Secrecy Outage Probability and Fairness of Packet Transmission Time in a NOMA System

TUNG PHAM HUU¹,⁵, TAM NINH THI-THANH², CHI NGUYEN-YEN³, HUNG TRAN⁴, VIET NGUYEN DINH⁵, (Member, IEEE), AND VAN NHAN VO⁶
¹Faculty of Information Technology, National University of Civil Engineering, Hanoi 11616, Vietnam
²National Academy of Education Management, Hanoi 11412, Vietnam
³Faculty of Information Technology, University of Transport and Communications, Hanoi 11512, Vietnam
⁴Faculty of Information Technology, Phenikaa University, Hanoi 12116, Vietnam
⁵Faculty of Information Technology, VNU University of Engineering and Technology, Hanoi 11309, Vietnam
⁶International School, Duy Tan University, Danang 550000, Vietnam
Corresponding author: Hung Tran (hung.tran@phenikaa-uni.edu.vn)

ABSTRACT In this paper, we analyze the secrecy outage probability (SOP) and the fairness of average packet transmission time for a non-orthogonal multiple access (NOMA) system which consists of a base station (BS) and two legal NOMA users in the presence of an eavesdropper (Eve). In order to extract the superimposed signal, the Eve is considered in two modes, i.e., successive interference cancellation (SIC) mode and parallel interference cancellation (PIC) mode. Accordingly, we analyze the secrecy performance of the considered system by deriving a new exact expression for SOP. Furthermore, the optimal power allocation between two legal users is determined such that the average transmission time from BS to two legitimate users are approximately equal to achieve the fairness of average packet transmission time. Monte Carlo simulations are provided to verify our analytical results.

INDEX TERMS NOMA, secrecy outage probability, packet timeout probability, fairness of average transmission time.

I. INTRODUCTION
Radio frequency is one of the most important resources in wireless communication. However, it has been exhausted due to outburst demands of wireless services. This problem becomes more serious as the era of Internet of things (IoT) is coming, in which massive wireless devices want to have connections to exchange information. To overcome the problem of massive connections and shortage of spectrum, NOMA has been proposed as a promising technique in the fifth generation (5G) networks due to its superior spectral efficiency [1], [2].

Furthermore, multiple users in NOMA can share the same radio resources such as the code-domain or power-domain [3]. In code-domain NOMA, different users are assigned different codes and multiplexed over the same time-frequency resources, such as multiuser shared access (MUSA) [4], sparse code multiple access (SCMA) [5], and low-density spreading (LDS) [6]. In contrast, users in power-domain NOMA are assigned different power levels on the basis of channel state information for communication, and users use SIC or PIC technique to process the received signal. This approach has been received much attention from both academia and industry recently.

Due to the broadcast nature of wireless communication, the transmitted signal may be overheard by Eves over illegal channels, this results in a lot of challenges in solving security problems for wireless networks. To measure the security risk, the concept of physical layer security (PLS) was introduced by Wyner from an information-theoretical perspective [7], i.e., the secrecy capacity is defined as the subtraction between the capacity of main channel and the one of Eve. Accordingly, many works addressing on the secrecy performance analysis for different systems has been studied [8]–[11]. However, there are a few results related to the NOMA technique [12]–[22]. More specifically, in [12], authors investigated the maximization of the secrecy sum rate (SSR) of single input
single output (SISO) NOMA system, where each user has a predefined quality of service requirement. They derived the closed-form expression of an optimal power allocation policy to maximize the SSR. On the basis of [23], the optimal power allocation to maximization of the secrecy rate for the strong user subject to a maximum allowable SOP while satisfying non-secure transmission rate requirement to the weak user was considered. The physical layer security (PLS) of using NOMA in large-scale network where both NOMA users and Eve have been spatially randomly deployed. Also, a protected zone around the source node has been introduced to enhance the security of a random network [13]. Y. Liu et al. derived a new analytical SOP expression for characterizing the system secrecy performance in both single antenna and multi-antenna scenarios [14]. In the single antenna scenario, they outlined a protected zone around the BS to create a forbidden area where Eves are impossible to access.

Taking the advantages of multi-antennas technique, artificial noise is generated at the BS for further improving the security. The authors of [24] proposed a novel beamforming design to enhance PLS of NOMA with the aid of artificial noise. The work in [15] derived exact expressions for SOP of full-duplex relay (FRD) and half-duplex relay (HRD) NOMA systems. The results showed that the SOP of FRD outperforms the one of HRD. Subject to the Rayleigh fading, Chinh et al. have calculated closed-form expressions for the outage probability and secrecy capacity in the NOMA system [16]. Considering the imperfect self-interference cancellation, in [17], the secrecy outage probabilities of NOMA has been analyzed. The literature [19] investigated SOP of two-user SISO and multiple-input single-out (MISO) NOMA systems with different transmit antenna selection strategies and proposed an effective power allocation policy to obtain the diversity order.

Given the secrecy outage and quality of service constraints, authors proposed a NOMA scheme that is able to minimize the transmit power and then reduce the risk of eavesdropping [18]. Regarding the security issues for cooperative NOMA communication, in [25], authors proved that combination of full-duplex and artificial noise technique at relays can improve the physical layer security significantly. The authors of [26] proposed new cooperative jamming NOMA scheme to improve secrecy performance. In particular, the source actively sends jamming signals while the relay is forwarding. They concluded that the NOMA outperforms than orthogonal multiple access (OMA) in terms of secrecy rate. In [20], the secrecy performance of cooperative NOMA system for both amplify-and-forward and decode-and-forward protocols have been analyzed.

Apart from the above performance aspects, fairness of NOMA system also has received much attention. The authors of [21] proposed power allocation techniques to maximize fairness in term of data-rate under instantaneous channel state information at transmitter and average channel state information among users of a NOMA downlink. X. Chen et al. studied the proportional fairness-based scheduling scheme to enhance uplink NOMA performance [22]. However, the impact of security and fairness in NOMA system has not been investigated yet. Motivated by all of the above, in this paper, we introduce the concept of fairness of average packet transmission time, and then examine the secrecy outage probability of each user in the presence of an Eve who can operate in one of the interference cancellation modes to extract desired signal, named SIC or PIC technique. Accordingly, our major contributions are summarized as follows:

- An analytical expression of the SOP for each user and whole system are derived for both SIC and PIC mode.
- The expression of packet timeout probability for each user in NOMA system is obtained.
- Fairness of average packet transmission time is introduced and the algorithm to determine power coefficient to obtain the approximation fairness is implemented.

To the best of our knowledge, there is no previous work addressing on this problem.

The rest of this paper is organized as follows. In Section II, the system and channel model are introduced. In Section III, the SOP of each user and SOP system for both PIC and SIC mode are derived. Section IV analyses packet timeout probability. Section V calculates average packet transmission time from BS to two users. In Section VI, the fairness of system in term of average transmission time is considered. In Section VIII, numerical result examples are provided to verify the analytical expressions. Finally, Section IX summarizes the paper.

II. SYSTEM MODEL AND PERFORMANCE METRICS

In this section, we describe the system model and channel assumptions. Thereafter, the performance metrics are also presented to evaluate the performance of a single user as well as the whole system.

A. SYSTEM MODEL AND CHANNEL ASSUMPTIONS

Let us consider a NOMA system as shown in Fig. 1, in which the BS wants to simultaneously communicate with two users $U_1$ and $U_2$ in the presence of an Eve at the same time. The BS is able to allocate its transmit power corresponding to the quality of channel for each user. It means that higher power

![FIGURE 1. A NOMA system with a BS, two users, and an Eve. User $U_1$ stays near the BS while $U_2$ is far away from the BS.](image-url)
level is allocated to the user staying far away from the BS, i.e., $U_2$, while a lower power level will be assigned to the user near by the BS, i.e., $U_1$.

Given this context, symbols $g_1$, $g_2$ and $g_e$ denote the channel coefficients of the BS→$U_1$, BS→$U_2$, and BS→Eve links, respectively. We also assume that users are operating in the indoor environment and there is no-line-of-sight among users. Accordingly, all channels are modeled as Rayleigh fading, and the channel gain $|g_i|^2$ ($i \in \{1, 2, e\}$) are random variables (RVs) distributed following exponential distribution with channel mean gain $\Omega_i$. Thus, the probability density function (PDF) and cumulative distribution function (CDF) of $X_i = |g_i|^2$ are formulated, respectively, as follows:

$$f_{X_i}(x) = \frac{1}{\Omega_i} \exp\left(-\frac{x}{\Omega_i}\right), \quad (1)$$

$$F_{X_i}(x) = 1 - \exp\left(-\frac{x}{\Omega_i}\right). \quad (2)$$

It is noted that the considered Eve is able to apply SIC or PIC technique to decode the superimposed signal from the BS. SIC technique was proposed from 1990 [27], wherein, the receiver will detect and then cancel other signals until it receives its own desired signal. Each user decodes its own signal by treating the signal of other users with lower power coefficients as noise [28]. In order to further improve performance of SIC, adaptive SIC and recently advanced SIC were proposed [29], [30]. In contrast to SIC, the PIC technique allows the Eve to cancel the interference in parallel [31]. In other words, the Eve with PIC technique has multiuser detection ability and is smarter than that with SIC technique [28].

For communication, the BS transmits a superimposed signal $x$ which is a mixture signal of $x_1$ and $x_2$ to $U_1$ and $U_2$ as

$$x = \sqrt{\alpha_1}P x_1 + \sqrt{\alpha_2}P x_2, \quad (3)$$

where $P$ is transmit power of BS, $\alpha_j$ ($j \in \{1, 2\}$) is power allocation coefficient corresponding of the user $U_j$ which satisfies the condition $\alpha_1 + \alpha_2 = 1$. Here, $U_2$ (far user) is allocated a high power level, i.e., $\alpha_2 = 1 - \alpha_1 > 0.5$, while $U_1$ (near user) is assigned a lower power level, i.e., $\alpha_1 < 0.5$. Accordingly, the received signal at the $U_1$, $U_2$, and the Eve is formulated as

$$y_i = \sqrt{\alpha_1}P x_1 g_i + \sqrt{\alpha_2}P x_2 g_i + n_i, \quad (4)$$

where $n_i$ is additive white Gaussian noise (AWGN) with zero-mean and variance $N_0$. Since the BS allocates a higher power level to the signal of $U_2$, according to the principle of NOMA, the received signal at $U_2$ can be decoded by considering the signal of $U_1$ as an interference, while $U_1$ can decode its signal directly [24]. As a result, the signal-to-noise ratio (SNR) and signal-to-interference-plus-noise ratio (SINR) at $U_1$ and $U_2$ can be expressed, respectively, as

$$\gamma U_1 = \frac{\alpha_1 P |g_1|^2}{N_0}, \quad (5)$$

$$\gamma U_2 = \frac{\alpha_2 P |g_2|^2}{\alpha_1 P |g_2|^2 + N_0}. \quad (6)$$

Further, the Eve is in the zone of the BS so it also eavesdrops signals from the BS, and then it can apply advanced signal processing techniques like SIC or PIC to decode the eavesdropped signals. In the SIC mode, the Eve can decode the signal of $U_1$ directly, while it can decode the signal of $U_2$ by treating the signal of user $U_1$ as interference. As a consequence, the SNR and SINR have the similar forms given in (5) and (6), i.e,

$$\gamma_{E,1}^{SIC} = \frac{\alpha_1 P |g_e|^2}{N_0}, \quad (7)$$

$$\gamma_{E,2}^{SIC} = \frac{\alpha_2 P |g_e|^2}{\alpha_1 P |g_e|^2 + N_0}, \quad (8)$$

where $\gamma_{E,1}^{SIC}$ is the SNR at Eve when it tries to decode the signal of $U_1$, and $\gamma_{E,2}^{SIC}$ is the SINR at the Eve when it manages to decode the signal of $U_2$.

In the PIC mode, the Eve is assumed to be smarter than $U_1$ and $U_2$, i.e., it is able to decode the signal of multi-user at the same time and the interference caused by other signals can be cancelled effectively. Therefore, the instantaneous SNR of the Eve when it detects the information of $U_1$ is the same SNR of Eve in the SIC mode, i.e,

$$\gamma_{E,1}^{PIC} = \frac{\alpha_1 P |g_e|^2}{N_0}, \quad (9)$$

while the SNR decoded at the Eve regarding to $U_2$ can be expressed as

$$\gamma_{E,2}^{PIC} = \frac{\alpha_2 P |g_e|^2}{N_0}. \quad (10)$$

It is clear to see that the SNR in the PIC mode is always greater than or equal the one of SIC mode. In the following, we analyze the impact of SIC and PIC mode of the Eve on the security issues for the considered system.

**B. PERFORMANCE METRICS**

1) **SECRET OUTAGE PROBABILITY (SOP)**

It is worth to remind that the secrecy capacity is defined as the subtraction between the capacity of the main channel $C_M$ and the one of illegitimate channel $C_E$ [7], i.e.,

$$C_S = C_M - C_E. \quad (11)$$

Accordingly, the SOP is defined as the probability that instantaneous secrecy capacity is dropped below a secrecy target rate $R_S$, i.e.,

$$O_{sec} = \Pr[C_S < R_S]. \quad (12)$$

This can be expressed by words that the decreasing of $O_{sec}$ leads to increasing of the security level.
2) PACKET TIMEOUT PROBABILITY (PTP)
When the BS sends packets with size of $L$ to users $U_1$ and $U_2$, it is expected to know how many percent that the packet is dropped given a specific channel condition. Here, the packet is dropped if its instantaneous transmission time $T^*$ is greater than a predefined threshold, $t_{out}$, i.e.,

$$P_{out} = \Pr \{T \geq t_{out} \}. \quad (13)$$

3) FAIRNESS OF USERS
In this paper, we consider the case that both users request to have the same quality of service, thus resource should be allocated so that there is the at least different average packet transmission time among users, i.e.,

$$\alpha^* = \max_{0<\alpha<0.5} |E[T_1] - E[T_2]|, \quad (14)$$

where $E[T_i]$ is expected packet transmission time from the BS to the user $U_i$.

III. SECURITY PERFORMANCE ANALYSIS
In this section, we derive the analytical expression for the SOP in both SIC and PIC mode of the Eve.

A. THE SOP WITH SIC MODE OF AN EVE
In the SIC mode, we assume that the Eve, $E$, and $U_2$ have the same capability in interference cancellation.

1) THE SOP WITH SIC MODE OF AN Eve FOR A SINGLE USER
As we know that the Eve want to eavesdrop the information of both users $U_1$ and $U_2$. According to the definition in (11), we can express the instantaneous secrecy capacities of $U_1 (C_{U_1}^{SIC})$ and $U_2 (C_{U_2}^{SIC})$, respectively, as follows:

$$C_{U_1}^{SIC} = (B \log_2(1 + \gamma_{U_1}B) - B \log_2(1 + \gamma_{E_1}^{SIC}))^+, \quad (15)$$

$$C_{U_2}^{SIC} = (B \log_2(1 + \gamma_{U_2}B) - B \log_2(1 + \gamma_{E_2}^{SIC}))^+, \quad (16)$$

where $x^+ = \max\{x, 0\}$, $B$ is the system bandwidth, and symbols $\gamma_{U_1}, \gamma_{U_2}, \gamma_{E_1}^{SIC}$ and $\gamma_{E_2}^{SIC}$ are formulated in (5), (6), (7) and (8), respectively.

On this basis, the SOP of $U_1$, which is defined as the instantaneous secrecy capacity dropped below a predefined secrecy target rate is calculated as

$$O_{U_1}^{SIC} = \Pr \{C_{U_1}^{SIC} < R_1 \} = \Pr \{\gamma_{U_1} < \delta_1 + (\delta_1 + 1)\gamma_{E_1}^{SIC} \} \quad (17)$$

Next, we use [32, 3.5] to obtain the SOP of $U_1$ as

$$O_{U_1}^{SIC} = \int_0^\infty F_{\gamma_{U_1}}(\delta_1 + (\delta_1 + 1)x) f_{\gamma_{E_1}^{SIC}}(x) dx, \quad (18)$$

where $\delta_1 = 2^{R_1/B} - 1$ and $R_1$ is the secrecy target rate of $U_1$.

In order to simplify the integral (17), we need to find the CDF and PDF of $\gamma_{U_1}$ and $\gamma_{E_1}^{SIC}$, respectively.

Applying exponential distribution [33], the CDF of $\gamma_{U_1}$ can obtain as follows:

$$F_{\gamma_{U_1}}(t) = \Pr \{\gamma_{U_1} < t \} = 1 - \exp(-\lambda_1 t), \quad (19)$$

where $\lambda_1 = \frac{N_0}{\alpha_1 P T_1}$. Furthermore, the CDF of $\gamma_{E_1}^{SIC}$ is calculated as

$$F_{\gamma_{E_1}^{SIC}}(x) = \Pr \{\gamma_{E_1}^{SIC} < x \} = 1 - \exp(-\lambda_{e_1} x), \quad (20)$$

where $\lambda_{e_1} = \frac{N_0}{\alpha_1 P T_1}$. Thus, the PDF of $\gamma_{E_1}^{SIC}$ is obtained easily by differentiating (20) w.r.t $x$ as

$$f_{\gamma_{E_1}^{SIC}}(x) = \lambda_{e_1} \exp(-\lambda_{e_1} x). \quad (21)$$

Substituting (19) with $t = \lambda_1 + (\lambda_1 + 1) x$ and (21) into (17), the SOP of $U_1$ is obtained as

$$O_{U_1}^{SIC} = 1 - \frac{\lambda_{e_1} \exp(-\lambda_{e_1} \delta_1)}{\lambda_1 (\delta_1 + 1) + \lambda_{e_1}}. \quad (22)$$

Similarly, the SOP of $U_2$ can be rewritten on the basis of (16) as

$$O_{U_2}^{SIC} = \Pr \{C_{U_2}^{SIC} < R_2 \} = 1 - \Pr \{\gamma_{E_2}^{SIC} < \frac{\gamma_2 - \delta_2}{\delta_2 + 1} \} \quad (23)$$

Using exponential distribution, the CDF of $\gamma_{E_2}^{SIC}$ is obtained as

$$F_{\gamma_{E_2}^{SIC}}(x) = \Pr \{\gamma_{E_2}^{SIC} < x \} = \Pr \left\{ |g_2|^2 < \frac{N_0 x}{(\alpha_2 - \alpha_1) P} \right\}. \quad (24)$$

By applying exponential distribution, the CDF of $\gamma_{E_2}^{SIC}$ is obtained as

$$F_{\gamma_{E_2}^{SIC}}(x) = \begin{cases} 1 - \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1} \right) & \text{if } x < \alpha_2/\alpha_1, \\ 0 & \text{if } x \geq \alpha_2/\alpha_1, \end{cases} \quad (25)$$

where $\lambda_2 = \frac{N_0}{\alpha_2 P T_2}$. Differentiating (25) w.r.t $x$, we obtain the PDF of $\gamma_{U_2}$ as

$$f_{\gamma_{U_2}}(x) = \begin{cases} \frac{\lambda_2 \alpha_2}{(\alpha_2 - \alpha_1)^2} \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1} \right) & \text{if } x < \alpha_2/\alpha_1, \\ 0 & \text{if } x \geq \alpha_2/\alpha_1. \end{cases} \quad (26)$$

Substituting (24) and (26) into (23) yields the SOP of user $U_2$ as

$$O_{U_2}^{SIC} = 1 - \lambda_2 \alpha_2 (I_1 - I_2). \quad (27)$$

where $I_1$ and $I_2$ are defined as follows:

$$I_1 = \int_0^{\alpha_2/\alpha_1} \frac{1}{(\alpha_2 - \alpha_1)^2} \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1} \right) dx, \quad (28)$$
and

$$I_2 = \int_{0}^{\alpha_2/\alpha_1} \frac{1}{(\alpha_2 - \alpha_1 x)^2} \exp \left( \frac{A_1 x^2 - B_1 x + C_1}{(\delta_2 + \alpha_2 - \alpha_1 x)(\alpha_2 - \alpha_1 x)} \right) dx,$$

(29)

here, $A_1$, $B_1$ and $C_1$ are defined as

$$A_1 = \lambda_x \alpha_1 + \lambda_2 \alpha_1,$$

(30)

$$B_1 = \lambda_x \alpha_2 \delta_2 + \lambda_x \alpha_1 \delta_2 + \lambda_2 \alpha_2,$$

(31)

$$C_1 = \lambda_x \alpha_2 \delta_2.$$

(32)

2) **THE SOP WITH SIC MODE OF AN Eve**

For a NOMA System

The BS broadcasts the signals to $U_1$ and $U_2$. Therefore, outage happens when either $C_{U_1}^{\text{SIC}}$ or $C_{U_2}^{\text{SIC}}$ falls below their own target rates. Given this definition, the SOP of system can be expressed as

$$\text{SOP}^{\text{SIC}} = \text{Pr}[C_{U_1}^{\text{SIC}} < R_1] = 1 - \text{Pr}[\frac{B \log_2 \left( \frac{1 + \gamma_{U_1}}{1 + \gamma_{E,1}} \right)}{1 + \gamma_{E,1}} > R_1],$$

(33)

$$B \log_2 \left( \frac{1 + \gamma_{U_2}}{1 + \gamma_{E,2}} \right) > R_2 \right)$$

$$= 1 - \int_{0}^{\rho} \text{Pr}[|g_1|^2 > F_1(x)] \text{Pr}[|g_2|^2 > F_2(x)] |f_{|g_1|^2}(x)| dx,$$

(34)

where $f_{|g_r|^2}(x)$ is PDF of $|g_r|^2$, $\rho = \frac{\beta_2 - \beta_1 \delta_2}{\alpha_2 \delta_2 (\beta_1 + \beta_2)}$, $\beta_1 = \frac{\alpha_1 \beta_1}{\alpha_0}$, $\beta_2 = \frac{\alpha_2 \beta_2}{\alpha_0}$, and $F_1(x)$ and $F_2(x)$ are defined as

$$F_1(x) = \frac{\delta_1 + (\delta_1 + 1)x}{\beta_1},$$

$$F_2(x) = \frac{\delta_2 + (\delta_2 + \beta_2) + \beta_2}{\beta_2 - \delta_2 \beta_1 - \delta_2 \beta_1 (\beta_1 + \beta_2)x}.$$

(35)

After some mathematical manipulations, we arrive at $\text{SOP}^{\text{SIC}}$ as follows:

$$\text{SOP}^{\text{SIC}} = 1 - \frac{1}{\Omega_2} \int_{0}^{\rho} \exp \left( - \frac{F_1(x)}{\Omega_1} - \frac{F_2(x)}{\Omega_2} - \frac{x}{\Omega_e} \right) dx,$$

(36)

$$= 1 - K \int_{0}^{\rho} \exp \left( - \frac{A_2 H x^2 + (A_2 G + A_3) x + B_2}{G \cdot H x} \right) dx,$$

where $K$, $A_2$, $B_2$, $G$, $H$ are defined as

$$K = \frac{\exp \left( - \frac{\delta_1}{\beta_1 \Omega_1} \right)}{\Omega_e},$$

(37)

$$A_2 = \frac{(\delta_1 + 1) \Omega_e + \Omega_1}{\Omega_1 \Omega_e},$$

(38)

2) **THE SOP WITH PIC MODE OF AN Eve**

For a NOMA System

In this mode, the SOP of $U_1$, i.e., $O_{U_1}^{\text{PIC}}$, is the same as that in SIC mode and is expressed in (22). On the other hand, the secrecy capacity of channel from the BS to $U_2$ is given by

$$C_{U_2}^{\text{SIC}} = \{B \log_2(1 + \gamma_{U_2}) - B \log_2(1 + \gamma_{E,2}^{\text{SIC}})\}^+.$$

(43)

Accordingly, the SOP at $U_2$ for SIC mode of the Eve can be expressed as

$$O_{U_2}^{\text{SIC}} = \text{Pr}[C_{U_2}^{\text{SIC}} < R_2] = 1 - \text{Pr}[C_{U_2}^{\text{SIC}} > R_2]$$

$$= 1 - \int_{0}^{\rho} \text{Pr}[\frac{\gamma_{E,2}}{\gamma_{E,1}} > x] f_{g_2}(x).$$

(44)

Similar to approach of (22), we need to find the CDF and PDF of $\gamma_{E,2}^{\text{SIC}}$ and $\gamma_{U_2}$ to solve (44) as follows:

$$f_{g_{E,2}^{\text{SIC}}}(x) = \text{Pr}[|g_{E,2}^{\text{SIC}}| < x] = \text{Pr} \left[ \frac{|g_e|^2 < \frac{N_0 x}{\alpha_0 P}}{1 + \frac{x}{\delta_2 + 1}} \right] = 1 - \exp(-\lambda_{e_2} x),$$

(45)

where $\lambda_{e_2} = \frac{N_0}{\alpha_0 P}$ and PDF of $f_{g_2}(x)$ is expressed in (26).

Substituting (26) and (45) into (44) we can obtain the expression of the SOP for user $U_2$ as follows:

$$C_{U_2}^{\text{PIC}} = 1 - \lambda_2 \alpha_2 (11 - 13),$$

(46)

where $I_1$ is defined as in (28) and $I_3$ is expressed as follows:

$$I_3 = \int_{0}^{\rho} \frac{1}{(\alpha_2 - \alpha_1 x)^2} \exp \left( - \frac{A_4 x^2 - B_3 x + C_2}{(\delta_2 + 1)(\alpha_2 - \alpha_1 x)} \right) dx,$$

(47)

where $A_4$, $B_3$, and $C_2$ are defined, respectively, as

$$A_4 = \alpha_1 \lambda_{e_2},$$

(48)

$$B_3 = \alpha_2 \lambda_{e_2} + \alpha_1 \lambda_{e_2} + \lambda_2 (\delta_2 + 1),$$

(49)

$$C_2 = \alpha_2 \lambda_{e_2}.$$

(50)
\[ = 1 - \int_0^\epsilon \Pr(|g_1|^2 > F_1(x)) \times \Pr(|g_2|^2 > F_3(x)) |_{g_1^2}(x) dx \]
\[ = 1 - \frac{1}{\Omega_e} \int_0^\epsilon \exp \left( -\frac{F_1(x)}{\Omega_1} - \frac{F_3(x)}{\Omega_2} - \frac{x}{\Omega_e} \right) dx, \]
(51)

where \( \epsilon \) and \( F_3(x) \) are defined as follows:
\[ F_3(x) = \frac{\beta_2 + (\delta_2 + 1)\beta_2 x}{\beta_2 - \beta_1\delta_2 - \beta_1\beta_2(\delta_2 + 1)x}, \]
\[ \epsilon = \frac{\beta_1\beta_2(\delta_2 + 1)}{\beta_2 - \beta_1\delta_2}. \]
(52)

After some mathematical manipulations, the \( SOP^{PIC} \) can be obtained as follows:
\[ SOP^{PIC} = 1 - K \int_0^\epsilon \exp (\psi) dx, \]
(54)

where \( \psi, A_5, A_6, J \) are defined as
\[ \psi = -A_3 H x^2 + (A_6 + A_2 G)x + B_2, \]
\[ A_5 = \frac{\delta_2 + 1)\lambda_2}{\Omega_2}, \]
\[ A_6 = \frac{(\delta_2 + 1)\beta_2}{\Omega_2}, \]
\[ J = \beta_1\beta_2(\delta_2 + 1). \]
(55)

\section*{IV. PACKET TIMEOUT PROBABILITY}

In section IV, V, and VI, we derive the packet timeout probability, and the average packet transmissions time for each user without considering the PIC and SIC mode of the Eve. This is because the Eve operates in passive mode and do not affect to the packet transmission rate. Note that the BS needs to transmit each packet to \( U_1 \) and user \( U_2 \) with bandwidth-normalized entropy \( \hat{B} \) (nats/Hz) and within a defined time-out \( t_{out} \). Symbol \( T_j \) \( (j \in \{1, 2\}) \) denotes the time that takes to transmit a packet from the BS to \( U_j \) (including packets dropped). Following the third Shannon theorem [34], we can express the time \( T_j \) that takes a transmit packet as
\[ T_j = \frac{\hat{B}}{\log_2(1 + \gamma_j)}. \]
(59)

where \( \gamma_j \) are defined in (5) and (6).

Given the channel conditions, the outage probability \( P_{out} \) is defined as the probability that the packet transmission time \( T_j \) exceeds the interval \( t_{out} \), i.e.,
\[ P_{out}^{(j)} = \Pr(T_j \geq t_{out}). \]
(60)

Accordingly, the packet timeout probability \( P_{out}^{(1)} \) can be expressed as
\[ P_{out}^{(1)} = \Pr(T_1 \geq t_{out}) = 1 - F_{T_1}(t_{out}). \]
(61)

In order to solve (61), we need to find the CDF and PDF of \( T_1 \). First, we use exponential distribution to calculate the CDF of \( T_1 \) as
\[ F_{T_1}(t) = \Pr(T_1 < t) = \exp \left\{ -\lambda_1 \left[ \exp \left( \frac{\hat{B}}{t} \right) - 1 \right] \right\}. \]
(62)

The PDF of \( T_1 \) then can be derived by differentiating (62) w.r.t \( t \) as follows:
\[ f_{T_1}(t) = \frac{\hat{B}\lambda_1}{t^2} \exp \left\{ \frac{\hat{B}}{t} - \lambda_1 \left[ \exp \left( \frac{\hat{B}}{t} \right) - 1 \right] \right\}. \]
(63)

By substituting (62) into (61), the outage probability of \( U_1 \) is expressed as follows:
\[ P_{out}^{(1)} = 1 - \exp \left\{ -\lambda_1 \left[ \exp \left( \frac{\hat{B}}{t_{out}} \right) - 1 \right] \right\}. \]
(64)

On the other hand, let \( T_{suc}^{(1)} \) denotes the transmission time of a packet that is not dropped, i.e., [35]
\[ T_{suc}^{(1)} = \{T_1|T_1 < t_{out}\}. \]
(65)

By applying Bayes’ rule [35], the probability of an event \( T_{suc}^{(1)} \) takes places that can be expressed as
\[ \Pr(T_1|T_1 < t_{out}) = \frac{\Pr(T_1, T_1 < t_{out})}{\Pr(T_1 < t_{out})}. \]
(66)

Accordingly, we can express the CDF of \( T_{suc}^{(1)} \) as follows [35]:
\[ F_{T_{suc}^{(1)}}(x) = \begin{cases} 1 - \frac{1}{1 - P_{out}^{(1)}} \int_0^{t_{out}} f_{T_1}(t) dt, & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out} \end{cases}. \]
(67)

Differentiating both side of (67) w.r.t \( x \), the PDF of packet timeout can be expressed as [35]
\[ f_{T_{suc}^{(1)}}(t) = \begin{cases} \frac{f_{T_1}(t)}{1 - P_{out}^{(1)}}, & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out} \end{cases}. \]
(68)

Substituting (63) into (68), the PDF \( f_{T_{suc}^{(1)}}(t) \) can be rewritten as
\[ f_{T_{suc}^{(1)}}(t) = \begin{cases} \frac{\hat{B}\lambda_1}{t^2} \exp \left[ \frac{\hat{B}}{t} - \lambda_1 \left( \exp \left( \frac{\hat{B}}{t} \right) - 1 \right) \right], & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out} \end{cases}. \]
(69)

Similar to \( P_{out}^{(1)} \), packet timeout probability \( P_{out}^{(2)} \) from the BS to user \( U_2 \) can be expressed as
\[ P_{out}^{(2)} = \Pr(T_2 \geq t_{out}) = 1 - F_{T_2}(t_{out}). \]
(70)
In order to solve (70), we need to find the CDF and PDF of $T_2$. The CDF of $T_2$ can be formulated as

$$F_{T_2}(t) = \Pr\{T_2 < t\} = 1 - F_{T_2}\left[\exp\left(\frac{\hat{B}}{t}\right) - 1\right].$$

(71)

Similar to the approach of the CDF of $T_1$, we have

$$F_{T_2}(t) = \begin{cases} \exp(M) & \text{if } t > \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \\ 1 & \text{if } t \leq \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \end{cases}$$

(72)

where $M = \frac{-1}{\alpha_1 \log_e(\frac{1}{\alpha_1})}$. The PDF of $T_2$ can be derived by differentiating (72) w.r.t $t$ as follows:

$$f_{T_2}(t) = \begin{cases} \frac{\exp(M + \frac{\hat{B}}{t})\lambda_2\alpha_2\hat{B}}{t^2\left(1 - \alpha_1 \exp\left(\frac{\hat{B}}{t}\right)\right)^2} & \text{if } t > \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \\ 0 & \text{if } t \leq \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \end{cases}$$

(73)

Substituting (72) into (70), we can obtain the closed-form expression for the outage probability of $U_2$ as

$$p_{out}^{(2)} = \begin{cases} 1 - \exp\left\{\frac{\lambda_2\left[\exp\left(\frac{\hat{B}}{t_{out}}\right) - 1\right]}{1 - \alpha_1 \exp\left(\frac{\hat{B}}{t_{out}}\right)}\right\} & \text{if } t_{out} > \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \\ 0 & \text{if } t_{out} \leq \frac{\hat{B}}{\log_e(\frac{1}{\alpha_1})} \end{cases}$$

(74)

On the other hand, let $T_{suc}^{(2)}$ denotes the transmission time that the packet is not dropped, i.e.,

$$T_{suc}^{(2)} = \{T_2 | T_2 < t_{out}\}.\tag{75}$$

Similar to (67) and (68), the CDF and PDF of $T_{suc}^{(2)}$ can be expressed as

$$F_{T_{suc}^{(2)}}(x) = \begin{cases} \frac{1}{1 - p_{out}^{(2)}} \int_{0}^{t_{out}} f_{T_2}(t)dt, & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out} \end{cases}$$

(76)

$$f_{T_{suc}^{(2)}}(t) = \begin{cases} \frac{f_{T_2}(t)}{1 - p_{out}^{(2)}}, & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out} \end{cases}$$

(77)

Substituting (73) into (77), the PDF of packet transmission time without being timeout can be rewritten as

$$f_{T_{suc}^{(2)}}(t) = \begin{cases} \frac{\lambda_2\alpha_2\hat{B}}{1 - p_{out}^{(2)}} \epsilon^2 \left[1 - \alpha_1 \exp\left(\frac{\hat{B}}{\epsilon}\right)\right]^2 & \text{if } 0 \leq t < t_{out} \\ 0, & \text{if } t \geq t_{out}, \end{cases}$$

(78)

where $I_4 = \exp\left\{\frac{\hat{B}}{\epsilon} - \frac{\lambda_2\left[\exp\left(\frac{\hat{B}}{\epsilon}\right) - 1\right]}{1 - \alpha_1 \exp\left(\frac{\hat{B}}{\epsilon}\right)}\right\}$.

V. AVERAGE PACKET TRANSMISSION TIME

Average transmission time is defined as the time that takes to transmit a packet from the BS to the users (including packets dropped).

A. AVERAGE PACKET TRANSMISSION TIME FROM THE BS TO $U_1$.

Let us start with the average transmission time of packet without timeout as

$$E[T_{suc}^{(1)}] = \int_{0}^{t_{out}} f_{T_{suc}^{(1)}}(t)dt.\tag{79}$$

Substituting (63) into (79), we obtain the first moment of packet transmission time from the BS to user $U_1$ without timeout as follows:

$$E[T_{suc}^{(1)}] = \int_{0}^{t_{out}} \frac{\lambda_1\hat{B}}{1 - p_{out}^{(1)}} \int_{\epsilon}^{t} \frac{\lambda_1\hat{B}}{1 - p_{out}^{(1)}} dt \times \exp\left\{\frac{\hat{B}}{\epsilon} - \frac{\lambda_1\left[\exp\left(\frac{\hat{B}}{\epsilon}\right) - 1\right]}{1 - \alpha_1 \exp\left(\frac{\hat{B}}{\epsilon}\right)}\right\} dt.\tag{80}$$

Finally, by applying the law of total expectation [35], the first moment of packet transmission time $T_1$ (including dropped packets) can be given by

$$E[T_1] = (1 - p_{out}^{(1)})E[T_{suc}^{(1)}] + t_{out} p_{out}^{(1)},$$

where $p_{out}^{(1)}$ and $E[T_{suc}^{(1)}]$ are given by (64) and (80), respectively.

B. AVERAGE TRANSMISSION TIME FROM THE BS TO $U_2$.

Similar to $E[T_{suc}^{(1)}]$, we obtain the first moment of packet transmission time from the BS to user $U_2$ without timeout as follows:

$$E[T_{suc}^{(2)}] = \int_{\epsilon}^{t} f_{T_{suc}^{(2)}}(t)dt$$

$$= \frac{\lambda_2\alpha_2\hat{B}}{1 - p_{out}^{(2)}} \int_{\epsilon}^{t} \frac{1}{1 - \alpha_1 \exp\left(\frac{\hat{B}}{\epsilon}\right)^2} dt.\tag{82}$$
where \( \epsilon = \frac{\hat{B}}{\log e} \left( \frac{1}{\alpha_1} \right) \) and \( I_5 \) is defined as

\[
I_5 = \exp \left[ \frac{-\lambda_2 (\exp \left( \frac{\hat{B}}{T} \right) - 1)}{1 - \alpha_1 (\exp \left( \frac{\hat{B}}{T} \right) - 1)} \right].
\] (83)

We finally obtain the first moment of packet transmission time \( T_2 \) (including dropped packets) by applying the law of total expectation as follows [35]:

\[
E[T_2] = (1 - P_{out}^2)E[T_{su}(2)] + t_{out}P_{out}^2,
\] (84)

where \( P_{out}^2 \) and \( E[T_{su}(2)] \) are given by (74) and (82), respectively.

**VI. THE FAIRNESS OF PACKET TRANSMISSION TIME**

In this section, we investigate the problem of optimal power allocation for each user to achieve the average packet transmission time \( E[T_1] \) from the BS to \( U_1 \) is the same one from the BS to \( U_2 \). Thus, the problem can be formulated as follows:

\[
\alpha_1^* = \max_{0 < \alpha_1 < 0.5} [E[T_1] - E[T_2]],
\] (85)

where \( \alpha_1^* \) is the power allocation coefficient satisfied criteria that minimum the difference between average packet transmission time from BS to user \( U_1 \) and user \( U_2 \). Accordingly, we propose **Algorithm 1** to determine the power allocation coefficient \( \alpha_1^* \) with desirable accuracy.

**Algorithm 1** Solution to Determine the Power Allocation Coefficient \( \alpha_1 \)

1. \( \alpha_1 \leftarrow \) an optional value \((0 < \alpha_1 < 0.5)\)
2. while \( \text{abs}(E[T_1] - E[T_2]) > \nu \) do
3. \( \alpha_2 \leftarrow 1 - \alpha_1 \)
4. Calculate \( E[T_1] \) by using (81)
5. Calculate \( E[T_2] \) by using (84)
6. \( \alpha_1 \leftarrow \alpha_1 + \zeta \)
7. \( \alpha_1^* \leftarrow \alpha_1 - \zeta \)
8. return \( \alpha_1^* \)

where \( \nu \) is desirable accuracy and \( \zeta \) is increasing step.

**VII. DISCUSSION AND EXTENSION**

Our analysis can be extended to the more general case in which the Eve is more powerful hardware such as having multiple antenna. We assume that Eve is equipped with \( N \) antennas and each antenna branch experiences i.i.d channel fading.

**A. EVE WITH MULTIPLE ANTENNAS IN SIC MODE**

According to (15) and (16), the secrecy capacity for signals \( s_1 \) and \( s_2 \) at the \( j \)th branch antenna of Eve can be expressed as follows:

\[
C_{SU(1)}^{SIC} = B \log_2 \left( 1 + \gamma_{UI(1)} \right) - B \log_2 \left( 1 + \gamma_{E,1(1)}^{SIC} \right),
\] (86)

\[
C_{SU(2)}^{SIC} = B \log_2 \left( 1 + \gamma_{UI(2)} \right) - B \log_2 \left( 1 + \gamma_{E,2(2)}^{SIC} \right),
\] (87)

where \( j \in \{1, 2, ..., N\} \). Therefore, the security outage happens either minimum \( C_{SU(1)}^{SIC} \) or minimum \( C_{SU(2)}^{SIC} \) falls below their own target rates. Given this definition, the SOP of the system can be written as

\[
SOP_N^{SIC} = \Pr \left\{ \min_{j=1,2,...,N} \left\{ C_{SU(1)}^{SIC} \right\} < R_1 \right. \\
\text{or} \left. \min_{j=1,2,...,N} \left\{ C_{SU(2)}^{SIC} \right\} < R_2 \right\}.
\] (88)

\[
= 1 - \Pr \left\{ \log_2 \left( 1 + \gamma_{UI(1)} \right) - \log_2 \left( 1 + \gamma_{E,1(1)}^{SIC} \right) > R_1 \right. \\
\text{and} \left. \log_2 \left( 1 + \gamma_{UI(2)} \right) - \log_2 \left( 1 + \gamma_{E,2(2)}^{SIC} \right) > R_2 \right\}
\] (89)

\[
= 1 - \int_0^\rho \Pr (|g_1|^2 > F_1(x) ) \Pr (|g_2|^2 > F_2(x) ) f_{|g_e,i|^2}(x) dx
\] (90)

After some mathematical manipulations, we arrived at \( SOP_N^{SIC} \) as follows:

\[
SOP_N^{SIC} = 1 - \int_0^\rho \exp \left[ -\frac{F_1(x)}{\Omega_1} - \frac{F_2(x)}{\Omega_2} \right] f_{|g_e,i|^2}(x) dx,
\] (91)

where \( |g_e,i|^2 = \max_{j=1,2,...,N} (|g_{ei,j}|^2) \), \( f_{|g_e,i|^2} \) is PDF of \( |g_e,i|^2 \), \( F_1(x) \) and \( F_2(x) \) are defined in (34), (34), respectively. In order to solve the (91), we need to find CDF and PDF of \( |g_e,i|^2 \). Let us start with the CDF of \( |g_e,i|^2 \) as follows:

\[
F_{|g_e,i|^2}(x) = \Pr \left\{ \max_{j=1,2,...,N} (|g_{ei,j}|^2) < x \right\}
\]

\[
= \prod_{j=1}^N \Pr (|g_{ei,j}|^2 < x)
\]

\[
= \prod_{j=1}^N \left[ 1 - \exp \left( -\frac{x}{\Omega_{ei,j}} \right) \right].
\] (92)

Here, we assume that all branches of antenna have the same channel mean gain, i.e., \( \Omega_{ei,1} = \Omega_{ei,2} = \cdots = \Omega_{ei,N} = \Omega_e \) [36]. Thus (92) can be rewritten as

\[
F_{|g_e,i|^2}(x) = \left[ 1 - \exp \left( -\frac{x}{\Omega_e} \right) \right]^N.
\] (93)

Differentiating (92) w.r.t \( x \), we obtain the PDF of \( |g_e,i|^2 \) as

\[
f_{|g_e,i|^2}(x) = \frac{N}{\Omega_e} \exp \left( -\frac{x}{\Omega_e} \right) \left[ 1 - \exp \left( -\frac{x}{\Omega_e} \right) \right]^{(N-1)}
\]

\[
= \frac{N}{\Omega_e} \exp \left( -\frac{x}{\Omega_e} \right) \sum_{k=0}^{N-1} c_k^{N-1} \left[ -\exp \left( -\frac{x}{\Omega_e} \right) \right]^k.
\] (94)
Substituting (94) into (88), the SOP of NOMA system can be rewritten as follows:

$$SOP_{N}^{NOMA} = 1 - N \cdot K \int_{0}^{\rho} \exp(\chi) \nu \, d\chi,$$  \hspace{1cm} (95)

where $\chi$ and $\nu$ are defined as

$$\chi = \left[ -A_2 H x^2 + (A_2 G + A_3) x + B_2 \right],$$  \hspace{1cm} (96)

$$\nu = \sum_{k=0}^{N-1} C_k^{N-1} \left[ - \exp \left( - \frac{k x}{2 e} \right) \right].$$  \hspace{1cm} (97)

**B. EVE WITH MULTIPLE ANTENNAS IN PIC MODE**

Similar to SIC mode, the secrecy capacity for signals $s_1$ and $s_2$ at the $i^{th}$ branch antenna of Eve in PIC mode can be expressed as follows:

$$C_{U_{1(i)}}^{PIC} = \left[ B \log_2 (1 + \gamma_{U_1}) - B \log_2 \left( 1 + \gamma_{E,1(i)}^{PIC} \right) \right]^+,$$  \hspace{1cm} (98)

$$C_{U_{2(i)}}^{PIC} = \left[ B \log_2 (1 + \gamma_{U_2}) - B \log_2 \left( 1 + \gamma_{E,2(i)}^{PIC} \right) \right]^+.$$  \hspace{1cm} (99)

Therefore, the SOP of system can be expressed as

$$SOP_{N}^{PIC} = \Pr \left\{ \min_{j=1,2,\ldots,N} \left[ C_{U_{j(i)}}^{PIC} \right] < R_1 \right\}$$

or

$$\min_{j=1,2,\ldots,N} \left[ C_{U_{j(i)}}^{PIC} \right] < R_2 \right\}$$

\hspace{1cm} (100)

$$= 1 - \Pr \left\{ \log_2 \left( 1 + \max_{i=1,2,\ldots,N} \gamma_{E,i(i)}^{PIC} \right) \right\} > R_1$$

$$= 1 - \log_2 \left( 1 + \max_{i=1,2,\ldots,N} \gamma_{E,i(i)}^{PIC} \right) \right\} > R_2 \right\}$$

\hspace{1cm} (101)

$$= 1 - \int_{0}^{\rho} \Pr \left\{ \frac{f_1(x)}{f_2(x)} > f_3(x) \right\} \, dx.$$  \hspace{1cm} (102)

After some mathematical manipulations, we obtained $SOP_{N}^{PIC}$ as follows:

$$SOP_{N}^{PIC} = 1 - N \cdot K \int_{0}^{\rho} \exp(\chi) \nu \, d\chi,$$  \hspace{1cm} (103)

where $F_3(x)$ is defined as in (52) and

$$\pi = \frac{-A_2 H x^2 + (A_6 + A_2 G)x + B_2}{Jx - G}.$$

**VIII. NUMERICAL RESULTS**

In this section, we provide numerical results for evaluating the secrecy performance and fairness of the considered system. We use Monte Carlo simulations by averaging results for independent loop. The system parameters is as follows:

- Transmit SNR of BS: $\gamma_{BS} = P/N_0$
- System bandwidth: $B = 5$ MHz
- Packet size: $L = 4096$ bits (512 bytes)
- Timeout: $t_{out} = 10^{-3}$ s
- Outage secrecy target rate: $R_1 = R_2 = 1000$ Kbps

Fig. 2 illustrates the impact of the transmit SNR of the BS on the SOP for both SIC and PIC modes. We can see that the SOP is significantly lower for SIC mode compared to that for the PIC mode in the entire range of the considered transmit SNR of the BS. This is a fact that the Eve with the PIC mode can use the multi-user detection ability to distinguish the superimposed mixture. Furthermore, the SOP increases with the higher transmit SNR of the BS for both of SIC and PIC modes; this is because that the actual secrecy capacity decreases when the Eve receives a stronger signal from the BS.

Fig. 3 depicts the effects of the transmit SNR on the SOP of both SIC and PIC modes. It can be observed that the SOPs of...
In both SIC and PIC modes, $U_1$ is the same and constant as SNR increases. This is because the transmit SNR exists in numerator and denominator of the secrecy capacity formula of $U_1$ (15) (can be written as $B \log_2 \left( \frac{1 + \gamma_1 |g_1|^2}{1 + \alpha_1 \gamma_1 |g_1|^2} \right)$ where $\gamma_1 = P/N_0$). Thus, as the transmit SNR increases, both numerator and denominator concurrently increase. It means that the secrecy capacity of $U_1$ does not change, i.e., $U_1$ has approximately constant SOP. Furthermore, the SOP of $U_2$ for both SIC and PIC mode increase when the transmit SNR increases. This is due to the same reason as discussed in Fig. 2, i.e., actual secrecy capacity decreases when the Eve receives a stronger signal from the BS. In addition, the SOP of $U_2$ in PIC mode is higher than that in SIC mode. This is due to the Eve with the PIC mode can use the multi-user detection ability to distinguish the superimposed mixture.

Fig. 4 presents the SOP with the SIC mode of the Eve for $U_1$, $U_2$, and NOMA system as a function of the coefficient $\alpha_1$. We can observe that changing the value of power coefficient has a little impact on the SOP of $U_1$, $U_2$, and NOMA system. This phenomenon can be explained as that $U_1$, $U_2$, and Eve use SIC technique in this case. When $\alpha_1$ increases, the SINR of signal $x_1$ at $U_1$ and Eve concurrently increases while the SINR of signal $x_2$ at $U_2$ and Eve concurrently deteriorates. Accordingly, the secrecy capacity of signal $x_1$ and $x_2$ does not change as $\alpha_1$ increases. This conclusion is also verified again by Fig. 5.

Fig. 5 plot the SOP with the SIC mode of the Eve for $U_1$, $U_2$, and NOMA system versus channel mean gain of Eve. It is clear that the SOP of system in both SIC and PIC mode increases as the number of antennas of Eve increases. This is due to that $\Omega_e$ increases, i.e., Eve is more near to BS so Eve is able to decode signal better, therefore the SOP of both $U_1$, $U_2$ and NOMA system deteriorates. Another observation is that the curves with different power allocation coefficient have the same plots. The SOP of both $U_1$, $U_2$ and NOMA system is not affected with the adjustment of $\alpha_1$. This confirms the conclusion in Fig. 4.

Fig. 6 investigates the impact of the power allocation coefficient $\alpha_1$ on the SOP with the PIC mode of the Eve. Note that this power allocation coefficient must be between 0 and 0.5. We can observe that the SOP of user $U_2$ and NOMA system increases quickly as increasing coefficient $\alpha_1$. It is because when the power allocation coefficient $\alpha_1$ increases, the SINR of $U_2$ decreases more quickly than the SNR at the Eve (base on (8) and (10)). This leads to a decrease of the secrecy capacity of $U_2$. It means that the SOP of $U_2$ and NOMA system increase.

Fig. 7 shows the impact of the number of antennas of the Eve on the SOP. It is clear that the SOP of system in both SIC and PIC mode increases as the number of antennas of Eve increases. This is due to that the higher number of the antennas lead to the higher diversity gain at the Eve.
FIGURE 7. Impact of the number of antennas of Eve on the SOP of NOMA system where \( \Omega_1 = 200, \Omega_2 = 100, \) and \( \Omega_e = 2. \)

Fig. 8 illustrates the relationship between the average transmission time of NOMA system and the transmit SNR. We see that the average transmission time from the BS to \( U_1 \) is lower than the one from the BS to \( U_2. \) This is due to the fact that mean channel gain of \( U_1 \) better than that one of \( U_2. \)

Fig. 9 illustrates the effects of the power allocation coefficient \( \alpha_1 \) on the average transmission time from the BS to \( U_1 \) and \( U_2. \) It is observed that there is an \( \alpha_1 \) that makes the average transmission time from the BS to \( U_1 \) and \( U_2 \) is the same, i.e., \( \alpha_1^*. \) With initialized value is \( 10^{-3} \), desirable accuracy \( \sigma = 10^{-5}, \) increasing step \( \xi = 10^{-3}, \alpha_1^* \) is approximately 0.035.

Fig. 10 plots the impact of the transmit SNR on the packet timeout probability of both \( U_1 \) and \( U_2. \) We can see that the packet timeout probability of both users decreases when the transmit SNR of the BS increases. This is due to the fact that the transmit SNR increases to induce a higher transmission rate and thus the transmission time of packet decreases. On the other hand, the packet timeout probability reduces very fast in the high regime of the transmit SNR of about \( \text{SNR} \geq 14 \text{ dB}. \) This is because the packet transmission time decreases as the increasing the transmit SNR.

IX. CONCLUSION

In this paper, we investigated the secrecy performance and the fairness of packet transmission time for a power domain NOMA system in the presence of an Eve. In particular, an Eve is considered in two working modes: PIC and SIC. Accordingly, the secrecy performance in terms of the SOP of each user and NOMA system for both of PIC and SIC modes of the Eve has been conducted over Rayleigh fading channel. In addition, the expression of the average packet transmission time from the BS to \( U_1 \) and \( U_2 \) as well as the packet timeout probability is derived to evaluate the fairness of system. Accordingly, the optimal power allocation coefficient of \( U_1 \) algorithm for guaranteeing the fairness of packet transmission time is proposed. We verified the correctness of our analysis by using Monte Carlo simulations. The numerical results
indicate that the SOP of each user as well as a NOMA system for SIC mode of the Eve significantly outperforms that for PIC mode of the Eve and the system achieves the fairness of packet transmission time with proposed power allocation coefficient.

REFERENCES

[1] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, “A survey of non-orthogonal multiple access for 5G,” IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.
[2] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA),” in Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), London, U.K., Sep. 2013, pp. 611–615.
[3] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, “Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges,” IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 712–742, 2nd Quart., 2017.
[4] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and I. Xu, “Multi-user shared access for Internet of Things,” in Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring), Nanjing, China, May 2016, pp. 1–5.
[5] H. Nikpour and H. Baligh, “Sparse code multiple access,” in IEEE Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), London, UK, Sep. 2013, pp. 332–336.
[6] R. Hoshyar, F. P. Wathan, and R. Tafazoli, “Novel low-density signature for synchronous CDMA systems over AWGN channel,” IEEE Trans. Signal Process., vol. 56, no. 4, pp. 1616–1626, Apr. 2008.
[7] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[8] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical layer security of TAS/MRC with antenna correlation,” IEEE Trans. Info. Forensics Security, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[9] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical-layer security in cooperative wireless networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[10] 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.
[11] 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, Dec. 2013.
[12] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, “Secrecy sum rate maximization in non-orthogonal multiple access,” IEEE Commun. Lett., vol. 20, no. 5, pp. 930–933, May 2016.
[13] Z. Guo, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, “Physical layer security for 5G non-orthogonal multiple access in large-scale networks,” in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[14] 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. Wireless Commun., vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[15] O. Abbasi and A. Ebrahimii, “Secrecy analysis of a NOMA system with full duplex and half duplex relay,” in Proc. Iran Workshop Commun. Inf. Theory (IWCI), Tehran, Iran, May 2017, pp. 1–6.
[16] T. C. M. Chu and H. J. Zepernick, “Outage probability and secrecy capacity of a non-orthogonal multiple access system,” in Proc. 31st Int. Conf. Signal Process. Commun. Syst. (ICSPCS), Gold Coast, QLD, Australia, Dec. 2017, pp. 1–6.
[17] C. Liu, L. Zhang, M. Xiao, Z. Chen, and S. Li, “Secrecy performance analysis in downlink NOMA systems with cooperative full-duplex relaying,” in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), Kansas City, MO, USA, May 2018, pp. 1–6.
[18] B. He, A. Liu, N. Yang, and V. K. N. Lau, “On the design of secure non-orthogonal multiple access systems,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2196–2206, Oct. 2017.
[19] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, “On secure NOMA systems with transmit antenna selection schemes,” IEEE Access, vol. 5, pp. 17450–17464, 2017.
[20] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, “On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming,” IEEE Trans. Commun., vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

TUNG PHAM HUU received the B.S. degree in information technology from Vietnam National University, Hanoi, in 2002, and the M.S. degree in information technology from Moscow State University, in 2005. He is currently pursuing the Ph.D. degree with the Department of Computer Networks and Communications, Faculty of Information and Technology, Vietnam National University. Since 2007, he has been with the National University of Civil Engineering, Hanoi, Vietnam. His research interests include physical layer security, non-orthogonal multiple access networks, and cognitive radio networks.
TAM NINH THI-THANH received the bachelor’s degree in applied mathematics and informatics, in 2006, and the master’s degree from Hanoi University of Science, Vietnam National University (VNU), Vietnam, in 2009. She is currently a Lecturer with the Faculty of Information Technology, National Academy of Education Management (NAEM), Vietnam. Her research interests include wireless communication, physical-layer security, reliable communication, and communications theory.

CHI NGUYEN-YEN received the B.S. degree in electronics and telecommunications engineering from the University of Transport and Communications, Hanoi, Vietnam, in 2011, and the M.S. degree in telecommunication engineering from the Hanoi University of Science and Technology, in 2016. She has been with the University of Transport and Communications, since 2011. Her research interests include non-orthogonal multiple access in 5G systems, physical layer security in wireless communications, underwater communications, and visible light communication.

HUNG TRAN received the B.S. and M.S. degrees in information technology from Vietnam National University, Vietnam, in 2002 and 2006, respectively, and the Ph.D. degree from the Blekinge Institute of Technology, Sweden, in March 2013. In 2014, he was with the Electrical Engineering Department, ETS, Montreal, Canada. In 2015, he was a Postdoctoral Researcher with Mälardalen University, Sweden. In February 2020, he joined Phenikaa University, Vietnam, as a Researcher. His research interests include cognitive radio networks, cooperative communication, physical layer security for wireless communication, wireless power transfer, and non-orthogonal multiple access communication.

VIET NGUYEN DINH (Member, IEEE) received the B.Sc. degree in radio physics from Hanoi University, in 1976, the M.Sc. degree in science from the University of Natural Sciences, Vietnam National University (VNU), and the Ph.D. degree from the University of Engineering and Technology (UET), VNU, in 2004. He has been an Associate Professor, since 2007. He is currently a Senior Lecturer with the Faculty of Information Technology, UET, VNU. His current research interests include wireless mobile ad hoc networks, wireless sensor networks, quality of service guaranteeing for multimedia communication, and network simulation.

VAN NHAN VO received the B.S. degree in computer science from the University of Da Nang, in 2006, and the M.S. degree in computer science from Duy Tan University, Danang, Vietnam, in 2014. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Faculty of Science, Khon Kaen University, Thailand. Since 2009, he has been with Duy Tan University. His research interests include information security, physical layer secrecy, RF-EH, wireless sensor networks, and the security of other advanced communication systems. He is a member of the Cisco Systems, the Juniper Systems, and ComPTIA Systems.