = \Pr\{|g_m|^2 \geq \Delta_{12},\ |g_e|^2 \leq \Delta_{13}\}, \text{ where} \tag{20}$$

$$\Delta_{11} = \tfrac{d_{ne}^{\alpha}}{a_n C_m^{th} \rho_u},\ \Delta_{12} = \tfrac{a_m d_{nm}^{\alpha}}{a_n \rho_u}, \tag{21}$$

$$\text{and } \Delta_{13} = \left(a_m + 1 - C_m^{th}\right)\Delta_{11}. \tag{22}$$

This in turn is equivalent to

$$P_m^1 = \Pr\{|g_m|^2 \geq \Delta_{12}\} \times \Pr\{|g_e|^2 \leq \Delta_{13}\}. \tag{23}$$

After the expansion and then simplification, this can be written as

$$P_m^1 = \begin{cases} \lambda \mathrm{e}^{-\lambda\Delta_{12}}\left(1 - e^{-\lambda\Delta_{13}}\right), & a_m + 1 - C_m^{th} > 0 \\ 0 & , \text{ Otherwise.} \end{cases}$$

On the other hand, the simplified expression of P_m^3 is given by

$$P_m^3 = \Pr\{|g_m|^2 < \Delta_{12},\ |g_m|^2 \geq \Delta_{31}|g_e|^2 + \Delta_{32}\}. \tag{24}$$

Let us denote $x = |g_m|^2$, $y = |g_e|^2$, and

$$G(x, y) = \begin{cases} 1, \text{ if } x < \Delta_{31} \text{ AND } x \geq \Delta_{31} y + \Delta_{32} > 0 \\ 0, \text{ Otherwise.} \end{cases}$$

As a result, if $E\left[G(x, y)\right]$ is the expected value of function $G(x, y)$, the relation in (24) can be given by

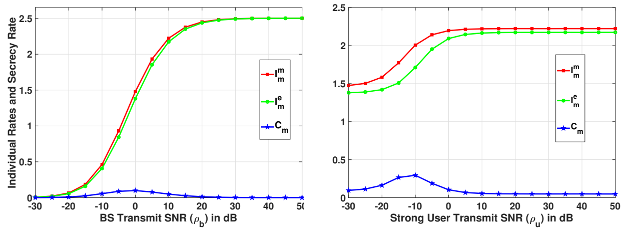
$$\begin{aligned} P_m^3 &= \Pr\{x < \Delta_{12},\ x \geq \Delta_{31}\, y + \Delta_{32}\} = E\left[G(x, y)\right] \\ &= \begin{cases} \int_0^{\frac{\Delta_{12}-\Delta_{31}}{\Delta_{32}}} f_y(y) \int_{x=\Delta_{31} y + \Delta_{32}}^{\Delta_{12}} f_x(x) dx dy \\ \qquad\qquad\qquad\qquad\qquad\qquad , \ \Delta_{12} > \Delta_{32} \\ 0 \qquad\qquad\qquad\qquad\qquad\quad , \ \text{Otherwise} \end{cases} \\ &= \int_0^{\frac{\Delta_{12}-\Delta_{31}}{\Delta_{31}}} \lambda e^{-\lambda y} \left[-e^{\lambda \Delta_{12}} + e^{-\lambda(\Delta_{31} y + \Delta_{32})} \right] dy, \\ &= e^{-\lambda \Delta_{12}} \left[e^{-\lambda \frac{\Delta_{12}-\Delta_{32}}{\Delta_{31}}} - 1 \right] \\ &\quad - \frac{e^{-\lambda \Delta_{32}}}{1 + \Delta_{31}} \left[e^{-\lambda(1+\Delta_{31})(\Delta_{12}-\Delta_{32})/\Delta_{31}} - 1 \right]. \end{aligned} \tag{25}$$

On the other hand, the value of P_n for user n is given by

$$\begin{aligned} P_n \quad &= \Pr\{C_n \geq R_n^{th}\} = \Pr\{\frac{1 + \gamma_{sn}^n}{1 + \gamma_{sn}^e} \geq C_n^{th}\} \\ &= \Pr\{1 + \frac{\rho_b a_n |h_n|^2}{d_n^\alpha} \geq C_n^{th} + \frac{C_n^{th} \rho_b a_n |h_e|^2}{d_e^\alpha}\} \\ &= \Pr\{|h_n|^2 \geq \frac{(C_n^{th} - 1) d_n^\alpha}{\rho_b a_n} + \frac{C_n^{th} d_n^\alpha |h_e|^2}{d_e^\alpha}\} \\ &= 1 - \Pr\{|h_n|^2 < \Psi_1 |h_e|^2 + \Psi_2\} \\ &= 1 - \int_{z=0}^{\infty} F_{|h_n|^2}(\Psi_1 |h_e|^2 + \Psi_2) f_{|h_e|^2}(z) dz \\ &= 1 - \int_{z=0}^{\infty} \left[1 - \exp\{-\lambda(\Psi_1 z + \Psi_2)\}\right] \lambda e^{-\lambda z} dz \\ &= \frac{e^{-\lambda \Psi_2}}{1 + \Psi_1}, \end{aligned} \tag{26}$$

where $\Psi_1 = \frac{C_n^{th} d_n^\alpha}{d_e^\alpha}$ and $\Psi_2 = \frac{(C_n^{th} - 1) d_n^\alpha}{\rho_b a_n}$.

B. Further Discussions



(a) Influence of ρ_b.

(b) Influence of ρ_u.

Fig. 2: A sample illustration to achieve the optimal secrecy performance through power control.

Given the aforementioned analysis, we would like to see whether we can achieve the optimal secrecy performance by tuning any of the system parameters. If we look at the effective SINR of both the strong user (γ_{sn}^n) and the eavesdropper (γ_{sn}^e), they are proportional to ρ_b in a straightforward manner. Therefore, the better the value of ρ_b, the better its secrecy rate. On the other hand, for the weak user case, its effective SINR (γ_m^m) and that of the eavesdropper (γ_m^e) are connected to the "min" function. At a lower value of ρ_b, both γ_m^m and γ_m^e are dominated by γ_{sm}^n while maintaining the increasing trend, and this is other way around (i.e., dominated by γ_{nm}^m and γ_{nm}^e, respectively) at a higher value of ρ_b. Therefore, for a certain value of ρ_u, the optimal secrecy rate is somewhere at the middle value of ρ_b, which is clearly shown in Fig. 2a.

In the similar manner, at lower value of ρ_u, γ_m^m and γ_m^e are dominated by γ_{nm}^m and γ_{nm}^e in an increasing manner, respectively, and this is other way around for the other case. Moreover, at high SNR regime, the value of γ_{sm}^n is the same constant a_m/a_n for the weak user and the eavesdropper. Therefore, the secrecy rate of the weak user has a convex pattern with respect to ρ_u. We provide a sample evidence of this argument in Fig. 2b. To summarize, these findings from our analytical study reveal that via an appropriate power control at the BS and the strong user, we will be able to reach the optimal secure state given the position of the eavesdropper. As an extension of this work, we would like to study a system with three legitimate users, in which the weakest user can improve its reception reliability via three cooperative transmission phases. In this case, we will require to have the power control at three nodes in order to reach the optimal secure state.

IV. Performance Evaluation

In this section, through numerical simulation, we evaluate the correctness of the proposed analytical scheme under different settings. For the simulation, the setup system is as same as that in Section II. The pico BS is at the center of the cell. There is an eavesdropper and two legitimate users in the system. The channel between two nodes in the system suffers both the small scale fading and path loss effect. Small scale fading follows the exponential distribution with the mean value 1 (i.e., $\lambda = 1$). The noise signal of all channels has the Gaussian distribution with 0 mean and variance 1. The path loss exponent α is set to 2.

In Fig. 3, we plot the SOP of each individual user as well as the system with the increasing value of ρ_b. The increasing value of ρ_b implies the increasing value of SNR. It is natural that as we increase the SNR, the secrecy rate is increased. Therefore, given the constant threshold for both the users, the SOP should decrease with the increasing secrecy rate. This trend is the same for the strong user as its secrecy rate is proportional to ρ_b and the eavesdropper is relatively far away. However, as discussed in Section III-B, due to the "min" function in the SNR expression of the weak user and the eavesdropper, the SOP decreases first and then increases. Moreover, the derived analytical expression for the weak user

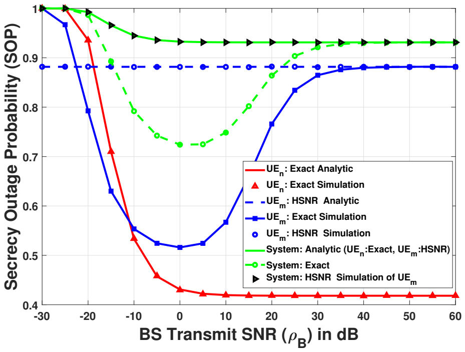


Fig. 3: Comparison of SOP with the increasing BS transmit SNR (ρ_b), where $a_m = 0.6$ and $\rho_u = 0$ dB.

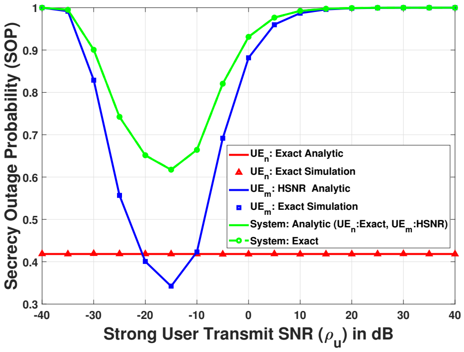


Fig. 4: Comparison of SOP with the increasing strong user transmit SNR (ρ_u), where $a_m = 0.6$ and $\rho_b = 60$ dB.

is valid only at high SNR regime, and hence we see that the analytical results just match with the simulation ones at around ≥ 30 dB. On the other hand, regarding the correctness of our analytical results at high SNR regime, we plot the results of the simulation that is conducted in high SNR regime as well. Since the analytical derivation of the strong user is exact (no matter the value of ρ_b is), it matches with the exact simulation results. The system SOP occurs if either of the users fails to achieve its threshold secrecy rate. Consequently, the system SOP is even larger than that of either of the users and its analytical results just match with the simulation ones at high SNR regime. Since the analytical derivation of the weak user is based on the assumption that the value of ρ_b is high, in the following subsequent results, we set ρ_b to 60 dB.

In Fig. 3, we show the SOP with the increasing value of ρ_u (i.e., the transmit SNR of the strong user). Since the secrecy rate of the strong user is independent of ρ_u, this remains constant no matter the value of ρ_u is. On the other hand, we see the interesting convex trend for the weak user. This is due to the "min" function of the SNR expression of both the weak user and the eavesdropper. At lower value of ρ_u, the effective SINR of UE$_m$ and the eavesdropper are dominated by the second parameter (which is a proportional function of ρ_u) of the "min" function. Consequently, at a lower value of ρ_u, the secrecy rate has an increasing trend (i.e., the SOP has a decreasing trend). However, at a higher value of ρ_u, the effective SINR is dominated by the first parameter of the "min" function which is equal for both the weak user and the eavesdropper. Consequently, the secrecy rate of the weak user is reduced due to the equality nature of the second parameter between the weak user and the eavesdropper. As a result, the SOP has an increasing trend at the increasing value of ρ_u. Since the SOP of the strong user is constant, the trend of the system SOP is dominated by that of the weak user.

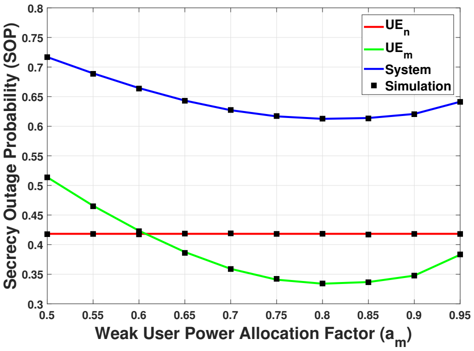


Fig. 5: Comparison of SOP with the increasing weak user power allocation factor (a_m), where $\rho_b = 60$ dB and $\rho_u = 0$ dB.

In order to show the variation of the SOP with different power allocation factors between the strong and weak users, we plot Fig. 5. The increasing value of a_m means the decreasing value of a_n ($a_m + a_n = 1$), and the secrecy rate of the weak and strong users are a function of a_m and a_n, respectively. As a result, the SOP of the weak and strong users have a decreasing and an increasing trend, respectively, with the increasing value of a_m. Although the increasing trend of the strong user is not that much obvious at high SNR regime, this is highly acute at low SNR regime. This is due to the fact that the secrecy rate of the strong user is mostly dominated by ρ_b rather than a_n (the value of which is < 1). On the other hand, since the change of SOP for the strong user is not that much obvious with the increasing value of a_m, the system SOP has the same trend as that of the weak user.

In Fig. 6, we plot the SOP with the increasing horizontal distance of the strong user from the BS (d_n). The secrecy rate of the strong user is inversely proportional to its distance from the BS, and hence the corresponding SOP has an increasing trend with the increasing value of d_n. On the other hand, the weak user receives information from the BS and the strong user in two phases. In the first phase, when it receives information from the BS, the corresponding secrecy rate of the weak user is independent of d_n. However, in the second phase, with the increasing value of d_n, the distance between the strong user and the weak user decreases. Moreover, at this stage, its secrecy rate is inversely proportional to its distance

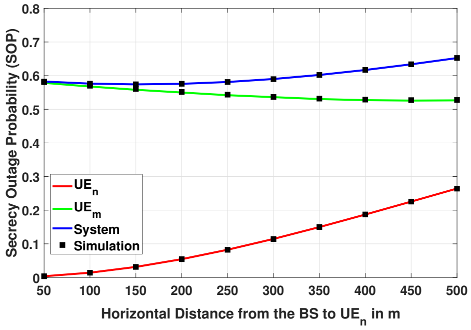


Fig. 6: Comparison of SOP with the increasing strong user horizontal distance from the BS (d_n), where $\rho_b = 60$ dB, $\rho_u = 0$ dB and $a_m = 0.6$.

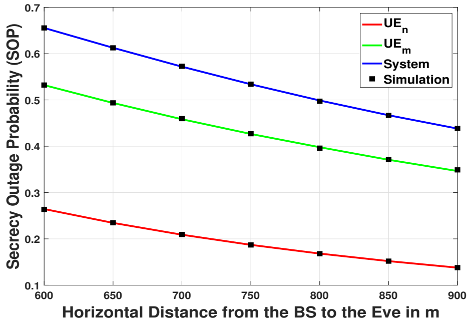


Fig. 7: Comparison of SOP with the increasing eavesdropper horizontal distance from the BS, where $\rho_b = 60$ dB, $\rho_u = 0$ dB and $a_m = 0.6$.

towards the strong user. As a result, the SOP of the weak user decreases with the increasing value of d_n. Since the SOP variation trend of the weak user is not that much acute, the system SOP is mostly dominated by that of the strong user.

The system setup of Fig. 7 is made in such a way that the eavesdropper remains in 45^o angle with the X-axis, but its horizontal distance is varied. The increasing horizontal distance implies the increasing distance of the eavesdropper from the BS. The secrecy rate of both the users is proportional to the distance of the eavesdropper from the BS. As a result, we see the decreasing trend of the SOP for both the users with the increasing horizontal distance of the eavesdropper. Consequently, the system SOP follows the same trend as that of both the users, but obviously has higher value compared to both the users.

V. Conclusion

Being motivated by the inherent cooperative feature of NOMA systems, in this paper, we studied the physical layer security of such a dual-user system in which the strong user acts as a relay for the weak user. Given the assumption that there is a passive eavesdropper in the system, we derived the closed form expression of SOP for both the users. Since the exact SOP of the weak user is intractable, we derived it in the high SNR regime. Extensive simulations were conducted in order to verify the correctness of the analytical derivations as well as to find the optimal setup in which the most secured communication is possible. Via both the analytical arguments and simulation, we showed that the optimal security can be achieved via an appropriate power control at the BS and the strong user.

References

[1] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA),” in *Proc. IEEE PIMRC*, June 2013, pp. 611–615.

[2] N. Otao, Y. Kishiyama, and K. Higuchi, “Performance of non-orthogonal access with SIC in cellular downlink using proportional fair-based resource allocation,” in *Proc. ISWCS*, Aug 2012, pp. 476–480.

[3] Z. Ding, M. Peng, and H. V. Poor, “Cooperative Non-Orthogonal Multiple Access in 5G Systems,” *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug 2015.

[4] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, “Cooperative Non-orthogonal Multiple Access With Simultaneous Wireless Information and Power Transfer,” *IEEE J. Sel. A. Commun.*, vol. 34, no. 4, pp. 938–953, April 2016.

[5] Y. Chen, L. Wang, and B. Jiao, “Cooperative multicast non-orthogonal multiple access in cognitive radio,” in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[6] Y. Zhou, V. W. Wong, and R. Schober, “Performance Analysis of Cooperative NOMA with Dynamic Decode-and-Forward Relaying,” in *Proc. IEEE GLOBECOM*, Dec 2017, pp. 1–6.

[7] Y. Liu, G. Pan, H. Zhang, and M. Song, “Hybrid Decode-Forward and Amplify-Forward Relaying With Non-Orthogonal Multiple Access,” *IEEE Access*, vol. 4, no. 1, pp. 4912–4921, Jan 2016.

[8] Z. Yang, Z. Ding, Y. Wu, and P. Fan, “Novel Relay Selection Strategies for Cooperative NOMA,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10 114–10 123, Nov 2017.

[9] X. Liang, Y. Wu, D. W. K. Ng, Y. Zuo, S. Jin, and H. Zhu, “Outage Performance for Cooperative NOMA Transmission with an AF Relay,” *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2428–2431, Nov 2017.

[10] C. Zhong and Z. Zhang, “Non-Orthogonal Multiple Access With Cooperative Full-Duplex Relaying,” *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2478–2481, Dec 2016.

[11] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[12] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical Layer Security of TAS/MRC With Antenna Correlation,” *IEEE Trans. Inform. Forensics and Security*, vol. 8, no. 1, pp. 254–259, Jan 2013.

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

[14] M. Zhang and Y. Liu, “Energy Harvesting for Physical-Layer Security in OFDMA Networks,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154–162, Jan 2016.

[15] Y. Zou, X. Wang, and W. Shen, “Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks,” *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, December 2013.

[16] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks,” *IEEE Trans. Wirel. Commun.*, vol. 16, no. 3, pp. 1656–1672, March 2017.

[17] B. He, A. Liu, N. J. Yang, and V. K. N. Lau, “On the Design of Secure Non-Orthogonal Multiple Access Systems,” *CoRR*, vol. abs/1612.06961, 2016. [Online]. Available: http://arxiv.org/abs/1612.06961

[18] J. Chen, L. Yang, and M. S. Alouini, “Physical Layer Security for Cooperative NOMA Systems,” *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2018.

[19] D. Tse and P. Viswanath, “Fundamentals of wireless communication,” *Cambridge University Press*, 2005.