Performance Analysis of Multi-Phase Cooperative NOMA Systems under Passive Eavesdropping[☆]

Rukhsana Ruby[a,1], Taneli Riihonen[c], Kaishun Wu[a,d,*], Ye Liu[a], Basem M ElHalawany[a,b,1]

[a] *College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China*
[b] *Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt*
[c] *Unit of Electrical Engineering, Faculty of Information Technology and Communication Sciences, Tampere University*
[d] *Guangzhou HKUST Fok Ying Tung Research Institute, Guangzhou, Guangdong, China*

Abstract

A key feature of the non-orthogonal multiple access (NOMA) technique is that users with better channel conditions have prior knowledge about the information of other weak users. Given this prior knowledge, the idea that a strong user can serve as a relay node for other weak users in order to improve their performance, is known as cooperative NOMA. In this paper, we study the physical layer security of such a cooperative NOMA system. In order to reduce the complexity of the analytical process, the considered system in this paper has three users, in which the performance of the weaker users are enhanced by the stronger users. Given that there is an eavesdropper in the system that can hear all the transmissions, we study the secrecy performance of all the users. More specifically, we make an attempt to derive the ergodic secrecy capacity (ESC) and secrecy outage probability (SOP) of all the users. Due to the intractable nature of the exact analysis for the weak users, we provide the closed form expressions of the ESC and SOP for these users at the high SNR regime, while providing the exact analysis for the strongest user. Targeting on the optimality, we further reveal that better secrecy performance of the system is achievable through an appropriate power control mechanism. Finally, based on the analytical methodology of the three-user cooperative system, we provide insightful observations on the performance (in terms of ESC and SOP) of a multi-phase cooperative NOMA system with N users at the high SNR regime. Through rigorous numerical simulations, we verify the correctness of our analytical derivations under different practical scenarios while providing evidence of achieving optimal secrecy performance with the proposed power control scheme.

Keywords: Cooperative NOMA Systems, Physical-Layer Security, Secrecy Outage Probability, Ergodic Secrecy Capacity, Power Control, Secure Communication Systems, Passive Eavesdropping

[☆]This research was supported in part by the China NSFC International Young Scientist Grant (61850410538), China NSFC Grant (U2001207, 61872248), Guangdong NSF 2017A030312008, Shenzhen Science and Technology Foundation (No. ZDSYS20190902092853047), the Project of DEGP (No. 2019KCXTD005). Kaishun Wu is the corresponding author.

[*]wu@szu.edu.cn

Email addresses: ruby@szu.edu.cn (Rukhsana Ruby), taneli.riihonen@tuni.fi (Taneli Riihonen), wu@szu.edu.cn (Kaishun Wu), ..@... (Ye Liu), basem.mamdoh@{szu.edu.cn, feng.bu.edu.eg} (Basem M ElHalawany)

[1]Joint First Author.

1. Introduction

Non-orthogonal multiple access (NOMA) [1] is considered one of the breakthrough technologies for 5G systems because of its ability to achieve superior spectral efficiency. Typically, this technique utilizes the information in the power domain for achieving the outcome of multiple-access strategies, which is unlike the conventional orthogonal multiple access structures, such as frequency division multiple access. Because of having less power level, users with better channel condition can decode the information of other weaker users by applying the successive interference cancellation (SIC) technique [2]. As a result, these stronger users can improve the performance of the weaker users by re-transmitting the decoded information using the decode-and-forward (DF) relaying technique via conventional short-range communication technologies, such as Bluetooth and Ultra Wide Band (UWB). Consequently, a weak user can use the maximum ratio combining (MRC) technique to combine all information sent to itself. Therefore, in NOMA systems, a strong user can play the role of a relay node for weaker users, and thus additional relay nodes are not required to be deployed in order to obtain the benefit of the cooperation concept in wireless communications [3, 4].

The expected benefits of cooperative NOMA transmission have drawn extensive research interest. With this idea, numerous works appeared in the literature from different technological perspectives. For example, in [5], the outage probability and diversity order are analytically studied. For the similar type of two-user system, in [6], the average block error rate (BLER) is derived for both the users. For the similar type of model, in [7], the amplify-and-forward (AF) relaying ability is considered for the strong user instead of the DF relay. A variant of two-user cooperative NOMA system is studied in [8], in which the base station (BS) jointly with the strong user transmit data to the weak user following the uplink NOMA strategy. Besides considering the strong user as a relay, a multi-relay cooperative two-user NOMA system is also studied in [9]. While assuming the strong user as a relay with the full-duplex and energy harvesting communication capabilities, one more similar type of work is [10]. For another such a system [11], in which near NOMA users that are close to the source node act as energy harvesting relays to help far NOMA users, outage probability and system throughput are studied. Cooperative NOMA concept in a multi-cast and multi-user system [12], [13] is studied as well. In [14], the authors have proposed a dynamic NOMA strong user selection scheme for each weak user that can improve its reception reliability. Moreover, since conventional multiple-input-multiple-output (MIMO)-NOMA systems have higher power consumption and implementation complexity, a much lower complexity cooperative MIMO-NOMA system is designed in [15] with the assistance of the spatial modulation idea.

Wireless communication networks are more vulnerable to security threats due to the broadcast nature of the wireless medium. Unlike the strategies at the higher layer, physical layer security (PLS) techniques can enhance the security of wireless communication networks [16] in a more convenient manner. In this paper, on the presence of a passive eavesdropper, we study the secrecy performance of a cooperative NOMA system. Many works came out recently for NOMA-equipped networks that studied the PLS. For example, in [17], secrecy performance is studied for a multi-relay NOMA system with the presence of an eavesdropper using

the relay selection idea. In [18], the security problem of preventing multi-cast receivers from intercepting unicast messages was considered. By applying the full duplex technology and artificial noises, the instantaneous and ergodic secrecy rates of a secure NOMA-based two-way relay network were analyzed in [19]. Under the presence of multi-eavesdropper, the authors in [20] have studied the secrecy performance of a uplink NOMA system. In [21], the authors have studied the maximization of the strong user secrecy rate under some user-specific constraints. Besides conventional NOMA systems, there are some works that studied the secrecy performance of cooperative NOMA networks. For example, in [22], the authors have studied the tradeoff between security and reliability in such a network with the cognitive ability. Another similar type of work with the cognitive ability is [23]. Under the presence of a passive eavesdropper, there is one work [24], that is similar to ours and studied the secrecy performance. However, unlike us, the authors in this work implemented the cooperation concept via deploying one real relay node either with the AF or DF mode. Relay-based cooperative NOMA has been used for emerging networks like vehicular networks [25].

Besides studying the theoretical secrecy performance, there are some works that designed a secure NOMA system. Along this line, in [26], the authors have proposed a secure SIC technique so that a strong user cannot hijack or eavesdrop the information of a weaker user. In [27], the authors have proposed a downlink cascaded zero forcing (ZF) beamforming technique to secure communications in a two-cell MIMO-NOMA-based network with the cognitive ability. The secrecy performance of both the single-antenna and multi-antenna networks can be enhanced by artificial noises, in which part of the transmit power is used to generate artificial jamming signals to confuse potential eavesdroppers. For example, in [28], an artificial-noise-aided cooperative jamming scheme was proposed to improve the security of a primary user network. A NOMA equipped two-way relay network was studied in [29], where all user pairs transmit jamming signals simultaneously in the multiple access phase. In [30], the PLS was studied under the presence of a full-duplex active eavesdropper. For multiple-input-single-output (MISO)-NOMA networks, there are works [31, 32] as well that enhance the secrecy performance using the jamming technique. Besides the usage of the jamming technique, the secure beamforming and power level optimization algorithm was designed for NOMA systems in [33][34]. In [35], for a large-scale NOMA-based 5G system, two different structures were proposed to improve the secrecy performance for single antenna and multiple-antenna networks via the stochastic geometry concept. A new design of the NOMA technique under secrecy considerations was proposed in [36], the objective of which is to determine the optimal decoding order, transmission rates and power level allocated to each user. In [37], inter-user interference and NOMA techniques were combined to deliberately confuse any eavesdropper. In [38], the authors proved that the mobility feature of a node improves the secrecy performance of a NOMA-based network. For a system similar to ours, in which a strong user acts as a relay for a weaker user, there are couple of works [39, 40] that attempt to enhance the secrecy performance. In [39], a full-duplex separate relay is equipped to enhance the secrecy performance via the jamming signal. Despite having the similar type of system model, in [40], the secrecy performance of two separate data streams, generated by the original source node and the strong user, are studied which is not

actually the achievable rate of any user in the system. Furthermore, the system in this work has only two users, and hence this is a two-phase cooperative NOMA system. On the other hand, in this paper, we have studied the secrecy performance (i.e., ergodic secrecy capacity (ESC) and secrecy outage probability (SOP)) of all the users separately in a three-phase cooperative NOMA system.

In this paper, we study the secrecy performance of a three-user cooperative NOMA system without deploying any real relay. The cooperation concept is achieved through the stronger users of the system, which act as the relay for the other weaker users with the objective of enhancing their message decoding reliability. More specifically, on the presence of a passive eavesdropper, we have studied the secrecy performance of all the users in the system in terms of ESC and SOP. Although we have provided the exact closed form expressions of the ESC and SOP for the strongest user, that for the weak users are provided in the high signal-to-noise-ratio (SNR) regime due to the intractable nature of the exact analysis. With the objective of achieving the best possible performance for all the users in the system, we reveal that the optimization of the ratio between the transmit and the noise power at the BS and the stronger users is critical in maximizing the secrecy performance. Besides studying the performance of such a three-phase cooperative NOMA system, we study a general system with N users, where the channel gain of the users follow some order. Specifically, we provide insightful observation on the performance (in terms of ESC and SOP) of all the users in such a multi-phase cooperative NOMA system. The key contributions of this paper are listed as follows.

- Under the presence of a passive eavesdropper, we study the secrecy performance of a three-user cooperative NOMA system, in which the strong user acts as a relay for the other weak users. More precisely, we derive the closed-form expressions of the SOP and ESC for all the users in the system. Since the exact analytical derivation is intractable for the weak users in the system, the analytical outcome for them are provided in the high SNR regime while the exact analytical outcome are provided for the strongest user. Although the derivation of SOP for a two-user cooperative NOMA system is presented already in our conference version [41], the derivation of the ESC and SOP for a three-user cooperative NOMA system are the new and key contributions in this paper.

- To the best our knowledge, this is the first work that studies the user-specific secrecy performance for a three-user cooperative NOMA system. Apparently, although the work in [40] has the same system model as ours, they studied the secrecy performance of two separate data streams generated by the original source node and the strong user, which are not the achievable performance of either the weak user or the strong user. Furthermore, the system in this work has only two users, and hence this is a two-phase cooperative NOMA system. On the other hand, we study the secrecy performance of all the users separately and individually in a three-phase cooperative NOMA system.

- Based on the analytical methodology of the three-phase cooperative system, we also provide insightful observation on the performance of a multi-phase cooperative NOMA system in terms of ESC and SOP. Given certain assumption on the placement and wireless channel of the users, at the high SNR regime,

the ESC and SOP of any weak user is a function of the transmit SNR of the last cooperative user at the last cooperative phase from which it receives signal, and the distance between the last transmitting user (at the last cooperative phase) and itself. Moreover, these metrics of this user are independent of the transmit SNR of the other cooperative users in other cooperative phases and the transmit SNR of the BS, but the functions of power allocation factors of all the cooperative and direct transmission phases from which it receives signal. On the other hand, the exact closed form expressions of the ESC and SOP for the strongest user are achievable, which are the functions of the BS transmit SNR and the distance between the BS and itself.

- Extensive numerical simulations have been conducted in order to verify the correctness of the analytical results under different scenarios. We further reveal that the optimal secrecy performance can be achieved through tweaking the ratio between the transmit and noise power at the BS and the stronger users. This insightful observation has also been verified by the numerical simulation.

The rest of the paper is organized as follows. In Section 2, 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 3. In Section 4, we evaluate the performance of the proposed analytical model. Finally, Section 5 concludes the paper.

For the sake of clarity and in order to improve the readability of this work, we summarize all the mathematical operators as follows. $F_x(.)$ and $f_x(.)$ represent the cumulative distribution function (CDF) and probability density function (PDF) functions of variable x, respectively. $\mathbb{E}[x]$ is the expectation function of variable x, and finally $\mathrm{Ei}(x)$ is the exponential integral function of x.

2. System Model and Background Information

Let us consider a NOMA-equipped cellular system, in which there are a pico BS, three users and a passive eavesdropper. It is assumed that time is slotted and there is one frequency channel in the system. The BS is located at the center of the cell, and a sample system model described herein is provided in Figure 1. The strong and weak users of the system are denoted by UE_z, UE_y and UE_x, respectively. The BS adopts the superposition coding (SC) technique to transmit information of all the users over a dedicated fixed channel. As a result, at this phase, user z is able to decode its and the information of both user x and user y using the successive interference cancellation (SIC) technique. Then, in the next time slot, the strong user applies the SC technique on the decoded signal of both the weak users, and broadcasts over the same fixed channel. At this phase, the MRC technique is adopted at the weak user y to realize the enhanced performance while combining the signals obtained from the BS and the strongest user. At the same time, this user is able to decode the information of user x transmitted by the strong user z. In order to realize the cooperation benefit of the NOMA technique, the weaker user y re-transmits the decoded information of user x spontaneously over the same channel. At this final stage, user x adopts the MRC technique to combine the signals transmitted

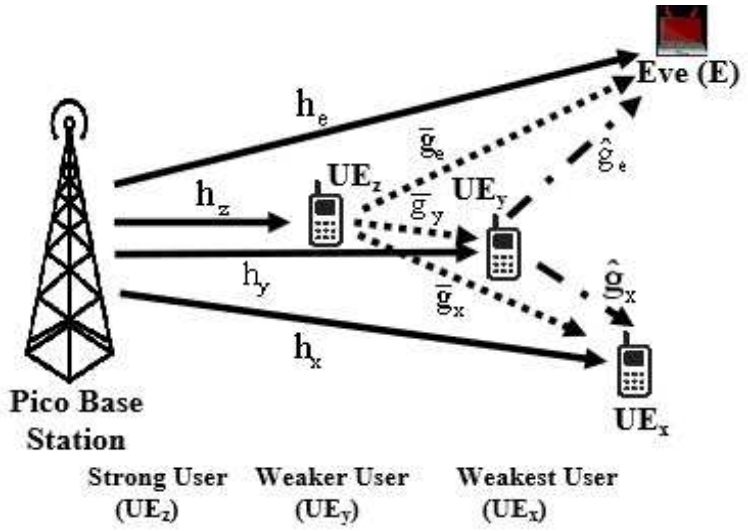


Figure 1: A sample three-phase cooperative NOMA system under a passive eavesdropping scenario.

by the BS, user z and then user y, which is obviously the enhanced and stronger signal compared to the original signal transmitted by only the BS. Thus, the cooperative concept is implemented via the stronger users in the system without employing any real relay nodes. The maximal transmit power level of the BS and the stronger users (i.e., user z and user y) are denoted by P_b, P_z and P_y, respectively. We assume that all nodes in the network are equipped with a single omni-directional antenna and all the channels follow the conventional path loss model accompanied with small scale fading. Moreover, the block fading channel model is assumed, in which the channel state information (CSI) of the users remain constant in a time slot, but vary over different time slots. The CSI can be obtained through the existing channel estimation technology at the user nodes (e.g., MMSE and its variants [42][43]) and feedback to the transmitters (the BS and strong users in the system). The eavesdropper in the system is considered to be an untrusted user, which is curious about the information of other users and has the perfect knowledge of the entire system[2]. The transmission in this network is accomplished in three phases, the description of each one is given in the following.

2.1. Direct Transmission Phase

In this phase, the BS broadcasts the SC-coded mixture, $\chi_b = \sqrt{a_x}s_x + \sqrt{a_y}s_y + \sqrt{a_z}s_z$, where s_x, s_y and s_z are the unit power signal received by user x, user y and user z, respectively, and a_x, a_y and a_z are their power allocation coefficients, respectively. While taking the quality-of-service (QoS) constraints of all the users into account, we assume that $a_x > a_y > a_z$ and $a_x + a_y + a_z = 1$. As a result, the received signals at user x, user y, user z and the eavesdropper can be given, respectively, by $\zeta_\theta = \frac{h_\theta}{d_\theta^\alpha}\ \chi_b\sqrt{P_b} + \omega_\theta$, where $\theta \in \{x, y, z, e\}$, and h_x, h_y, h_z and h_e are the channel gain associated with the small scale fading from the BS to user x, user y, user z and the eavesdropper, respectively. d_x, d_y, d_z and d_e are the distance from the

[2]All the legitimate users in the system are trustworthy to each other, and hence there is no any secrecy concern to any of the users. It is noteworthy that some other recent work in the literature considered security concerns between legitimate users with different security clearance but this is out of the scope of this paper [44].

BS to user x, user y, user z and the eavesdropper, respectively. ω_x, ω_y, ω_z and ω_e are the additive white Gaussian noise (AWGN) with zero mean and variance N_0, and α is the path loss exponent. User z first decodes s_x by treating s_y and s_z as the interference, and then decodes s_y by treating s_z as the interference, and finally obtains s_z by applying the SIC technique. For the sake of simplicity, we assume that $\rho_b = P_b/N_0$. As a result, the signal-to-interference-plus-noise-ratio (SINR) of signals s_x, s_y and s_z at user z can be given by

$$\gamma_{sx}^{z} = \frac{a_x|h_z|^2}{a_y|h_z|^2 + a_z|h_z|^2 + d_z^{\alpha}/\rho_b},\ \gamma_{sy}^{z} = \frac{a_y|h_z|^2}{a_z|h_z|^2 + d_z^{\alpha}/\rho_b} \text{ and } \gamma_{sz}^{z} = \frac{a_z\rho_b|h_z|^2}{d_z^{\alpha}},\ \text{respectively.}$$

User y decodes the signal of user x, s_x, while considering signals s_y and s_z as interference, and then decodes its own signal while taking s_z as the interference, via the adoption of the SIC technique. The resultant SINRs are given by

$$\gamma_{sx}^{y} = \frac{a_x|h_y|^2}{a_y|h_y|^2 + a_z|h_y|^2 + d_y^{\alpha}/\rho_b} \text{ and } \gamma_{sy}^{y} = \frac{a_y|h_y|^2}{a_z|h_y|^2 + d_y^{\alpha}/\rho_b},\ \text{respectively.}$$

Finally, user x decodes its own signal while taking s_y and s_z as the collective interference, and hence its SINR is given by

$$\gamma_{sx}^{x} = \frac{a_x|h_x|^2}{a_y|h_x|^2 + a_z|h_x|^2 + d_x^{\alpha}/\rho_b}.$$

On the other hand, since the eavesdropper is aware of the entire information of the system, it first decodes signal s_x by treating signals s_y and s_z as the interference, then decodes signal s_y while taking signal s_z as the interference, and finally decodes signal s_z deliberately, using the SIC technique. As a result, the SINR of signals s_x, s_y and s_z at the eavesdropper can be given by

$$\gamma_{sx}^{e} = \frac{a_x|h_e|^2}{a_y|h_e|^2 + a_z|h_e|^2 + d_e^{\alpha}/\rho_b},\ \gamma_{sy}^{e} = \frac{a_y|h_e|^2}{a_z|h_e|^2 + d_e^{\alpha}/\rho_b} \text{ and } \gamma_{sz}^{e} = \frac{a_z\rho_b|h_e|^2}{d_e^{\alpha}},\ \text{respectively.}$$

2.2. Cooperative Phase I

In this phase, the strong user z broadcasts the SC-coded mixed signal of the weaker users from the first phase, $\bar{\chi}_u = \sqrt{a_{zx}}s_{zx} + \sqrt{a_{zy}}s_{zy}$, where s_{zx} and s_{zy} are the unit power signal received by user x and user y, respectively, and a_{zx} and a_{zy} are their power allocation coefficients, respectively. Similar to the first transmission phase, we assume that $a_{zx} > a_{zy}$ and $a_{zx} + a_{zy} = 1$, that are based on the fairness criterion. As a result, the received signal at user x, user y and the eavesdropper can be given, respectively, by $\zeta_{z\theta} = \frac{\bar{g}_\theta}{d_{z\theta}^{\alpha}}\ \bar{\chi}_u\sqrt{P_z} + \omega_{z\theta}$, where $\theta \in \{x, y, e\}$, and $\bar{g}_x$, $\bar{g}_y$ and $\bar{g}_e$ are the channel gain associated with the small scale fading from the strong user to user x, user y and the eavesdropper, respectively. d_{zx}, d_{zy} and d_{ze} are the distance from the strong user to user x, user y and the eavesdropper, respectively. ω_{zx}, ω_{zy} and ω_{ze} are the AWGN with zero mean and variance N_0. User y first decodes s_{zx} by treating s_{zy} as the interference, and then obtains s_{zy} by applying the SIC technique. As a result, the SINR of signals s_{zx} and s_{zy} at user y can be given by

$$\gamma_{zx}^{y} = \frac{a_{zx}|\bar{g}_y|^2}{a_{zy}|\bar{g}_y|^2 + d_{zy}^{\alpha}/\rho_z} \text{ and } \gamma_{zy}^{y} = \frac{a_{zy}\rho_z|\bar{g}_y|^2}{d_{zy}^{\alpha}},\ \text{respectively,}$$

where $\rho_z = P_z/N_0$. User x decodes its own signal s_{zx} while considering signal s_{zy} as interference, and hence its SINR is given by

$$\gamma_{zx}^{x} = \frac{a_{zx}|\bar{g}_x|^2}{a_{zy}|\bar{g}_x|^2 + d_{zx}^{\alpha}/\rho_z}.$$

On the other hand, the eavesdropper first decodes signal s_{zx} by treating signal s_{zy} as interference, and then decodes signal s_{zy} deliberately. As a result, the SINR of signal s_{zx} and s_{zy} at the eavesdropper can be given by

$$\gamma_{zx}^{e} = \frac{a_{zx}|\bar{g}_e|^2}{a_{zy}|\bar{g}_e|^2 + d_{ze}^{\alpha}/\rho_z} \text{and } \gamma_{zy}^{e} = \frac{a_{zy}\rho_z|\bar{g}_e|^2}{d_{ze}^{\alpha}}, \text{ respectively.}$$

2.3. Cooperative Phase II

In this phase, the weaker user y broadcasts the extracted weakest user signal from the previous phases, $\hat{\chi}_u = s_{yx}$ with its full power P_y, where s_{yx} is the unit power signal received by user x. Consequently, the received signal at user x and the eavesdropper are given by $\zeta_{y\theta} = \frac{\hat{g}_\theta}{d_{y\theta}^{\alpha}}\hat{\chi}_u\sqrt{P_y} + \omega_{y\theta}$, where $\theta \in \{x, e\}$, and where $\hat{g}_x$ and $\hat{g}_e$ are the channel gain associated with the small scale fading from user y to user x and the eavesdropper, respectively. d_{yx} and d_{ye} are the distance from user y to user x and the eavesdropper, respectively. ω_{yx} and ω_{ye} are the AWGN with zero mean and variance N_0. Given that $\rho_y = P_y/N_0$, we obtain

$$\gamma_{yx}^{x} = \frac{\rho_y|\hat{g}_x|^2}{d_{yx}^{\alpha}} \text{ and } \gamma_{yx}^{e} = \frac{\rho_y|\hat{g}_e|^2}{d_{ye}^{\alpha}},$$

where γ_{yx}^{x} is the SINR of user x decoded by itself, and γ_{yx}^{e} is the SINR of user x decoded by the eavesdropper. Using the maximal ratio combining technique, the combined SINR of user x decoded by itself (i.e., γ_x^x) and the eavesdropper (i.e., γ_x^e) can be given by

$$\begin{aligned}\gamma_x^x &= \gamma_{sx}^{x} + \min\left(\gamma_{sx}^{z}, \gamma_{zx}^{x}\right) + \min\left(\gamma_{zx}^{y}, \gamma_{yx}^{x}\right) \text{ and} \\ \gamma_x^e &= \gamma_{sx}^{e} + \min\left(\gamma_{sx}^{z}, \gamma_{zx}^{e}\right) + \min\left(\gamma_{zx}^{y}, \gamma_{yx}^{e}\right).\end{aligned}$$

In the similar manner, the combined SINR of user y decoded by itself (i.e., γ_y^y) and the eavesdropper (i.e., γ_y^e) are given by

$$\gamma_y^y = \gamma_{sy}^{y} + \min\left(\gamma_{sy}^{z}, \gamma_{zy}^{y}\right) \text{ and } \gamma_y^e = \gamma_{sy}^{e} + \min\left(\gamma_{sy}^{z}, \gamma_{zy}^{e}\right).$$

2.4. Instantaneous Secrecy Capacity

Using the Shannon's capacity formula [45], in an arbitrary time slot, the instantaneous secrecy capacity of user z, user y and user x can be given by

$$C_z = \left[I_z^z - I_z^e\right]^+, \; C_y = \tfrac{1}{2}\left[I_y^y - I_y^e\right]^+ \text{and } C_x = \tfrac{1}{2}\left[I_x^x - I_x^e\right]^+,$$

where $[x]^+ = \max(x, 0)$, and

$$I_z^z = \log_2\left[1 + \gamma_{sz}^{z}\right]^+, \; I_z^e = \log_2\left(1 + \gamma_{sz}^{e}\right), \; I_y^y = \log_2\left(1 + \gamma_y^y\right), I_y^e = \log_2\left(1 + \gamma_y^e\right),$$
$$I_x^x = \log_2\left(1 + \gamma_x^x\right), \text{ and } I_x^e = \log_2\left(1 + \gamma_x^e\right).$$

3. Performance Analysis and Implications

In this paper, we study the ESC and SOP of the aforementioned system. ESC is one of the prominent secrecy measures for a system in which encoded messages experience random channel fading. The ergodicity of the fading channel in such a system can be captured through the evaluation of secrecy capacity or rate. SOP is defined as the probability that the instantaneous secrecy capacity is lower than a predefined threshold. Both the ESC and SOP are important in the context of cooperative NOMA systems since this system transmits multiple data streams over a time slot via the same frequency channel. Given that the fading nature of the wireless channel follows some distribution, ESC and SOP are the appropriate performance metrics to evaluate the achievable performance of the individual data streams or the individual users. In this section, we first derive the closed form expression of the SOP and ESC for all the users in the system, then study the analytical derivation for developing an optimal secure cooperative NOMA system, and finally provide insightful observation on the performance (in terms of ESC and SOP) of a general multi-phase cooperative system with N users.

3.1. Derivation of ESC

Let denote the ESC of user x, user y and user z by $\bar{C}_x$, $\bar{C}_y$ and $\bar{C}_z$, respectively. For the sake of analysis, we assume that $|h_x|^2$, $|h_y|^2$, $|h_z|^2$, $|h_e|^2$, $|\bar{g}_x|^2$, $|\bar{g}_y|^2$, $|\bar{g}_e|^2$, $|\hat{g}_x|^2$ and $|\hat{g}_e|^2$ all follow the exponential distribution with mean $1/\lambda$. We derive the ESC of each user as follows.

3.1.1. User x

According to the definition, the ESC of user x, $\bar{C}_x$ is given by

$$\begin{aligned}\bar{C}_x &= \mathbb{E}\left[(I_x^x - I_x^e)^+\right] \\ &\geq \left(\mathbb{E}[I_x^x] - \mathbb{E}[I_x^e]\right)^+ . \end{aligned} \tag{1}$$

The inequality in (1) is the lower bound of $\bar{C}_x$. The simulation results in [46] reveal that this lower bound is close to $\bar{C}_x$ under many realistic simulation settings. Now, we know that

$$\begin{aligned}\mathbb{E}[I_x^x] &\cong \frac{1}{2\ln(2)}\mathbb{E}\left[\ln(1+\gamma_x^x)\right] \\ &= \frac{1}{2\ln(2)}\mathbb{E}\left[\ln\left(1+\gamma_{sx}^x + \min\left(\gamma_{sx}^z, \gamma_{zx}^x\right) + \min\left(\gamma_{zx}^y, \gamma_{yx}^x\right)\right)\right].\end{aligned}$$

While letting $\Pi_x = \min(a_x/(a_y+a_z), a_{zx}/a_{zy})$, at the high SNR regime, we can write

$$\begin{aligned}\mathbb{E}[I_x^x] &\cong \frac{1}{2\ln(2)}\mathbb{E}\left[\ln\left(1+\Pi_x + \frac{a_x}{a_y+a_z} + \min\left\{\frac{a_{zx}}{a_{zy}}, \frac{\rho_y|\hat{g}_x|^2}{d_{yx}^\alpha}\right\}\right)\right] \\ &= \frac{1}{2\ln(2)}\left[D_1 + D_2\right],\end{aligned}$$

where

$$\begin{aligned}D_1 &= \mathbb{E}\left[\ln\left(\frac{1}{a_y+a_z} + \Pi_x + \frac{a_{zx}}{a_{zy}}\right) | \frac{a_{zx}}{a_{zy}} < \frac{\rho_y|\hat{g}_x|^2}{d_{yx}^\alpha}\right], \text{ and} \\ D_2 &= \mathbb{E}\left[\ln\left(\frac{1}{a_y+a_z} + \Pi_x + \frac{\rho_y|\hat{g}_x|^2}{d_{yx}^\alpha}\right) | \frac{a_{zx}}{a_{zy}} > \frac{\rho_y|\hat{g}_x|^2}{d_{yx}^\alpha}\right].\end{aligned}$$

While letting $\xi_{\hat{g}}^x = \frac{a_{zx}}{a_{zy}\mu_{\hat{g}}^x}$ and $\mu_{\hat{g}}^x = \frac{\rho_y}{d_{yx}^\alpha}$, D_1 is rewritten as

$$\begin{aligned} D_1 &= \mathbb{E}\left[\ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{a_{zx}}{a_{zy}}\right) \mid |\hat{g}_x|^2 > \xi_{\hat{g}}^x\right] \\ &= \int_{\xi_{\hat{g}}^x}^{\infty} \ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{a_{zx}}{a_{zy}}\right) f_{|\hat{g}_x|^2}(m)dm \\ &= \lambda e^{-\lambda\xi_{\hat{g}}^x} \ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{a_{zx}}{a_{zy}}\right). \end{aligned}$$

On the other hand, for D_2, we can write

$$\begin{aligned} D_2 &= \mathbb{E}\left[\ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{\rho_y|\hat{g}_x|^2}{d_{yx}^\alpha}\right) \mid |\hat{g}_x|^2 < \xi_{\hat{g}}^x\right] \\ &= \int_0^{\xi_{\hat{g}}^m} \ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{\rho_y}{d_{yx}^\alpha}m\right)\lambda e^{-\lambda m}dm \\ &= \ln\left(\frac{1}{a_y+a_z}+\Pi_x\right) - \lambda e^{-\lambda\xi_{\hat{g}}^x}\ln\left(\frac{1}{a_y+a_z}+\Pi_x+\frac{a_{zx}}{a_{zy}}\right) \\ &\quad - e^{\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^x}}\left[\mathrm{Ei}\left(-\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^x}\right) - \mathrm{Ei}\left(-\frac{a_{zy}+(a_{zx}+\Pi_x a_{zy})(a_y+a_z)}{(a_y+a_z)a_{zy}\mu_{\hat{g}}^x}\right)\right]. \end{aligned}$$

where Ei(.) is the exponential integral function, i.e., $\mathrm{Ei}(x) \cong \int_{-\infty}^{x}(e^{-t}/t)dt$. Now, for the other part of (1), we have

$$\begin{aligned} \mathbb{E}\left[I_x^e\right] &= \mathbb{E}\left[\ln\left(1+\gamma_x^e\right)\right] \\ &= \mathbb{E}\left[\ln\left(1+\gamma_{sx}^e+\min\left(\gamma_{sx}^z,\gamma_{zx}^e\right)+\min\left(\gamma_{zx}^y,\gamma_{yx}^e\right)\right)\right]. \end{aligned}$$

At the hign SNR regime, this can be simplified as

$$\mathbb{E}[I_x^e] \cong \frac{1}{2\ln(2)}\mathbb{E}\left[\ln\left(\frac{1}{a_y+a_z}+\Pi_x+\min\left\{\frac{a_{zx}}{a_{zy}},\frac{\rho_y|g_e|^2}{d_{ye}^\alpha}\right\}\right)\right].$$

Similar to the derivation of $\mathbb{E}[I_x^x]$, we can write

$$\mathbb{E}\left[I_x^e\right] = -\frac{1}{2\ln(2)}e^{\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^e}}\left[\mathrm{Ei}\left(-\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^e}\right) - \mathrm{Ei}\left(-\frac{a_{zy}+(a_{zx}+\Pi_x a_{zy})(a_y+a_z)}{(a_y+a_z)a_{zy}\mu_{\hat{g}}^e}\right)\right],$$

where $\mu_{\hat{g}}^e = \frac{\rho_y}{d_{ye}^\alpha}$. Thus, the derivation of $\bar{C}_x$ is completed, which is given by

$$\begin{aligned} \bar{C}_x &\cong -\frac{1}{2\ln(2)}e^{\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^x}}\left[\mathrm{Ei}(-\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^x}) - \mathrm{Ei}\left(-\frac{a_{zy}+(a_{zx}+\Pi_x a_{zy})(a_y+a_z)}{(a_y+a_z)a_{zy}\mu_{\hat{g}}^x}\right)\right] \\ &+ \frac{1}{2\ln(2)}e^{\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^e}}\left[\mathrm{Ei}(-\frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^e}) - \mathrm{Ei}\left(-\frac{a_{zy}+(a_{zx}+\Pi_x a_{zy})(a_y+a_z)}{(a_y+a_z)a_{zy}\mu_{\hat{g}}^e}\right)\right]. \end{aligned}$$

3.1.2. User y

Similar the derivation of user x, the ESC of user y can be derived as

$$\begin{aligned} \bar{C}_y \cong &-\frac{1}{2\ln(2)}e^{\frac{1-a_x}{a_z\mu_{\hat{g}}^y}}\left[\mathrm{Ei}(\frac{-(1-a_x)}{a_z\mu_{\hat{g}}^y}) - \mathrm{Ei}\left(-\frac{1-a_x+a_y}{a_z\mu_{\hat{g}}^y}\right)\right] \\ &+\frac{1}{2\ln(2)}e^{\frac{1-a_x}{a_z\mu_{\hat{g}}^e}}\left[\mathrm{Ei}(\frac{-(1-a_x)}{a_z\mu_{\hat{g}}^e}) - \mathrm{Ei}\left(-\frac{1-a_x+a_y}{a_z\mu_{\hat{g}}^e}\right)\right], \end{aligned}$$

where $\mu_{\bar{g}}^{y} = \frac{\rho_z}{d_{zy}^{\alpha}}$ and $\mu_{\bar{g}}^{e} = \frac{\rho_z}{d_{ze}^{\alpha}}$.

3.1.3. User z

Finally, we derive the ESC of user z, $\bar{C}_z$, as follows.

$$\bar{C}_z = \mathbb{E}\left[I_z^z - I_z^e\right]^+ = \frac{\Pr\{\gamma_{sz}^z > \gamma_{sz}^e\}}{\ln(2)} \mathbb{E}\left[\ln(1+\gamma_{sz}^z) - \ln(1+\gamma_{sz}^e)\right].$$

Let $p = \gamma_{sz}^n = \mu_p |h_z|^2$ and $q = \gamma_{sz}^e = \mu_q |h_e|^2$, where $\mu_p = a_z \rho_b / d_z^{\alpha}$ and $\mu_q = a_z \rho_b / d_e^{\alpha}$.

$$\begin{aligned}
\bar{C}_z &= \frac{1}{\ln(2)} \left[\int_0^{\infty} \ln(1+p) f_P(p) F_Q(p) dp - \int_0^{\infty} \ln(1+q) f_Q(q) (1 - F_P(q)) dq \right] \\
&= \frac{1}{\ln(2)} \left[M_1 + M_2 - M_3 \right], \text{where}
\end{aligned}$$

$$\begin{aligned}
M_1 &= \int_0^{\infty} \ln(1+p) f_P(p) F_Q(p) dp \\
M_2 &= \int_0^{\infty} \ln(1+q) f_Q(q) F_P(q) dq \\
M_3 &= \int_0^{\infty} \ln(1+q) f_Q(q) dq.
\end{aligned}$$

Note that $f_P(p) = \frac{\lambda}{\mu_p} e^{-\lambda p/\mu_p}$, $f_Q(q) = \frac{\lambda}{\mu_q} e^{-\lambda q/\mu_q}$, $F_P(p) = 1 - e^{-\lambda p/\mu_p}$, $F_Q(q) = 1 - e^{-\lambda q/\mu_q}$, $F_P(q) = 1 - e^{-\lambda q/\mu_p}$ and $F_Q(p) = 1 - e^{-\lambda p/\mu_q}$. Now,

$$\begin{aligned}
M_1 &= \int_0^{\infty} \ln(1+p) \frac{\lambda e^{-\lambda p/\mu_p}}{\mu_p} \left(1 - e^{-\lambda p/\mu_q}\right) dp \\
&= \int_0^{\infty} \frac{\lambda \ln(1+p)}{\mu_p} e^{-\lambda p/\mu_p} dp - \int_0^{\infty} \frac{\lambda \ln(1+p)}{\mu_p} e^{-\lambda p(\frac{1}{\mu_p} + \frac{1}{\mu_q})} dp.
\end{aligned}$$

Based on the fact $\int_0^{\infty} e^{-\mu m} \ln(\beta + m) dm = \frac{1}{\mu} \left[\ln\beta - e^{\mu\beta} \mathrm{Ei}(-\mu\beta)\right]$, we can write

$$M_1 = -\lambda e^{\lambda/\mu_p} \mathrm{Ei}\left(\frac{-\lambda}{\mu_p}\right) + \frac{\lambda \mu_q e^{\frac{\lambda \mu_p \mu_q}{\mu_p + \mu_q}}}{\mu_p + \mu_q} \mathrm{Ei}\left(-\frac{\lambda \mu_p \mu_q}{\mu_p + \mu_q}\right).$$

In the similar manner, we can write M_2 and M_3 as

$$M_2 = -\lambda e^{\lambda/\mu_q} \mathrm{Ei}\left(\frac{-\lambda}{\mu_q}\right) + \frac{\lambda \mu_p e^{\frac{\lambda \mu_p \mu_q}{\mu_p + \mu_q}}}{\mu_p + \mu_q} \mathrm{Ei}\left(-\frac{\lambda \mu_p \mu_q}{\mu_p + \mu_q}\right) \text{ and}$$

$$M_3 = \int_0^{\infty} \ln(1+q) \frac{\lambda e^{-\lambda q/\mu_q}}{\mu_q} dq = -\lambda e^{\lambda/\mu_q} \mathrm{Ei}\left(-\frac{\lambda}{\mu_q}\right), \text{ respectively.}$$

While combining M_1, M_2 and M_3, the derivation of $\bar{C}_z$ for user z is completed.

3.1.4. Comparison with [40]

The system in [40] is a two-phase cooperative NOMA system, while our one is a three-phase cooperative NOMA system. The work in [40] has derived only ESC of the transmitted data streams destined to only one user, while we derive both ESC and SOP of all the users in the system individually. Moreover, the authors in [40] derive the achievable secrecy rate of these two data streams separately while considering the minimum one achieved over the direct transmission and relay transmission links. On the other hand, in our case, each data stream belongs to each user in the system. Since the strong users in our system can decode the information signal of other weak users, in order to improve the signal reliability of these weak users, the strong users broadcast the decoded information of these users at the following cooperative transmission phases. At the end of all transmissions, each weak user adds up the information signal received from all the strong users (stronger than the corresponding weak user) and the BS using the MRC technique. Then, we derive the ESC and SOP of all the users individually based on their instantaneous achievable rate obtained at the end of all transmissions. Because of the aforementioned difference between our system and that in [40], we have not compared the performance of our system with that of [40] in the evaluation section (i.e., Section 4).

3.2. Derivation of SOP

The partial content of this section is taken from our conference paper [41]. For the sake of derivation, let us denote the threshold capacity of user x, user y and user n by C_x^{th}, C_y^{th} and C_z^{th}, respectively. Therefore, according to the definition, the outage probability of the system can be given by

$$\begin{aligned} \text{SOP} &= \Pr\{C_x < C_x^{th} \text{ OR } C_y < C_y^{th} \text{ OR } C_z < C_z^{th}\} \\ &= 1 - \Pr\{C_x \geq C_x^{th},\ C_y \geq C_y^{th},\ C_z \geq C_z^{th}\}. \end{aligned}$$

As a result, the individual SOP of user x, user y and user z can be given by $1 - P_x$, $1 - P_y$ and $1 - P_z$, respectively, where $P_x = \Pr\{C_x \geq C_x^{th}\}$, $P_y = \Pr\{C_y \geq C_y^{th}\}$ and $P_z = \Pr\{C_z \geq C_z^{th}\}$. It is noteworthy that the system SOP can be formulated as $SOP = 1 - P_x\ P_y\ P_z$ at the high SNR regime due to the absence of correlation among different users. We derive the SOP of each user as follows.

3.2.1. User x

We first explore the probability P_x for user x as follows. According to the definition, we have $P_x = \Pr\{\frac{1+\gamma_x^x}{1+\gamma_x^e} \geq 2^{2C_x^{th}}\}$. If $\zeta_x^{th} = 2^{2C_x^{th}}$, the expression $\frac{1+\gamma_x^x}{1+\gamma_x^e} \geq \zeta_x^{th}$ can be written as

$$\min\left(\gamma_{sm}^z, \gamma_{zx}^x\right) + \min\left(\gamma_{zx}^y, \gamma_{yx}^x\right) \geq \zeta_m^{th}(1+\gamma_{sx}^e) + \zeta_x^{th} \min\left(\gamma_{sx}^z, \gamma_{zx}^e\right) + \zeta_x^{th} \min\left(\gamma_{zx}^y, \gamma_{yx}^e\right) - 1 - \gamma_{sx}^x. \tag{2}$$

Because of the "min" function and the interference term of γ_{sx}^x, γ_{sx}^z, γ_{zx}^x, γ_{zx}^y, γ_{sx}^e and γ_{zx}^e, the closed form expression of P_x is not tractable. However, at the high SNR regime, we can write $\gamma_{sx}^x = \gamma_{sx}^z = \gamma_{sx}^e = \frac{a_x}{a_y + a_z}$ and $\gamma_{zx}^x = \gamma_{zx}^y = \gamma_{zx}^e = \frac{a_{zx}}{a_{zy}}$. In this case, while letting $\Pi_x = \min(a_x/(a_y + a_z), a_{zx}/a_{zy})$, the expression in

(2) can be written as

$$\min\left(\frac{a_{zx}}{a_{zy}}, \gamma_{yx}^{x}\right) \geq \frac{\zeta_x^{th}-1}{a_y+a_z} + \Pi_x(\zeta_x^{th}-1) + \zeta_x^{th}\min\left(\frac{a_{zx}}{a_{zy}}, \gamma_{yx}^{e}\right). \tag{3}$$

Let $B_x = \frac{\zeta_x^{th}-1}{a_y+a_z} + \Pi_x(\zeta_x^{th}-1)$, the probability of the expression in (3) is equivalent to

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

where

$$\begin{aligned}
P_x^1 &= \Pr\{\gamma_{yx}^{x} \geq \frac{a_{zx}}{a_{zy}} \text{ AND } \frac{a_{zx}}{a_{zy}} \geq \zeta_x^{th}\gamma_{yx}^{e} + B_x\} \\
P_x^2 &= \Pr\{\gamma_{yx}^{x} \geq \frac{a_{zx}}{a_{zy}} \text{ AND } \frac{a_{zx}}{a_{zy}} \geq \zeta_x^{th}\frac{a_{zx}}{a_{zy}} + B_x\} \\
P_x^3 &= \Pr\{\frac{a_{zx}}{a_{zy}} \geq \gamma_{yx}^{x} \text{ AND } \gamma_{yx}^{x} \geq \zeta_x^{th}\gamma_{yx}^{e} + B_x\} \text{ and} \\
P_x^4 &= \Pr\{\frac{a_{zx}}{a_{zy}} > \gamma_{yx}^{x} \text{ AND } \gamma_{yx}^{x} \geq \zeta_x^{th}\frac{a_{zx}}{a_{zy}} + B_x\}.
\end{aligned}$$

The values of P_x^2 and P_x^4 are 0 as the expressions associated with these probabilities are impossible to happen in practice. However, the simplified value of P_x^1 can be written as

$$P_x^1 = \Pr\{|\hat{g}_x|^2 \geq \Delta_{12},\ |\hat{g}_e|^2 \leq \Delta_{13}\},\ \text{where}$$
$$\Delta_{11} = \frac{d_{ye}^{\alpha}}{a_{zy}\zeta_x^{th}\rho_y},\ \Delta_{12} = \frac{a_{zx}d_{yx}^{\alpha}}{a_{zy}\rho_y} \text{and } \Delta_{13} = \Delta_{11} - \frac{B_x d_{ye}^{\alpha}}{\rho_y \zeta_x^{th}}.$$

This in turn is equivalent to

$$P_x^1 = \Pr\{|\hat{g}_x|^2 \geq \Delta_{12}\} \times \Pr\{|\hat{g}_e|^2 \leq \Delta_{13}\}.$$

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

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

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

$$\begin{aligned}
P_x^3 &= \Pr\{|\hat{g}_x|^2 < \Delta_{12}, |\hat{g}_x|^2 \geq \Delta_{31}|\hat{g}_e|^2 + \Delta_{32}\} \\
&= \begin{cases} \displaystyle\int_0^{\Delta_o} f_{|\hat{g}_e|^2}(n) \int_{m=\Delta_{31}n+\Delta_{32}}^{\Delta_{12}} f_{|\hat{g}_x|^2}(m) dm dn \\ \qquad\qquad\qquad\qquad , \Delta_{12} > \Delta_{32} \\ 0 \qquad\qquad\qquad\qquad , \text{Otherwise} \end{cases}
\end{aligned} \tag{5}$$

where $\Delta_{31} = \zeta_x^{th} d_{yx}^{\alpha}/d_{ye}^{\alpha}$, $\Delta_{32} = B_x d_{yx}^{\alpha}/\rho_y$ and $\Delta_o = \frac{\Delta_{12}-\Delta_{32}}{\Delta_{31}}$. By solving the integration in (5), we can express P_x^3 as follows

$$P_x^3 = e^{-\lambda\Delta_{12}}\left[e^{-\lambda\Delta_o} - 1\right] - \frac{e^{-\lambda\Delta_{32}}}{1+\Delta_{31}}\left[e^{-\lambda(1+\Delta_{31})\Delta_o} - 1\right].$$

3.2.2. User y

Following the derivation of user x, for user y, P_y can be derived in a straightforward manner as follows.

$$P_y = P_y^1 + P_y^3,$$

$$P_y^1 = \begin{cases} \lambda \mathrm{e}^{-\lambda \nabla_{12}} \left(1 - e^{-\lambda \nabla_{13}}\right), & \nabla_{13} > 0 \\ 0 & , \text{ Otherwise} \end{cases}$$

$$P_y^3 = e^{-\lambda \nabla_{12}} \left[e^{-\lambda \nabla_o} - 1\right] - \tfrac{e^{-\lambda \nabla_{32}}}{1+\nabla_{31}} \left[e^{-\lambda (1+\nabla_{31}) \nabla_o} - 1\right],$$

$$\text{where } B_y = \tfrac{(1-a_x)(\zeta_y^{th}-1)}{a_z},\ \nabla_{11} = \tfrac{d_{ze}^{\alpha}}{a_z \zeta_y^{th} \rho_z},\ \nabla_{12} = \tfrac{a_y d_{zy}^{\alpha}}{a_z \rho_z},$$

$$\nabla_{13} = \nabla_{11} - \tfrac{B_y d_{ze}^{\alpha}}{\rho_z \zeta_y^{th}},\ \nabla_{31} = \tfrac{\zeta_y^{th} d_{zy}^{\alpha}}{d_{ze}^{\alpha}}, \nabla_{32} = \tfrac{B_y d_{zy}^{\alpha}}{\rho_z} \text{ and } \Delta_o = \tfrac{\nabla_{12} - \nabla_{32}}{\nabla_{31}}.$$

3.2.3. User z

Finally, the value of P_z for user z is given by

$$\begin{aligned} P_z &= \Pr\{C_z \geq C_z^{th}\} = \Pr\{\frac{1+\gamma_{sz}^z}{1+\gamma_{sz}^e} \geq \zeta_z^{th}\} \\ &= 1 - \Pr\{|h_z|^2 < \Psi_1 |h_e|^2 + \Psi_2\} \\ &= 1 - \int_{m=0}^{\infty} F_{|h_z|^2}(\Psi_1 |h_e|^2 + \Psi_2) f_{|h_e|^2}(m) dm \\ &= 1 - \int_{m=0}^{\infty} \left[1 - \exp\{-\lambda(\Psi_1 m + \Psi_2)\}\right] \lambda e^{-\lambda m} dm \\ &= \frac{e^{-\lambda \Psi_2}}{1+\Psi_1}, \text{ where} \\ &\quad \Psi_1 = \frac{\zeta_z^{th} d_z^{\alpha}}{d_e^{\alpha}}, \Psi_2 = \frac{(\zeta_z^{th} - 1) d_z^{\alpha}}{\rho_b a_z} \text{ and } \zeta_z^{th} = 2^{2C_z^{th}}. \end{aligned}$$

3.3. Optimal Secure State 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_{sz}^z) and the eavesdropper (γ_{sz}^e), these are proportional to ρ_b in a straightforward manner. Therefore, following the principle of number theory, the better the value of ρ_b, the better its secrecy rate. On the other hand, for the weak users, their effective SINR (γ_x^x and γ_y^y) and that for the eavesdropper (γ_x^e and γ_y^e) are connected by the "min" function. As a result, this is not straightforward to find the values of ρ_b, ρ_z and ρ_y at which point the secrecy capacity of user x and user y achieve the maximal value (the point at which the corresponding SOP is minimal). Before applying the conventional convex optimization tools in order to obtain the optimal values of ρ_b, ρ_z and ρ_y, we would like to study the convexity property of the ESC for user x. Since the objective of this system is to maximize the ESC of user x (which is essentially a maximization problem), we require to transform it to a minimization problem by introducing a negative sign in front of $\bar{C}_x$. In order to prove that the negative value of ESC for user x (i.e., $-\bar{C}_x$) is convex, the corresponding Hessian matrix of $(-\bar{C}_x)$ has to be positive semi-definite. With the aim of finding the Hessian matrix, we

have

$$\frac{d\bar{C}_x}{d\rho_y} = \frac{1}{2\rho_y^2 \ln(2)} \sum_{b\in\{e,x\}} (-1)^b \left[\Theta_1^b e^{\Theta_2^b}\{\text{Ei}(-\Theta_2^b) - \text{Ei}(-\Theta_3^b)\} - e^{-\xi_{\hat{g}}^b} + 1\right], \text{ where}$$

$$\Theta_1^b = \frac{d_{yx}[1+\Pi_x(a_y+a_z)]}{a_y+a_z}, \Theta_2^b = \frac{1+\Pi_x(a_y+a_z)}{(a_y+a_z)\mu_{\hat{g}}^b} \text{ and } \Theta_3^b = \frac{a_{zy}+(a_{zx}+\Pi_x a_{zy})(a_y+a_z)}{(a_y+a_z)a_{zy}\mu_{\hat{g}}^b}.$$

$$\frac{d^2\bar{C}_x}{d{\rho_y}^2} = \frac{1}{2\ln(2)} \sum_{b\in\{e,x\}} (-1)^b - \frac{2}{\rho_y^3}\left[-\frac{\Theta_1^b}{\rho_y^2} e^{\Theta_2^b}\{\text{Ei}(-\Theta_2^b) - \text{Ei}(-\Theta_3^b)\} + e^{-\xi_{\hat{g}}^b} - 1\right]$$

$$+\frac{1}{\rho_y^2}\left[\Theta_1^b\left(\frac{\Theta_1^b}{\rho_y^2} e^{\Theta_2^b}\{\text{Ei}(-\Theta_2^b) - \text{Ei}(-\Theta_3^b)\} - e^{-\xi_{\hat{g}}^b} + 1\right) + \frac{\xi_{\hat{g}}^b}{\rho_y} e^{-\xi_{\hat{g}}^b}\right],$$

$$\frac{d\bar{C}_x}{d\rho_b} = 0, \ \frac{d\bar{C}_x}{d\rho_z} = 0, \text{ and } \frac{d^2\bar{C}_x}{d\rho_b d\rho_y} = 0.$$

Note that the value of $(-1)^b$ is 1 for $b = e$, and -1 for the other case. Using the aforementioned expressions, it is straightforward to construct the Hessian matrix of $(-\bar{C}_x)$. Since the resultant Hessian matrix is a function of complex term Ei(.), we approximate this by $\text{Ei}(-m) \approx E_c + \ln(m)$. Upon the approximation, we find that the Hessian matrix is neither positive semi-definite nor negative semi-definite, which implies that $(-\bar{C}_x)$ is not a convex function with respect to (w.r.t.) ρ_b, ρ_z and ρ_y. Still, we have tried another way to find the optimal values of ρ_b, ρ_z and ρ_y at which the instantaneous capacity (while taking average power gain of all links into account) of user x (i.e., C_x) achieves the maximal value. Intuitively, the values of ρ_b, ρ_z and ρ_y at which C_x achieves the maximal value is approximately equivalent to that at which $\tilde{C}_x$ has the maximal point, where $\tilde{C}_x$ is constructed by the average power gain of all links (i.e., $\overline{|h_x|^2}$, $\overline{|h_y|^2}$, $\overline{|h_z|^2}$ $\overline{|h_e|^2}$, $\overline{|\bar{g}_x|^2}$, $\overline{|\bar{g}_y|^2}$, $\overline{|\bar{g}_e|^2}$, $\overline{|\hat{g}_x|^2}$ and $\overline{|\hat{g}_e|^2}$). The corresponding optimization problem is provided in (6)-(13). For the sake of clarification, $\overline{|h_x|^2}$ is the average power gain of the link between the BS and the weak user x. Similar definition goes with the other links.

$$\underset{\rho_b,\rho_z,\rho_y,\chi_1,\chi_2,\chi_3,\chi_4}{\arg\min} \frac{1 + \frac{a_x\overline{|h_e|^2}}{a_y\overline{|h_e|^2}+a_z\overline{|h_e|^2}+d_e^\alpha/\rho_b} + \chi_2 + \chi_4}{1 + \frac{a_x\overline{|h_x|^2}}{a_y\overline{|h_x|^2}+a_z\overline{|h_x|^2}+d_x^\alpha/\rho_b} + \chi_1 + \chi_3} \tag{6}$$

$$\frac{a_x\overline{|h_y|^2}}{a_y\overline{|h_y|^2}+a_z\overline{|h_y|^2}+d_y^\alpha/\rho_b} \geq \chi_1, \ \frac{a_{zx}\overline{|\bar{g}_x|^2}}{a_{zy}\overline{|\bar{g}_x|^2}+d_{zx}^\alpha/\rho_z} \geq \chi_1 \tag{7}$$

$$\frac{a_x\overline{|h_y|^2}}{a_y\overline{|h_y|^2}+a_z\overline{|h_y|^2}+d_y^\alpha/\rho_b} \geq \chi_2, \ \frac{a_{zx}\overline{|\bar{g}_e|^2}}{a_{zy}\overline{|\bar{g}_e|^2}+d_{zx}^\alpha/\rho_z} \geq \chi_2 \tag{8}$$

$$\frac{a_{zx}\overline{|\bar{g}_y|^2}}{a_{zy}\overline{|\bar{g}_y|^2}+d_{zy}^\alpha/\rho_z} \geq \chi_3, \ \frac{\rho_y\overline{|\hat{g}_x|^2}}{d_{yx}^\alpha} \geq \chi_3 \tag{9}$$

$$\frac{a_{zx}\overline{|\bar{g}_y|^2}}{a_{zy}\overline{|\bar{g}_y|^2}+d_{zy}^\alpha/\rho_z} \geq \chi_4, \ \frac{\rho_y\overline{|\hat{g}_e|^2}}{d_{yx}^\alpha} \geq \chi_4 \tag{10}$$

$$0 \leq \rho_b \leq \rho_b^{max} \tag{11}$$

$$0 \leq \rho_z \leq \rho_z^{max} \tag{12}$$

$$0 \leq \rho_y \leq \rho_y^{max}, \tag{13}$$

where $\chi_1 = \min(\bar{\gamma}_{sx}^z, \bar{\gamma}_{zx}^x)$, $\chi_2 = \min(\bar{\gamma}_{sx}^z, \bar{\gamma}_{zx}^e)$, $\chi_3 = \min(\bar{\gamma}_{zx}^y, \bar{\gamma}_{yx}^x)$ and $\chi_4 = \min(\bar{\gamma}_{zx}^y, \bar{\gamma}_{yx}^e)$. $\bar{\gamma}_{sx}^z$, $\bar{\gamma}_{zx}^x$, $\bar{\gamma}_{zx}^e$, $\bar{\gamma}_{yx}^x$ and $\bar{\gamma}_{yx}^e$ are also constructed based on the average power gain of all links (i.e., $\overline{|h_x|^2}$, $\overline{|h_y|^2}$, $\overline{|h_z|^2}$ $\overline{|h_e|^2}$, $\overline{|\bar{g}_x|^2}$, $\overline{|\bar{g}_y|^2}$, $\overline{|\bar{g}_e|^2}$, $\overline{|\hat{g}_x|^2}$ and $\overline{|\hat{g}_e|^2}$). According to the definition of geometric programming (GP) [47, 48] technique,

the objective function in (6) is the ratio of two posynomials. Moreover, the constraints in (7), (8), (9) and (10) can also be written in terms of posynomial functions. Therefore, the entire problem in (6)-(13) can be mapped to a problem that is solvable via the GP-based heuristic methods. Consequently, we have adopted the GP-based single condensation method to solve this problem in order to obtain the optimal values of ρ_b, ρ_z and ρ_y.

3.4. Investigation of General Multi-Phase Cooperative NOMA Systems

In this section, we provide some possible insights about the performance of a general scenario, i.e., a cooperative NOMA system with N users. The node placement and the wireless communication channels are designed in such a way that the weakest user can be benefit from $N-1$ cooperative phases including the direct transmission one from the BS. We already have detailed investigation about the detailed wireless communications from the signal-level at the direct and cooperative transmission phases. Moreover, due to the scarcity of space, we only provide the resultant final SINR outcome of each user for the general scenario. Let denote all users in the system are indexed by $1, \cdots, N$, and the index of the BS is 0. We denote the channel gain associated with the small scale fading from node m to node n at phase s by H^s_{mn}. The transmitting node could be the BS or any user, and phase s is any cooperative phase or the first phase (i.e., the direct transmission from the BS). The lower and upper bounds of m are 0 and $N-1$, respectively, that for n are 1 and $m+1$, respectively, and that for s are 0 and $N-1$, respectively. For any phase s, no matter what the transmission node is, the order of $|H^s_{mn}|^2$ follow the $|H^s_{mN}|^2 \leq |H^s_{m(N-1)}|^2 \leq \cdots \leq |H^s_{m(m+2)}|^2 \leq |H^s_{m(m+1)}|^2$ trend. Correspondingly, for the sake of QoS constraint in NOMA-based communications, $A^s_{mN} \geq A^s_{m(N-1)} \geq \cdots \geq A^s_{m(m+2)} \geq A^s_{m(m+1)}$ should hold. $P_m,\ m = 0, 1, \cdots, N-1$ is the highest power level of node m. Similar to the description in Section 2, the noise level of all links are AWGN with zero mean and N_0 variance. For the sake of simplicity, we have $\rho_m = P_m/N_0,\ m = \{0, 1, \cdots, N-1\}$. Moreover, $D_{mn},\ m = \{0, 1, \cdots, N-1\},\ n = \{1, 2, \cdots, N\}$ is the distance between node m and node n. On the other hand, $D_{m(e)},\ m = \{0, 1, \cdots, N-1\}$ is the distance between node m and the eavesdropper. The final SINR of the users in the decreasing order of their index are listed as follows.

$$\gamma^N_N = \gamma^N_{(0)(N)} + \sum_{m=0}^{N-2} \min\left(\gamma^{m+1}_{mN}, \gamma^N_{(m+1)N}\right) + \min\left(\gamma^{N-1}_{(N-2)N}, \gamma^N_{(N-1)N}\right)$$

$$\gamma^{N-1}_{N-1} = \gamma^{N-1}_{(0)(N-1)} + \sum_{m=0}^{N-3} \min\left(\gamma^{m+1}_{m(N-1)}, \gamma^{N-1}_{(m+1)(N-1)}\right) + \min\left(\gamma^{N-2}_{(N-3)(N-1)}, \gamma^{N-1}_{(N-2)(N-1)}\right)$$

$$\vdots$$

$$\gamma^2_2 = \gamma^2_{(0)(2)} + \min\left(\gamma^1_{(0)(2)}, \gamma^2_{(1)(2)}\right)$$

$$\gamma^1_1 = \frac{\rho_0 A^1_{(0)(1)} |H^1_{(0)(1)}|^2}{D^\alpha_{(0)(1)}}.$$

On the other hand, from the perspective of the eavesdropper, the corresponding SINR of the users are listed as follows.

$$\gamma^e_N = \gamma^e_{(0)(N)} + \sum_{m=0}^{N-2} \min\left(\gamma^{m+1}_{mN}, \gamma^e_{(m+1)N}\right) + \min\left(\gamma^{N-1}_{(N-2)N}, \gamma^e_{(N-1)N}\right)$$

$$\gamma^e_{N-1} = \gamma^e_{(0)N-1} + \sum_{m=0}^{N-3} \min\left(\gamma^{m+1}_{m(N-1)}, \gamma^e_{(m+1)(N-1)}\right) + \min\left(\gamma^{N-2}_{(N-3)N}, \gamma^e_{(N-2)N}\right)$$

$$\vdots$$

$$\gamma^e_2 = \gamma^e_{(0)(2)} + \min\left(\gamma^1_{(0)(2)}, \gamma^e_{(1)(2)}\right)$$

$$\gamma^e_1 = \frac{\rho_0 A^1_{(0)(1)} |H^1_{(0)(e)}|^2}{D^\alpha_{(0)(e)}},$$

where

$$\gamma^N_{(0)(N)} = \frac{A^1_{(0)N} |H^1_{(0)N}|^2}{\sum_{n=1}^{N-1} A^1_{(0)n} |H^1_{(0)N}|^2 + \dfrac{D^\alpha_{(0)N}}{\rho_0}}$$

$$\gamma^{m+1}_{mN} = \frac{A^{m+1}_{mN} |H^{m+1}_{m(m+1)}|^2}{\sum_{n=1}^{N-2} A^{m+1}_{mn} |H^{m+1}_{m(m+1)}|^2 + \dfrac{D^\alpha_{m(m+1)}}{\rho_m}}$$

$$\gamma^N_{(m+1)N} = \frac{A^{m+2}_{(m+1)N} |H^{m+2}_{(m+1)N}|^2}{\sum_{n=1}^{N-2} A^{m+2}_{(m+1)n} |H^{m+2}_{(m+1)N}|^2 + \dfrac{D^\alpha_{(m+1)N}}{\rho_{m+1}}}$$

$$\gamma^N_{(N-1)N} = \frac{\rho_{N-1} A^N_{(N-1)(N)} |H^N_{(N-1)(N)}|^2}{D^\alpha_{(N-1)(N)}}$$

$$\gamma^{N-1}_{N-1} = \frac{A^1_{(0)(N-1)} |H^1_{(0)(N-1)}|^2}{\sum_{n=1}^{N-2} A^1_{(0)n} |H^1_{(0)(N-1)}|^2 + \dfrac{D^\alpha_{(0)(N-1)}}{\rho_0}}$$

$$\gamma^{m+1}_{m(N-1)} = \frac{A^{m+1}_{m(N-1)} |H^{m+1}_{m(m+1)}|^2}{\sum_{n=1}^{N-3} A^{m+1}_{mn} |H^{m+1}_{m(m+1)}|^2 + \dfrac{D^\alpha_{m(m+1)}}{\rho_m}}$$

$$\gamma^{N-1}_{(m+1)(N-1)} = \frac{A^{m+2}_{(m+1)(N-1)} |H^{m+2}_{(m+1)(N-1)}|^2}{\sum_{n=1}^{N-3} A^{m+2}_{(m+1)n} |H^{m+2}_{(m+1)(N-1)}|^2 + \dfrac{D^\alpha_{(m+1)(N-1)}}{\rho_{m+1}}}$$

$$\gamma^{N-1}_{(N-2)(N-1)} = \frac{\rho_{N-2} A^{N-1}_{(N-2)(N-1)} |H^{N-1}_{(N-2)(N-1)}|^2}{D^\alpha_{(N-2)(N-1)}}$$

$$\vdots$$

At the high SNR regime, we have

$$\gamma_N^N = \frac{A^1_{(0)N}}{\sum_{n=1}^{N-1} A^1_{(0)n}} + \sum_{m=0}^{N-2} \min\left(\frac{A^{m+1}_{mN}}{\sum_{n=1}^{N-2} A^{m+1}_{mn}}, \frac{A^{m+2}_{(m+1)N}}{\sum_{n=1}^{N-2} A^{m+2}_{(m+1)n}} \right)$$
$$+\min\left(\frac{A^{N-1}_{(N-2)N}}{A^{N-1}_{(N-2)(N-1)}}, \frac{\rho_{N-1} A^N_{(N-1)(N)} |H^N_{(N-1)(N)}|^2}{D^\alpha_{(N-1)(N)}} \right)$$

$$\gamma_{N-1}^{N-1} = \frac{A^1_{(0)(N-1)}}{\sum_{n=1}^{N-2} A^1_{(0)n}} + \sum_{m=0}^{N-3} \min\left(\frac{A^{m+1}_{m(N-1)}}{\sum_{n=1}^{N-3} A^{m+1}_{mn}}, \frac{A^{m+2}_{(m+1)(N-1)}}{\sum_{n=1}^{N-3} A^{m+2}_{(m+1)n}} \right)$$
$$+\min\left(\frac{A^{N-2}_{(N-3)(N-1)}}{A^{N-2}_{(N-3)(N-2)}}, \frac{\rho_{N-2} A^{N-1}_{(N-2)(N-1)} |H^{N-1}_{(N-2)(N-1)}|^2}{D^\alpha_{(N-2)(N-1)}} \right)$$

$$\vdots$$

$$\gamma_2^2 = \frac{A^1_{(0)(2)}}{A^1_{(0)(1)}} + \min\left(\frac{A^1_{(0)(2)}}{A^1_{(0)(1)}}, \frac{\rho_1 A^2_{(1)(2)} |H^2_{(1)(2)}|^2}{D^\alpha_{(1)(2)}} \right).$$

In the similar manner, we can derive γ_N^e, γ_{N-1}^e, $\cdots$ and γ_2^e at the high SNR regime. Following the derivation in Section 3.1, the ESC of the weakest user is written as

$$\bar{C}_N \cong \frac{1}{2\ln(2)} (-1)^b \sum_{b \in N,e} (-1)^b \exp\left(\frac{1 + \Pi_N \sum_{n=1}^{N-1} A^1_{(0)n}}{\sum_{n=1}^{N-1} A^1_{(0)n} \mu^b_{H^N_{(N-1)N}}} \right)$$
$$\left[\mathrm{Ei}\left(-\frac{1+\Pi_N \sum_{n=1}^{N-1} A^1_{(0)n}}{\sum_{n=1}^{N-1} A^1_{(0)n} \mu^b_{H^N_{(N-1)N}}} \right) - \mathrm{Ei}\left(-\frac{A^{N-1}_{(N-2)(N-1)} + A^{N-1}_{(N-2)(N)} + \Pi_N A^{N-1}_{(N-2)(N-1)}) \sum_{n=1}^{N-1} A^1_{(0)n}}{\sum_{n=1}^{N-1} A^1_{(0)n} A^{N-1}_{(N-2)(N-1)} \mu^b_{H^N_{(N-1)N}}} \right) \right],$$

where

$$\mu^b_{H^N_{(N-1)N}} = \frac{\rho_{N-1}}{D^\alpha_{(N-1)b}}, \ \Pi_N = \sum_{m=0}^{N-2} \min\left(\frac{A^{m+1}_{mN}}{\sum_{n=1}^{N-2} A^{m+1}_{mn}}, \frac{A^{m+2}_{(m+1)N}}{\sum_{n=1}^{N-2} A^{m+2}_{(m+1)n}} \right) \text{ and } b \in \{N, e\}.$$

Note that the value of $(-1)^b$ is 1 for $b = e$ and -1 for the other case. Thus, we see that the ESC of the weak user with index N is a function of the transmit SNR of the last cooperative user (i.e., ρ_{N-1}) at the last cooperative phase from which it receives signal, and the distance between the last transmitting user (at the last cooperative phase) and itself. Moreover, the ESC of this user is independent of the transmit SNR of the other cooperative users in other cooperative phases and the transmit SNR of the BS as well, but the function of power allocation factors of all the cooperative and direct transmission phases from which it receives signal. Under the deployment of users discussed in this section, following the analytical methodology in Section 3.2, we can derive the SOP of the weakest user with index N, which is a function of the transmit SNR of the last cooperative user (i.e., ρ_{N-1}) at the last cooperative phase from which it receives signal and the distance

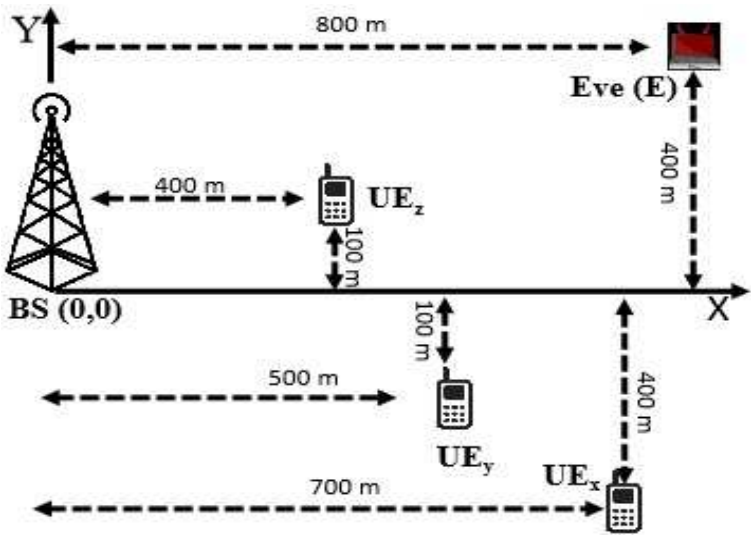


Figure 2: A sample simulation scenario for a three-phase cooperative NOMA system under the presence of an eavesdropper.

between the last transmitting user (at the last cooperative phase) and itself. In the similar manner, we can conclude the closed form expressions of the ESC and SOP for all the other weak users in the system. The ESC and SOP of the strongest user are the functions of the BS transmit SNR (i.e., ρ_b) and the distance between the BS and itself (i.e., $D_{(0)1}$).

4. Performance Evaluation

In this section, via simulation, we evaluate evaluate the correctness of the proposed analytical schemes under different settings. Followed by the methodology, we exhibit the detailed outcome of the simulation in order to verify the effectiveness of the proposed schemes.

4.1. Simulation Settings

As of the setup, the model of the system is as same as that in Section 2. The pico BS is at the center of the cell, there are an eavesdropper and two legitimate users in the system. The strongest and weaker users stay on the straight lines which are parallel to the X-axis, however the line that holds the strongest user is slightly upward of the X-axis, and the line that holds the weaker user is slightly downward of the X-axis. Moreover, the weaker user is farther away from the BS compared to the strongest user. The weakest user is on the line that makes -30° with the X-axis. Finally, while listening to these three users, the eavesdropper stays on the straight line that makes 26° angle with the X-axis. To summarize, the exact coordinates of all the nodes in the system are shown in Fig. 2. Unless otherwise specified, we assume $a_z = 0.4$, $a_x = a_y = 0.3$, $a_{zx} = 0.6$ and $a_{zy} = 0.4$. Moreover, 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 3. The simulations are conducted over 10000 independent channel realizations for each data point.

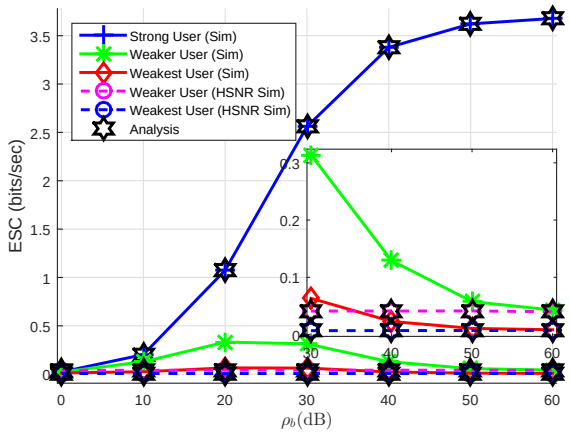


Figure 3: Comparison of ESC with the increasing BS transmit SNR (ρ_b), where $\rho_z = \rho_y = 0$ dB.

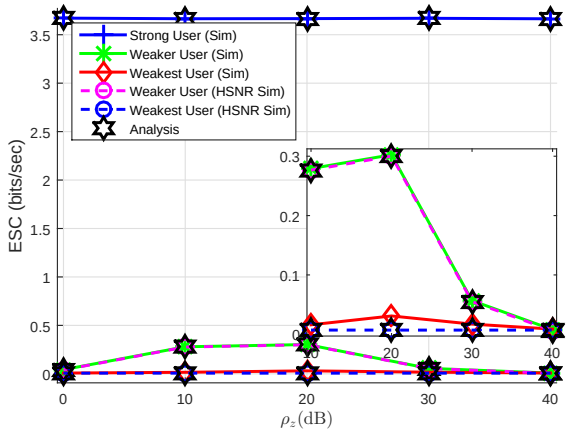


Figure 4: Comparison of ESC with the increasing strong user transmit SNR (ρ_z), where $\rho_b = 60$ dB and $\rho_y = 0$ dB.

4.2. Simulation Results

We first exhibit the results in the context of ESC, and then that related to the SOP under different settings.

4.2.1. The Evaluation of ESC

In Figure 3, we present the ESC of each individual user with the increasing value of ρ_b. The increasing value of ρ_b implies the increasing value of SNR. As presented in Section 2, the effective SINR of both the users as well as the eavesdropper are positively proportional to ρ_b. Therefore, the effective SINR of all the nodes are increased with the increasing ρ_b. In such circumstances, although the definition of secrecy capacity (presented in Section 2.4) produces confusion on whether it will increase or decrease with the increasing ρ_b, the principle of the number theory affirms that the secrecy capacity should increase with the increasing ρ_b. As a result, given that the eavesdropper is relatively far away, the ESC for the strongest user follows the increasing trend as both the effective SINR (at both the user and the eavesdropper sides) are positively proportional to the increasing ρ_b. On the other hand, as discussed in Section 3.3, due to the "min"

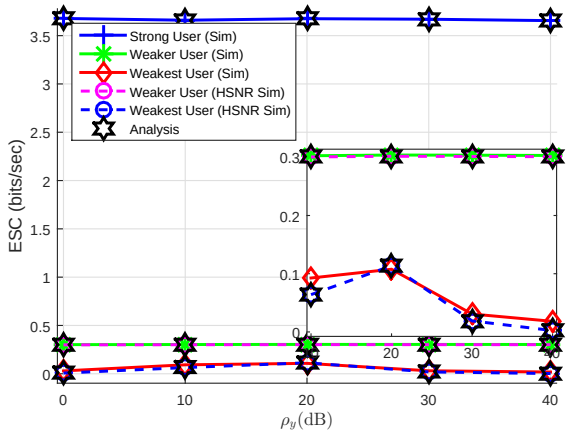
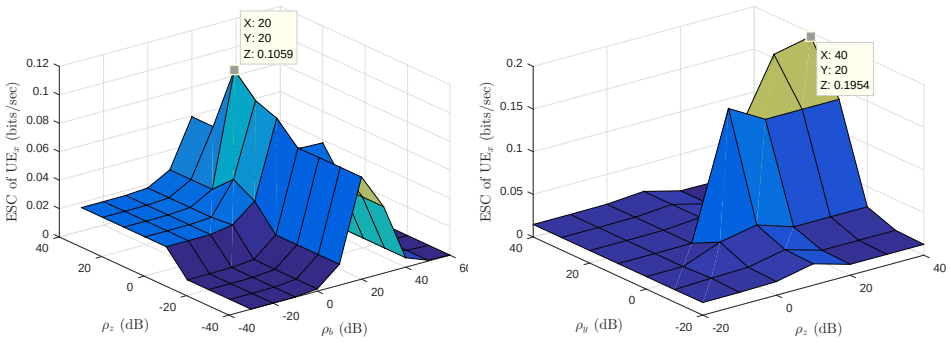


Figure 5: Comparison of ESC with the increasing weaker user transmit SNR (ρ_y), where $\rho_b = 60$ dB and $\rho_z = 20$ dB.

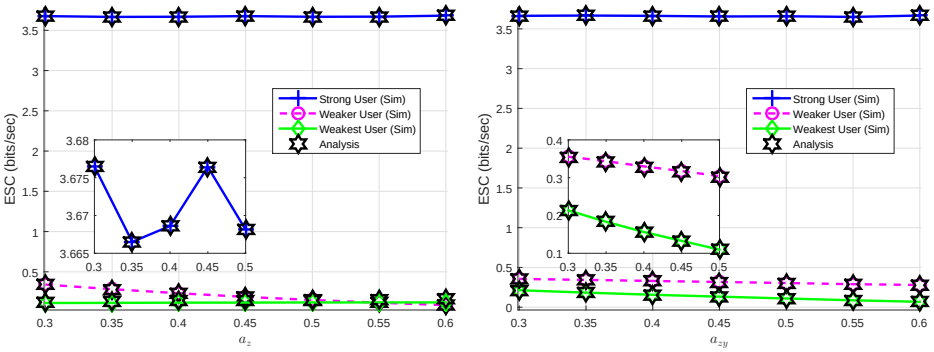
function in the SINR expression of the weaker users and the eavesdropper, the resultant ESC does not have a straightforward trend w.r.t. ρ_b. Rather, the ESC for this case has a concave trend with the increasing ρ_b. The optimal point in the simulation is consistent with the optimal outcome (i.e., $\rho_b = 0$ dB) obtained from the solution of the problem in (6)-(13) while keeping the values of ρ_z and ρ_y constant. These results verify the effectiveness of the proposed solution technique in the context of obtaining optimal ρ_b at which the ESC for the weakest user has the maximal value. Moreover, the derived analytical expressions for the weak users are valid only at the high SNR regime, and hence we see that the analytical results just match with the simulation ones at around ≥ 50 dB. On the other hand, regarding the correctness of our analytical results at the high SNR regime, we plot the results of the simulation that is conducted in the high SNR regime as well. Since the analytical derivation of the strongest user is exact (no matter the value of ρ_b is), it matches with the exact simulation results. In the following subsequent results, we set ρ_b to 60 dB, as the analytical derivation of the weak users are based on the assumption that the value of ρ_b is very high (around 60 dB). The system ESC is the sum ESC of the individuals users, and we skip this outcome in this plot due to the sake of clarity.

In Figure 4 and Figure 5, we present the ESC with the increasing value of ρ_z (i.e., the transmit SNR of the strong user) and ρ_y (i.e., the transmit SNR of the weaker user), respectively. Since the instantaneous secrecy rate as well as the ESC of the strong user is independent of ρ_z and ρ_y, this remains constant under the varying ρ_z and ρ_y in these two figures. On the other hand, we see the interesting concave trend for both the weak users in Figure 4, and that for only the weakest user in Figure 5. This is due to the "min" function in the effective SINR expressions of both the weak users and the eavesdropper. For example, at the lower value of ρ_z, the effective SINR of UE_y and the eavesdropper are dominated by the second parameter (which is a proportional function of ρ_z) of the "min" function. Consequently, at a lower value of ρ_z, the ESC has an increasing trend. However, at a higher value of ρ_z, the effective SINR is dominated by the first parameter of the "min" function which is equal for both the weaker user and the eavesdropper. Consequently, the ESC of the weaker user is reduced due to the equality nature of the second parameter between this user and the



(a) ρ_b vs. ρ_z (b) ρ_z vs. ρ_y

Figure 6: The ergodic secrecy capacity of the weakest user (i.e., UE$_x$) under the varying ρ_b, ρ_z and ρ_y.



(a) ESC vs. a_z (b) ESC vs. a_{zy}

Figure 7: Comparison of ESC with the increasing strong user power allocation factor (a_z) (first phase) and weaker user power allocation factor (a_{zy}) (second phase), where $\rho_b = 60$ dB and $\rho_z = \rho_y = 40$ dB.

eavesdropper. For the similar reason, we see such a concave trend for the weakest user both in Figure 4 and Figure 5. In Figure 5, the ESC of the weaker user remains constant with the increasing ρ_y as the ESC expression is independent of ρ_y in this case. On the other hand, in Figure 6, we compare the simulation outcome of UE$_x$ with the optimal point obtained from our proposed solution technique shown in Section 3.3 for different values of ρ_b, ρ_z and ρ_y. Interestingly, the optimal outcome of the joint optimization ($\rho_b = 20$ dB and $\rho_b = 20$ dB) match with that of the individual optimization results presented in Figure 4 and Figure 5.

In Figure 7a, we present the ESC of each individual user with the increasing strong user power allocation factor a_z. Apparently, one can argue that the ESC of the strong user should be increasing in this case as the SINR expressions of both this user and the eavesdropper are positively proportional to a_z. However, due to the definition of ESC (which is a function of log function) and the small changing range of a_z, we see such a non-convex trend for the ESC of the strong user in Figure 7a. On the other hand, increasing a_z implies decreasing value of a_x and a_y as $a_x + a_y + a_z = 1$ holds. Moreover, the ESC of UE$_y$ and UE$_z$ are positively proportional to a_y and a_z, respectively. Therefore, intuitively, the ESC of both the users should

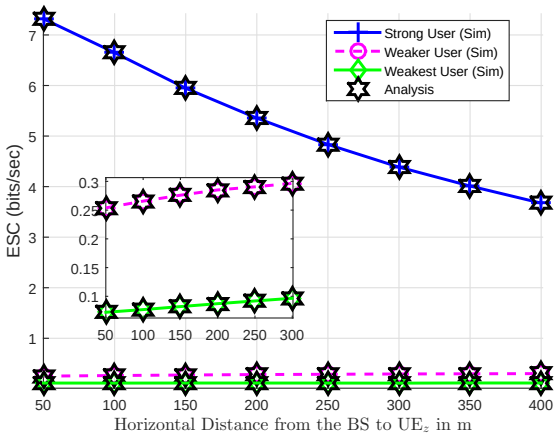


Figure 8: Comparison of ESC with the increasing strong user horizontal distance from the BS, where $\rho_b = 60$ dB and $\rho_z = \rho_y = 40$ dB.

be decreasing with the increasing a_z, and so thus we observe in this figure. In fact, when the value of a_z is close to 0.4, the weakest user outperforms the weaker user. This is due to the fact that the weakest user is further benefit from the third transmission phase. To see the effect of the power allocation factor at the second transmission phase (i.e., cooperative phase II), we plot Figure 7b. Since the performance of the strong user is independent of the subsequent cooperative phases, the ESC of this user remains constant with the increasing a_{zy}. On the other hand, we see the decreasing trend for the weakest user as the ESC for this user is negatively proportional to the value of a_{zy}. Although the performance of the weaker user is positively proportional to the value of a_{zy}, due to the "min" function in the SINR expression of this user, the first term (which is independent of a_{zy}) of the min operator becomes its effective SINR. On the other hand, the effective SINR of the far-away eavesdropper remains the second term of the "min" operator, which is increasing with the increasing a_{zy}. As a result, the ESC of the weaker user is slightly decreasing with the increasing a_{zy}. Intuitively, due to the "min" function in the ESC expression, based on the position of the eavesdropper, it is possible that the performance of the weaker user could have a concave trend with the increasing a_{zy}, and so thus we observe in this figure.

In Figure 8, we plot the ESC of each individual user with the increasing horizontal distance of the strong user from the BS. The increasing horizontal distance of this user from the BS implies the increasing d_z. The effective SINR of the strong user is inversely proportional to its distance from the BS (i.e., d_z), and hence the corresponding ESC has a decreasing trend with the increasing d_z. On the other hand, the weak users in the system receive information from both the BS and the strong user in two phases. In the first phase, when it receives information from the BS, the corresponding effective SINR of the weak user is independent of d_z. However, in the second phase, with the increasing value of d_z, the distance between the strong user and the weak users decrease. Therefore, at this stage, their effective SINR are inversely proportional to their distance towards the strong user. As a result, the ESC of the weak users increase with the increasing value of d_z.

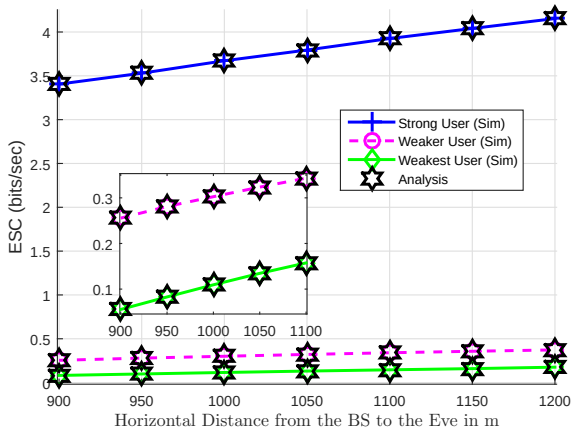


Figure 9: Comparison of ESC with the increasing eavesdropper horizontal distance from the BS, where $\rho_b = 60$ dB and $\rho_z = \rho_y = 40$ dB.

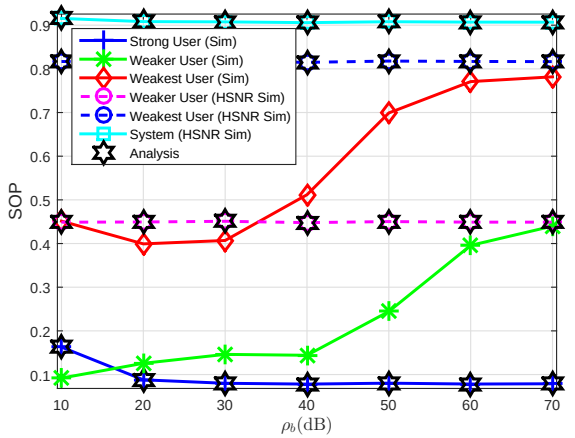


Figure 10: Comparison of SOP with the increasing BS transmit SNR (ρ_b), where $\rho_z = \rho_y = 0$ dB.

The system setup of Figure 9 is made in such a way that the eavesdropper remains on a line which makes 26^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 as well as the strong and weaker users. The effective SINR of all the users at the first transmission phase are positively proportional to the distance between the eavesdropper and the BS. Moreover, at the subsequent cooperative transmission phases, the effective SINR of the weak users are positively proportional to the distance between the eavesdropper and the strong user and that between the two weak users, respectively. Since the strong user and the weaker user always remain fixed in their positions, as the eavesdropper goes far away, their distance from the eavesdropper increase. As a result, we see that the ESC of all the users increase with the increasing horizontal distance of the eavesdropper.

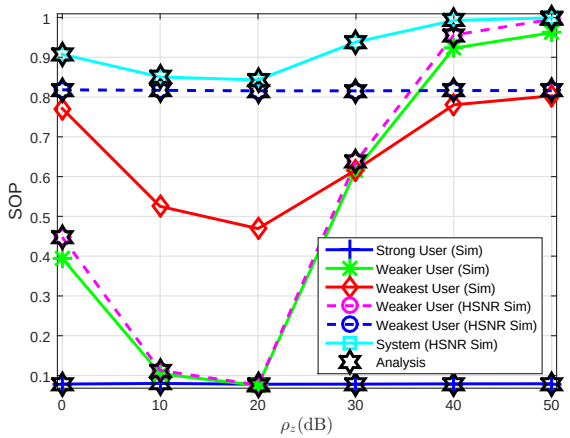


Figure 11: Comparison of SOP with the increasing strong user transmit SNR (ρ_z), where $\rho_b = 60$ dB and $\rho_y = 0$ dB.

4.2.2. The Evaluation of SOP

In Figure 10, we plot the SOP of each individual user as well as the system with the increasing value of ρ_b. As we saw in Figure 3, the ESC of both the users is a function of ρ_b. For the strong user case, we saw that the ESC is the increasing function of ρ_b. On the other hand, from the definition of SOP, the higher the ESC level, it is less likely that the ESC drops below some predefined threshold. Moreover, the relationship between the ESC and the SOP of any of the users is inversely proportional in a linear manner. Therefore, for UE_z, the SOP is a decreasing function of ρ_b, which is just the opposite trend of that in Figure 3. For the weak users, in Figure 3, we saw that their ESC are the concave function of ρ_b. Therefore, the SOP of these users should be a convex function of ρ_b, and this is what exactly observed in this figure. Interestingly, the point at which (ρ_b) the ESC of UE_x and UE_y is maximal, is the point at which the corresponding SOP is minimal. Similar to the ESC, the SOP is also approximated at the high SNR regime. Therefore, we see that the analytical results just match with the simulation ones at around ≥ 50 dB for both the weak users. Regarding the correctness of our analytical results at the high SNR regime, we plot the results of the simulation that is conducted at the 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 compared to that of either of the users and its analytical results just match with the simulation ones at the high SNR regime. Since the analytical derivation of the weak users 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 Figure 11 and Figure 12, we show the SOP of each individual user as well as the system with the increasing value of ρ_z (i.e., the transmit SNR of the strong user) and ρ_y (i.e., the transmit SNR of the weaker user), respectively. As we saw in Figure 4 and Figure 5, the ESC of the strong user is independent of ρ_z and ρ_y, this remains constant no matter the values of ρ_z and ρ_y are. As a result, the SOP of this user should remain constant with the increasing ρ_z and ρ_y, which is exactly observed in Figure 11 and Figure 12. On

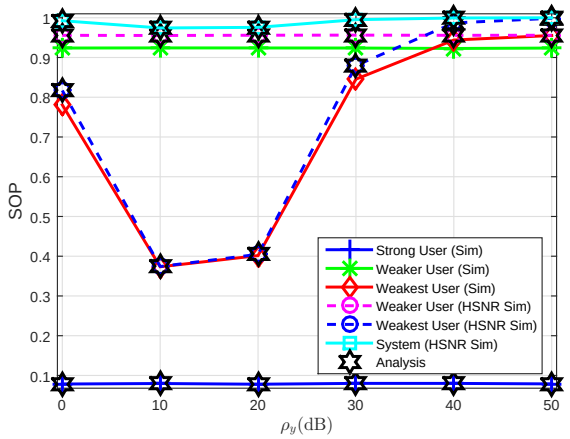


Figure 12: Comparison of SOP with the increasing weaker user transmit SNR (ρ_y), where $\rho_b = 60$ dB and $\rho_z = 40$ dB.

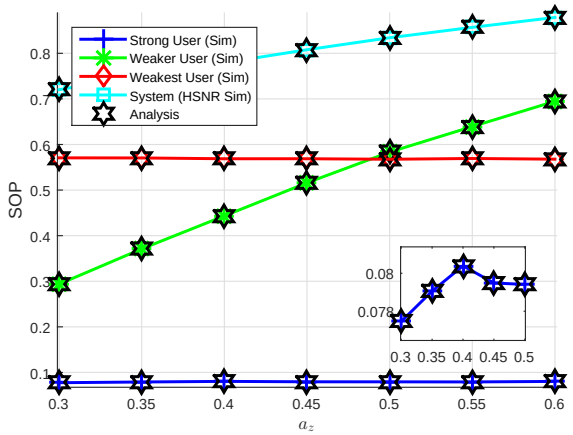


Figure 13: Comparison of SOP with the increasing strong user power allocation factor (a_z) (first phase), where $\rho_b = 60$ and $\rho_z = \rho_y = 40$ dB.

the other hand, we see the interesting convex trend for both the weak users in the former figure and only for the weakest user in the latter figure. This is due to the fact that the ESC of these user are the concave functions of ρ_z and ρ_y, which were shown in Figure 4 and Figure 5, respectively. Similar to the relationship between the ESC/SOP of the weak users and ρ_b, the point ($\rho_z = 20$ dB) at which the ESC is maximal, it is the same point at which the SOP is minimal. Since the SOP of the strong user is constant, the trend of the system SOP is dominated by that of the weak users.

In order to show the variation of the SOP with different power allocation factors among the strong and weak users at the first transmission phase, we plot Figure 13. The increasing value of a_z means the decreasing value of a_x and a_y ($a_x + a_y + a_z = 1$), and the ESC of both the users are a function of a_x and a_y, respectively. As we saw in Figure 7a, the ESC of the weak users are the decreasing function of a_z, and that of the strong user is a non-convex function of a_z. Therefore, to hold the truth about the relationship between the ESC and SOP, the SOP of the weak users are the increasing functions of a_z and that of the strong user is the

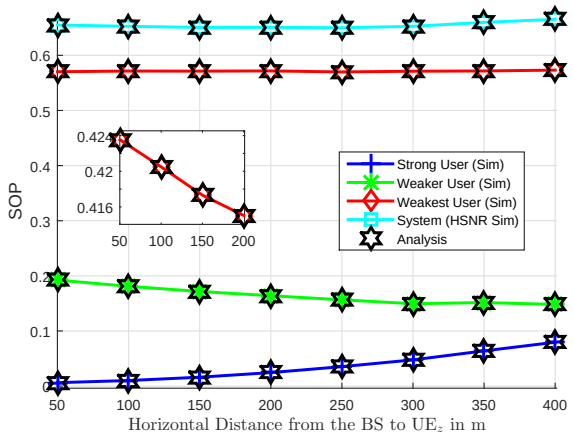


Figure 14: Comparison of SOP with the increasing strong user horizontal distance from the BS, where $\rho_b = 60$ and $\rho_z = \rho_y = 40$ dB.

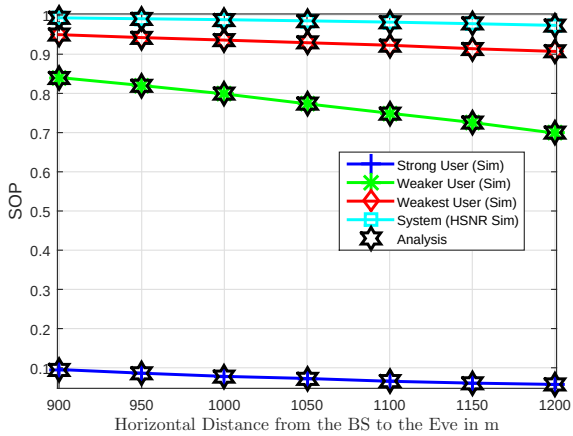


Figure 15: Comparison of SOP with the increasing eavesdropper horizontal distance from the BS, where $\rho_b = 60$ and $\rho_z = \rho_y = 40$ dB.

non-convex function of a_z, as shown in Figure 13. In this figure, we see that the increasing trend of the weakest user is not that much obvious. This is due to the fact that the effective SINR of this user is mostly dominated by the SINR obtained from the subsequent cooperative phases rather than the first transmission phase. As a result, with the increasing a_z, the ESC as well as the SOP of this user is not that much visibly varying. On the other hand, since the change of SOP for the strong and the weakest users are not that much obvious with the increasing value of a_z, the system SOP has the same trend as that of the weaker user.

In Figure 14, we plot the SOP of each individual user as well as the system with the increasing horizontal distance of the strong user from the BS. As we saw in Figure 8, the ESC 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_z. On the other hand, since both the weak users receive information from the strong user at the second transmission phase, the ESC of these users become better as the strong user gets closer to the weak users with the increasing d_z. As a result, the SOP of the weak users get better (i.e., decreasing) with the increasing d_z. Although the SOP of the strong user is increasing, the system SOP is decreasing.

This is due to the fact that the SOP of the weak users are much higher compared to that of the strong user which is decreasing with the increasing d_z. Basically, the system SOP is mostly dominated by that of the weak users although the decreasing rate is not exactly same to that of the weak users. This is due to the fact that the SOP of the strong user is increasing with the increasing d_z.

The system setup of Figure 15 is as same as that of Figure 9. Similar to the previous figure, in this figure, we present the results in the context of SOP with the horizontal distance of the eavesdropper from the BS (i.e., $d_e\sin(26^\circ)$). As we saw in Figure 9, the ESC of all the users are decreasing with the increasing horizontal distance of the eavesdropper from the BS. As a result, we see the decreasing trend of the SOP for all the users with the increasing $d_e\sin(26^\circ)$. Consequently, the system SOP follows the same trend as that of all the users, but obviously has higher value compared to any of the users.

5. Conclusion

Being motivated by the inherent cooperative feature of NOMA systems, we studied the PLS of a three-user system in which the strong users act as the relay for the other weaker users. Given the assumption that there is a passive eavesdropper in the system, we derived the closed form expressions of the ESC and SOP for all the users in the system. Since the exact derivation of the ESC and SOP for the weak users are intractable, we derived these metrics at the high SNR regime while keeping the exactness for the strongest user. Based on the analytical methodology of the three-user cooperative system, we provided insightful observations on the ESC and SOP of a general multi-phase cooperative NOMA system at the high SNR regime. Extensive numerical simulations were conducted to verify the correctness of the analytical derivations as well as to find the optimal setup at 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 scheme at the BS and the stronger users in the system.

References

[1] Y. Saito, A. Benjebbour, Y. Kishiyama, T. Nakamura, System-Level Performance Evaluation of Downlink Non-orthogonal Multiple Access (NOMA), in: Proc. IEEE PIMRC, pp. 611–615.

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

[3] D. Wan, M. Wen, F. Ji, H. Yu, F. Chen, On the Achievable Sum-Rate of NOMA-Based Diamond Relay Networks, IEEE Trans. Veh. Technol. 68 (2019) 1472–1486.

[4] Y. Li, X. Chu, Y. Ye, H. Zhang, Performance Analysis of Relay Selection in Cooperative NOMA Networks, IEEE Commun. Lett. 23 (2019) 760–763.

[5] Z. Ding, M. Peng, H. V. Poor, Cooperative Non-Orthogonal Multiple Access in 5G Systems, IEEE Commun. Lett. 19 (2015) 1462–1465.

[6] X. Lai, Q. Zhang, J. Qin, Cooperative NOMA Short-Packet Communications in Flat Rayleigh Fading Channels, IEEE Trans. Veh. Technol. (2019) 1–1.

[7] O. Abbasi, A. Ebrahimi, N. Mokari, NOMA Inspired Cooperative Relaying System Using an AF Relay, IEEE Wirel. Commun. Lett. 8 (2019) 261–264.

[8] M. F. Kader, M. B. Uddin, S. R. Islam, S. Y. Shin, Capacity and outage analysis of a dual-hop decode-and-forward relay-aided NOMA scheme, Digital Signal Processing 88 (2019) 138 – 148.

[9] Z. Yu, C. Zhai, W. Ni, D. Wang, Non-Orthogonal Multiple Access With Cooperative Truncated ARQ and Relay Selection, IEEE Access 7 (2019) 56228–56243.

[10] S. Wang, T. Wu, Stochastic geometric performance analyses for the cooperative NOMA with the full-duplex energy harvesting relaying, IEEE Trans. Veh. Technol. (2019) 1–1.

[11] Y. Liu, Z. Ding, M. Elkashlan, H. V. Poor, Cooperative Non-orthogonal Multiple Access With Simultaneous Wireless Information and Power Transfer, IEEE J. Sel. A. Commun. 34 (2016) 938–953.

[12] Y. Chen, L. Wang, B. Jiao, Cooperative multicast non-orthogonal multiple access in cognitive radio, in: Proc. IEEE ICC, pp. 1–6.

[13] N. Guo, J. Ge, Q. Bu, C. Zhang, Multi-User Cooperative Non-Orthogonal Multiple Access Scheme With Hybrid Full/Half-Duplex User-Assisted Relaying, IEEE Access 7 (2019) 39207–39226.

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

[15] Q. Li, M. Wen, E. Basar, H. V. Poor, F. Chen, Spatial Modulation-Aided Cooperative NOMA: Performance Analysis and Comparative Study, IEEE J. Sel. T. Signal Process. (2019) 1–1.

[16] A. D. Wyner, The wire-tap channel, The Bell System Technical Journal 54 (1975) 1355–1387.

[17] H. Lei, Z. Yang, K. Park, I. S. Ansari, Y. Guo, G. Pan, M. Alouini, Secrecy Outage Analysis for Cooperative NOMA Systems with Relay Selection Scheme, CoRR abs/1811.03220 (2018).

[18] Z. Ding, Z. Zhao, M. Peng, H. V. Poor, On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming, IEEE Trans. Commun. 65 (2017) 3151–3163.

[19] B. Zheng, M. Wen, C. Wang, X. Wang, F. Chen, J. Tang, F. Ji, Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex, IEEE J. Sel. A. Commun. 36 (2018) 1426–1440.

[20] K. Jiang, T. Jing, Y. Huo, F. Zhang, Z. Li, SIC-Based Secrecy Performance in Uplink NOMA Multi-Eavesdropper Wiretap Channels, IEEE Access 6 (2018) 19664–19680.

[21] Y. Feng, S. Yan, Z. Yang, Secure Transmission to the Strong User in Non-Orthogonal Multiple Access, IEEE Commun. Lett. 22 (2018) 2623–2626.

[22] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, R. Q. Hu, Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks, IEEE Trans. Commun. 67 (2019) 83–96.

[23] Z. Xiang, W. Yang, G. Pan, Y. Cai, Y. Song, Physical Layer Security in Cognitive Radio Inspired NOMA Network, IEEE J. Sel. T. Signal Process. (2019) 1–1.

[24] J. Chen, L. Yang, M. S. Alouini, Physical Layer Security for Cooperative NOMA Systems, IEEE Trans. Veh. Technol. PP (2018) 1–1.

[25] B. M. ElHalawany, A. A. A. El-Banna, K. Wu, Physical-layer security and privacy for vehicle-to-everything, IEEE Communications Magazine 57 (2019) 84–90.

[26] G. Satrya, S. Shin, Enhancing security of SIC algorithm on non-orthogonal multiple access (NOMA) based systems, Phy. Commun. 33 (2019) 16 – 25.

[27] N. Nandan, S. Majhi, H. Wu, Secure Beamforming for MIMO-NOMA-Based Cognitive Radio Network, IEEE Commun. Lett. 22 (2018) 1708–1711.

[28] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, L. Hanzo, Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT, IEEE J. Sel. A. Commun. 36 (2018) 918–931.

[29] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis, V. C. M. Leung, Secure Communications in NOMA System: Subcarrier Assignment and Power Allocation, CoRR abs/1801.04441 (2018).

[30] X. Tang, P. Ren, Y. Wang, Z. Han, Combating Full-Duplex Active Eavesdropper: A Hierarchical Game Perspective, IEEE Trans. Commun. 65 (2017) 1379–1395.

[31] N. Zhao, W. Wang, J. Wang, Y. Chen, Y. Lin, Z. Ding, N. C. Beaulieu, Joint Beamforming and Jamming Optimization for Secure Transmission in MISO-NOMA Networks, IEEE Trans. Commun. 67 (2019) 2294–2305.

[32] M. Zeng, P. Nguyen, O. Dobre, H. V. Poor, Securing Downlink Massive MIMO NOMA Networks with Artificial Noise, IEEE J. Sel. T. Signal Process. (2019) 1–1.

[33] Y. Li, M. Jiang, Q. Zhang, Q. Li, J. Qin, Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems, IEEE Trans. Veh. Tech. 66 (2017) 7563–7567.

[34] H. Wang, X. Zhang, Q. Yang, T. Tsiftsis, Secure Users Oriented Downlink MISO NOMA, IEEE J. Sel. T. Signal Process. (2019) 1–1.

[35] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, L. Hanzo, Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks, IEEE Trans. Wirel. Commun. 16 (2017) 1656–1672.

[36] B. He, A. Liu, N. J. Yang, V. K. N. Lau, On the Design of Secure Non-Orthogonal Multiple Access Systems, CoRR abs/1612.06961 (2016).

[37] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, R. Jia, Exploiting Inter-User Interference for Secure Massive Non-Orthogonal Multiple Access, IEEE J. Sel. A. Commun. 36 (2018) 788–801.

[38] J. Tang, L. Jiao, N. Wang, P. Wang, K. Zeng, H. Wen, Mobility Improves NOMA Physical Layer Security, in: Proc. IEEE GLOBECOM, pp. 1–6.

[39] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, M. Alouini, Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay, IEEE Trans. Commun. (2019) 1–1.

[40] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, P. Zhang, Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming, IEEE Trans. Veh. Technol. 68 (2019) 2682–2696.

[41] B. M. ElHalawany, R. Ruby, T. Riihonen, K. Wu, Performance of Cooperative NOMA Systems under Passive Eavesdropping, in: Proc. IEEE GLOBECOM, pp. 1–6.

[42] M. K. Ozdemir, H. Arslan, Channel Estimation for Wireless OFDM Systems, IEEE Commun. Surveys Tutorials 9 (2007) 18–48.

[43] Y. Tan, J. Zhou, J. Qin, Novel Channel Estimation for Non-orthogonal Multiple Access Systems, IEEE Signal Processing Lett. 23 (2016) 1781–1785.

[44] B. M. ElHalawany, K. Wu, Physical-layer security of noma systems under untrusted users, in: Proc. IEEE GLOBECOM, pp. 1–6.

[45] D. Tse, P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press (2005).

[46] D. Deng, X. Li, L. Fan, W. Zhou, R. Q. Hu, Z. Zhou, Secrecy Analysis of Multiuser Untrusted Amplify-and-Forward Relay Networks, Wireless Communications and Mobile Computing 17 (2017) 1–11.

[47] S. Boyd, S.-J. Kim, L. Vandenberghe, A. Hassibi, A tutorial on geometric programming, Optimization and Engineering 8 (2007) 67.

[48] M. Chiang, Geometric Programming for Communication Systems, Commun. Inf. Theory 2 (2005) 1–154.