On the Secrecy Outage Probability of NOMA Systems Affected by Imperfect SIC over κ−μ Fading Channels

Adrián S. Arias[1], Leidy C. Huera[1], Brandon S. Rueda[1], Henry R. Carvajal[1], Nathaly V. Orozco [1,*], and Fernando D. Almeida[2]
[1] Universidad de Las Américas (UDLA), Faculty of Engineering and Applied Sciences (FICA), Quito 170503, Ecuador; Email: {adrian.arias, leidy.huera, brandon.rueda, henry.carvajal, nathaly.orozco}@udla.edu.ec
[2] University of Campinas (UNICAMP), School of Electrical and Computer Engineering, Campinas 13083-852, Brazil; Email: ferdaral@decom.fee.unicamp.br
* Correspondence: nathaly.orozco@udla.edu.ec

***Abstract*—Fifth-generation (5G) and beyond fifth-generation (B5G) wireless systems increase the transmission capabilities of simple devices, such as Internet of Things (IoT) devices. However, they are vulnerable to eavesdropping attacks due to their low computational processing capacity. Thus, physical layer security (PLS) appears as an interesting alternative essential for their proper operation. In this work, the secrecy performance of power-domain non-orthogonal-multiple-access (NOMA) systems affected by imperfect successive interference cancellation (SIC) is evaluated in a scenario consisting of two users operating over κ−μ fading channels. By considering that the user furthest from the base station (BS) is an untrusted user, expressions to calculate the signal-to-noise-plus-interference ratio (SNIR) of both users are derived, and with these results, an expression to evaluate the secrecy-outage-probability (SOP) for the trusted user is derived. Numerical results using Monte-Carlo simulations are carried out in some scenarios to validate the derived expressions. The results also evidence a simple strategy to minimize the SOP for the trusted user based on the κ and μ fading parameters.**

***Keywords*—NOMA, physical-layer-security, κ-μ fading, secrecy-outage-probability**

I. Introduction

Network capacity and coverage are key elements for fifth-generation (5G) systems. However, security capabilities must also be incorporated in the standardization of these new wireless systems architectures mainly due to the appearance of various internet of things (IoT) devices with low computational processing capacity, which cannot use complex encryption algorithms [1−3]. In this sense, security requirements must overlap and penetrate through the different layers of a wireless systems, that is, it is not enough to guarantee security over the network or the application layers in the Open Systems Interconnection (OSI) model. Then, it is necessary to ensure security even in the physical layer of the communication system [4, 5].

IMT-2020 standard establishes that up to 1 million devices will connect to wireless networks every square kilometer [6]. This leads to the search for new multiuser transmission/reception strategies. As a result, a proposal called non-orthogonal multiple access (NOMA) appears as an option to allow several users to transmit simultaneously over the same radio resource [7−10]. In particular, when a different transmission power is allocated to each user, the scheme is known as power domain NOMA [11], which implements successive interference cancellation (SIC) at the User Equipment (UE) receivers for subtracting the undesired received signals until the signal of interest is obtained [12]. Some works assume that SIC performs perfectly [13, 14]. However, it does not occur in practical scenarios since residual interference appears in electronic components of NOMA receivers. Hence, a realistic analysis must consider the existence of residual interference, given by the implementation of imperfect SIC [15].

Some works have evaluated the performance of power domain NOMA systems in presence of Rayleigh fading channels [16−19]. However, it is well-known that 5G wireless networks also operate at millimeter wave frequencies. In this scenario, the Rayleigh distribution does not emulate adequately the behavior of the fading channel [20, 21]. Therefore, other statistical models can be used to emulate millimeter waves fading behavior. One of these alternatives is the κ−μ distribution [22, 23], which models scenarios composed of clusters of multipath waves propagating in a non-homogeneous environment. In addition, this model assumes that the clusters of multipath waves have scattered waves with identical powers, but, within each cluster, a dominant component is found, which presents an arbitrary power. Moreover, this distribution allows modeling other simpler scenarios, among which we can include Rayleigh and Rician fading [24].

Recently, a new field of research has been opened in the literature related to the analysis of physical-layer-security (PLS) in NOMA systems [10, 25, 26]. In particular, PLS

Manuscript received August 12, 2022; revised October 12, 2022, accepted January 18, 2023.

takes advantage of the random nature of the transmission channel, ensuring confidentiality and authentication aspects for the wireless communication with a computational cost much lower than encryption and security algorithms used in higher layers of the OSI model [27]. Nevertheless, an aspect that has been considered recently is the fact that spectrum sharing and SIC in power-domain NOMA generates secrecy challenges because untrusted users can decode the information of trusted users since the information of these users is transmitted over the same radio resource. In addition, the presence of imperfect SIC at the receivers creates the opportunity for eavesdroppers to decode information from residual interference.

Based on the above, PLS emerges as an alternative to solve security problems in power-domain NOMA systems.

In the literature, there are some works that address this scenario. For instance, in [28], PLS for NOMA is analyzed using random spatial patterns considering assisted transmission scenarios for single antenna systems, as well as multiple antenna systems. In [29], a scheme capable of improving PLS is proposed by means of full-duplex retransmission assisted by NOMA-artificial-noise. In [30], in order to protect the information of users assisted by NOMA, a secrecy beamforming scheme is proposed. In all these studies, perfect SIC at the receivers and Rayleigh fading are considered. Moreover, there are also works focused on the performance and optimization of PLS for NOMA in presence of external eavesdroppers or relay nodes [31, 32]. However, a few works consider that the eavesdropper can be one of the users served by a same base station (BS). For instance, ElHalawany and Wu [33] addresses this scenario and analyzes the performance in terms of the Secrecy Outage Probability (SOP), but considering receivers performing perfect SIC. In [34], it is considered the existence of an internal untrusted user and a cooperative blocker is used for generating artificial noise that prevents the eavesdropper from retrieving sensitive information [35]. In [36], when investigating secure transmissions in NOMA systems with untrusted nearby users, the authors propose a joint scheme of beam formation and power allocation along with artificial noise to improve the SOP. In addition, in [37], the authors deal with the random deployment of users and intruders to minimize the SOP. More specifically, a protected zone around the source node is adopted to enhance the security of the network.

As evidenced, one of the most employed parameters to evaluate the secrecy performance is the SOP, which is defined as the probability that the secrecy capacity is below a given threshold value [38, 39]. The secrecy capacity is defined as the channel capacity obtained with the trusted user signal-to-noise-plus-interference ratio (SNIR) minus the channel capacity obtained with the untrusted user's SNIR. In addition, the higher the given threshold, the greater the protection of the information. Moreover, the lower the SOP, the greater the protection of the information. Thus, the SOP concept comes from the analysis of channel capacity performed by the scientist Claude Shannon, known as the father of the information theory [40].

Motivated by the fact that security in the physical layer of NOMA systems has not been previously analyzed in generalized fading channels, in this work we consider the downlink of power domain NOMA systems in a cellular system composed of a trusted user and an untrusted one (eavesdropper), where transmissions are performed over a κ-μ fading channel, which is shown to be quite suitable for modeling fading in millimeter wave scenarios. We assume that the fading of both user are independent but not necessarily identically distributed (i.n.i.d). As a consequence, the parameters κ and μ can be different for each user. Thus, in this work we evaluate the network security based on the impact that these parameters have on the SOP of the trusted user. In addition, in order to emulate a practical scenario, imperfect SIC at both receivers is considered. In this sense, the main contributions of this work are:

- Expressions for the SNIR of both user are derived. Then, expressions to calculate the achievable rate capacity are obtained.
- An expression to evaluate the SOP of the trusted user is obtained, which is validated employing Monte-Carlo simulations in some representative scenarios.
- Numerical results evidence a user matching strategy in NOMA systems based on the κ and μ fading parameters for guaranteeing security for the user that is close to the BS.

The remaining sections are organized as follows. The list of symbols is shown in Section II. Section III describes the system model, where we also describe the structure of the received signals. In Section IV, we first derive an expression to calculate the achievable rate for the trusted and untrusted users. Then, the SOP is calculated. Numerical results are carried out in Section V. Finally, Section VI presents the main conclusions of this work.

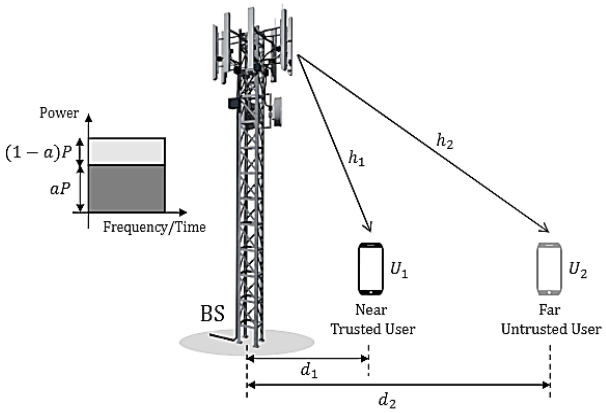

Figure 1. NOMA downlink communication with two users.

II. List of Symbols

Table I shows the list of the symbols used in this paper.

TABLE I. LIST OF SYMBOLS AND NOTATION

Symbol	Connotation
a	power allocation coefficient in the NOMA system
b_i	imperfect SIC level at the i-th receiver
c	parameter to modify the mean fading power
d_i	distance between the BS and the i-th user
h	channel gain
n_i	noise sample at the i-th receiver
s_i	complex symbol transmitted by the i-th user
x	signal transmitted by the BS
y_i	signal received by the i-th user
$I_v(.)$	modified Bessel function of the first type and order v
N_0	unilateral noise power spectral density
P	total power available at the base station
T_s	symbol duration
U_i	i-th user in the NOMA system
$\gamma_{1,1}$	instantaneous SNIR for U_1 trying to decode its own signal
$\gamma_{2,1}$	instantaneous SNIR for U_2 trying to decode the signal of U_1
ϕ	random phase
ρ	fading amplitude
σ_n^2	noise variance
σ_s^2	mean power of the symbols constellation
$(.)^*$	complex conjugate
$\|.\|$	norm
P[.]	probability operator
E[.]	expectation
Var[.]	variance
$\mathbb{C}$	set of complex numbers
$f(x)$	probability density function (PDF) of the random variable x
j	imaginary unit, $j = \sqrt{-1}$

III. SYSTEM AND CHANNEL MODELS

In this section, the system and channel models are presented. For this, the structure of the received signals is also obtained.

Consider a downlink NOMA system with two users. Thus, there are three nodes in the system as shown in Fig. 1, where the trusted user (U_1) is closer to the BS and the untrusted user (U_2) is the user further away. Moreover, $h_i = \rho_i \exp(j\phi_i)$ denotes the i-th complex channel coefficients, where ρ_i is the κ-μ fading envelope and ϕ_i is a random phase. The PDF for a κ-μ random variable with normalized mean power is given by [24, Eq. (1)]

$$f(\rho) = \frac{2\mu(1+\kappa)^{\frac{\mu+1}{2}}}{\kappa^{\frac{\mu-1}{2}}\exp(\mu\kappa)}\rho^{\mu}\exp(-\mu(1+\kappa)\rho^2) \times I_{\mu-1}\left(2\mu\sqrt{\kappa(1+\kappa)}\rho\right), \rho \geq 0, \quad (1)$$

where κ is defined as the ratio between the total power of the dominant components and the total power of the scattered waves, $\mu = \frac{1}{Var[\rho^2]}\frac{1+2\kappa}{(1+\kappa)^2}$ and I_v is the modified Bessel function of the first type and order ν [41, Eq. (9.6.20)].

Moreover, in Fig. 1, d_i is the distance between the BS and the i-th user. Thus, the BS simultaneously sends signals to both users in the same radio resource resulting in the overlapping of the signals. In the receivers of both users, a practical imperfect SIC is implemented. In addition, since $d_1 \leq d_2$, we also consider that $E[\rho_2^2] = cE[\rho_1^2]$, where $0 < c \leq 1$.

Based on the NOMA criterion, for U_1 is assigned a lower power because it is closer to the BS, while for U_2 is assigned a higher power because it is farther from the BS. Therefore, the BS sends two superimposed signals employing different power allocation levels. Thus, let aP be the power allocated to U_1, such that $0 \leq a \leq 0.5$, where a is a power allocation coefficient and P is the total power available at the BS. Consequently, the power allocated to U_2 is $(1-a)P$. By the above, the signal transmitted by the BS can be written as

$$x = \sqrt{aP}s_1 + \sqrt{(1-a)P}s_2, \quad (2)$$

where s_i, for $i = 1, 2$, is the complex symbol transmitted by the i-th user belonging to a constellation with mean power σ_s^2.

In a common scenario, where U_2 is a trusted user, it directly decodes its own signal taking the signal of U_1 as noise. However, in our system model, U_2 is an eavesdropper trying to recover U_1's signal.

In the following, consider that the SIC imperfection level at the receiver of the i-th user is represented by bi, for $i = 1,2$, such that $0 \leq b_i \leq 1$. Thus, for U_1, $b_1 = 0$ means that there is no residual interference, and consequently, perfect SIC is performed at the receiver of the trusted user. Otherwise, $b_1 = 1$ represents a completely imperfect SIC [42]. In the context of U_2, $b_2 = 0$ means that the eavesdropper can remove its own signal perfectly from the total received signal and therefore, only additive white Gaussian noise (AWGN) prevents it from properly detecting the trusted user information. Moreover, $b_2 = 1$ means that its own signal generates self-interference in the process of detecting the information of U_1. In addition, a coherent detection process is performed at the receivers, i.e, a phase compensation stage is applied. By the above, the signals received by U_1 and U_2 are respectively given by

$$y_1 = \left[\left(\sqrt{aP}s_1 + b_1\sqrt{(1-a)P}s_2\right)h_1 + n_1\right]\exp(-j\phi_1) \overset{(i)}{=} \left(\sqrt{aP}s_1 + b_1\sqrt{(1-a)P}s_2\right)\rho_1 + \tilde{n}_1, \quad (3)$$

$$y_2 = \left[\left(\sqrt{aP}s_1 + b_2\sqrt{(1-a)P}s_2\right)h_2 + n_2\right]\exp(-j\phi_2) \overset{(i)}{=} \left(\sqrt{aP}s_1 + b_2\sqrt{(1-a)P}s_2\right)\rho_2 + \tilde{n}_2, \quad (4)$$

where in step (i) we use that $h_i = \rho_i \exp(j\phi_i)$ and that $\tilde{n}_i = n_i \exp(-j\phi_i)$, where n_i denotes an AWGN sample that can be modeled as $\mathcal{CN}(0, \sigma_n^2)$, where

$$\sigma_n^2 = \frac{N_0}{T_s}, \quad (5)$$

is the noise variance, with N_0 being the unilateral noise power spectral density and Ts is the symbol duration. Consequently, $\tilde{n}_i \sim \mathcal{CN}(0, \sigma_n^2)$, for $i = 1, 2$.

$$\gamma_{1,1} = \frac{E\left[\left|\sqrt{aP}s_1\rho_1\right|^2 \middle| \rho_1\right]}{E\left[\left|b_1\sqrt{(1-a)P}s_2\rho_1 + \tilde{n}_1\right|^2 \middle| \rho_1\right]},$$
$$\overset{\text{(i)}}{=} \frac{E\left[(\sqrt{aP}s_1\rho_1)(\sqrt{aP}s_1\rho_1)^* \middle| \rho_1\right]}{E\left[\left(b_1\sqrt{(1-a)P}s_2\rho_1 + \tilde{n}_1\right)\left(b_1\sqrt{(1-a)P}s_2\rho_1 + \tilde{n}_1\right)^* \middle| \rho_1\right]}, \quad (6)$$
$$\overset{\text{(ii)}}{=} \frac{E\left[aP|s_1|^2\rho_1^2 \middle| \rho_1\right]}{E\left[b_1^2(1-a)P|s_2|^2\rho_1^2 + b_1\sqrt{(1-a)P}s_2\rho_1\tilde{n}_1^* + b_1\sqrt{(1-a)P}s_2^*\rho_1^*\tilde{n}_1 + |\tilde{n}_1|^2 \middle| \rho_1\right]}.$$

IV. Secrecy Performance Analysis

In this section, we first derive expressions to calculate the instantaneous SNIR[1] for U_1 trying to decode its own signal, denoted by $\gamma_{1,1}$, and then, we obtain an expression for the instantaneous SNIR of U_2 trying to decode the signal of U_1, named as $\gamma_{2,1}$. After that, expressions to calculate the achievable rates for U_1 and U_2 are obtained. Finally, an expression to evaluate the SOP for U_1 is derived.

A. Instantaneous SNIRs

From Eq. (3), the term $\sqrt{aP}s_1\rho_1$ corresponds to the signal of interest for U_1, while the other terms are considered as interference plus noise. With this in mind, $\gamma_{1,1}$ can be obtained as Eq. (6) located at the top of this page, where in step (i) we use that $|z|^2 = zz^*$ for $z \in \mathbb{C}$ and in step (ii) we use that $(z_1 z_2 \ldots z_n)^* = z_1^* z_2^* \ldots z_n^*$.

Then, using that $E[\tilde{n}_1] = E[\tilde{n}_1^*] = 0$, that $E[|\tilde{n}_1|^2] = \sigma_n^2$, that $E[|s_i|^2] = \sigma_s^2$, for $i = 1, 2$ and after some algebraic simplifications, (6) can be rewritten as

$$\gamma_{1,1} = \left[b_1^2\frac{(1-a)}{a} + \frac{\sigma_n^2}{aP\sigma_s^2\rho_1^2}\right]^{-1}. \quad (7)$$

Finally, with the aid of Eq. (5) and using that the energy per symbol is $E_s = P\sigma_s^2 T_s$, the instantaneous SNIR $\gamma_{1,1}$ can be rewritten as

$$\gamma_{1,1} = a\left[b_1^2(1-a) + \frac{N_0}{E_s}\frac{1}{\rho_1^2}\right]^{-1}. \quad (8)$$

Similarly, from Eq. (4), the term $\sqrt{aP}s_1\rho_2$ contains the information of interest for the eavesdropper, that is, the information sent to U_1, and the remaining terms can be considered as interference plus noise. Thus, $\gamma_{2,1}$ can be obtained as

$$\gamma_{2,1} = \frac{E\left[\left|\sqrt{aP}s_1\rho_2\right|^2 \middle| \rho_2\right]}{E\left[\left|b_2\sqrt{(1-a)P}s_2\rho_2 + \tilde{n}_2\right|^2 \middle| \rho_2\right]}. \quad (9)$$

By employing a procedure similar to that used in Eqs. (6–8) and after performing some algebraic simplifications, $\gamma_{2,1}$ can be calculated as

$$\gamma_{2,1} = a\left[b_2^2(1-a) + \frac{N_0}{E_s}\frac{1}{\rho_2^2}\right]^{-1}. \quad (10)$$

B. Achievable Rates

Since the received signals are affected by AWGN, from [40] and Eq. (8), the achievable rate for U_1 trying to decode his own signal can be obtained as

$$\mathcal{C}_{1,1} \triangleq \log_2(1+\gamma_{1,1})$$
$$= \log_2\left(1 + a\left[b_1^2(1-a) + \frac{N_0}{E_s}\frac{1}{\rho_1^2}\right]^{-1}\right) \quad (11)$$

Similarly, from Eq. (10), the achievable rate of U_2 trying to decode the information of U_1 is given by

$$\mathcal{C}_{2,1} \triangleq \log_2(1+\gamma_{2,1})$$
$$= \log_2\left(1 + a\left[b_2^2(1-a) + \frac{N_0}{E_s}\frac{1}{\rho_2^2}\right]^{-1}\right). \quad (12)$$

C. Secrecy Outage Probability

The non-negative secrecy capacity of U_1 is given by

$$\mathcal{C}_1 = \left[C_{1,1} - C_{2,1}\right]^+, \quad (13)$$

where $[x]^+ = max(x, 0)$. Finally, with this result, the SOP of U_1 is obtained as

$$SOP = P(\mathcal{C}_1 \leq R), \quad (14)$$

where R represents the secrecy target rate.

Assuming that $C_{1,1} - C_{2,1}$ is always a positive real number, from Eqs. (11–13), the SOP can be rewritten as

$$SOP = P\left(\frac{x_{1,1}}{x_{2,1}} \leq 2^R\right), \quad (15)$$

where

$$x_{i,1} = 1 + \gamma_{i,1}, \quad (16)$$

and we have used that $\log_2 y - \log_2 z = \log_2 y/z$ and $\gamma_{1,1}$ and $\gamma_{2,1}$ are given by Eq. (8) and Eq. (10), respectively. By performing a transformation of variables and some algebraic manipulations, from Eq. (1), Eq. (8) and Eq. (10), it is possible to show that the PDF of $x_{i,1}$ is given by

[1]With instantaneous SNIR we refer to the SNIR conditioned on the instantaneous value that assumes ρ_1 or ρ_2, as appropriate.

$$f(x_{i,1}) = \frac{\mu}{a\exp(\mu\kappa)}\Big[1 + (1-a)b_i^2\omega_{x,i}\Big]^2\left(\frac{\omega_{x,i}}{\kappa}\right)^{\frac{\mu-1}{2}}\left[\frac{1+\kappa}{\delta_i}\frac{N_0}{E_s}\right]^{\frac{\mu+1}{2}} \times \exp\left(-\mu\frac{1+\kappa}{\delta_i}\frac{N_0}{E_s}\omega_{x,i}\right) I_{\mu-1}\left(2\mu\sqrt{\kappa\frac{1+\kappa}{\delta_i}\frac{N_0}{E_s}\omega_{x,i}}\right) \quad (17)$$

for $1 \le x_{i,1} \le 1 + a[b_i^2(1-a)]^{-1}$, where

$$\omega_{x,i} = \left[\frac{a}{x_{i,1}-1} - (1-a)b_i^2\right]^{-1}, \quad (18)$$

and

$$\delta_i = \begin{cases} 1, & i = 1 \\ c, & i = 2. \end{cases} \quad (19)$$

Finally, from Eqs. (15–17), the SOP can be calculated as

$$\text{SOP} = \int_1^{1+a[b_2^2(1-a)]^{-1}} \int_1^{x_{2,1}2^R} f(x_{1,1})dx_{1,1}\, f(x_{2,1})dx_{2,1}, \quad (20)$$

which, unfortunately, does not generate a closed-form expression, but can be easily evaluated via numerical integration employing mathematical software.

The above expression can be reduced to the calculation of only one integral when perfect SIC exists in the NOMA system. In this scenario, $b_1 = b_2 = 0$, consequently, $\gamma_{1,1}$ and $\gamma_{2,1}$, which are given respectively by Eq. (8) and Eq. (10), can be simplified to

$$\gamma_{1,i} = a\frac{E_s}{N_0}\rho_i, \quad (21)$$

for i=1, 2. Assuming that $\gamma_{1,i} \gg 1$, which is a valid assumption in the high SNR regime, and from (11)-(14), the SOP can be written as

$$\text{SOP} \approx P\left(\rho_1 \le \rho_2\sqrt{2^R}\right). \quad (22)$$

Since ρ_1 and ρ_2 are independent and identically distributed (i.i.d.) κ–μ random variables and because $E[\rho_2^2] = cE[\rho_1^2]$, Eq. (22) can be rewritten as

$$\text{SOP} \approx \int_0^\infty F\left(\sqrt{c2^R}\rho\right) f(\rho)d\rho, \quad (23)$$

where F(·) is the cumulative distribution function (CDF) of a κ–μ random variable, that is given by [24, Eq. (3)] and f (ρ) is given by Eq. (1).

V. Numerical Results and Discussions

In this section, the secrecy performance of the considered NOMA network is evaluated employing our derived expressions in some representative scenarios. In addition, Monte-Carlo simulations validate the accuracy of the expressions obtained. For simulation purposes, we use $\sigma_s^2 = 1$, R = 1 bps, and 5×10^7 realizations for the Monte-Carlo trials. In addition, the parameters associated with the fading channel, as well as the values of a, b_1, b_2 and c have been selected arbitrarily in such a way that the system behavior and the accuracy of the analytical modeling can be evidenced in different operating scenarios. In all the following figures, the theoretical results are obtained through the numerical integration of (20).

Fig. 2 shows the SOP as a function of the Es/N0, parameterized by b_2, considering $\kappa = 0.6$, $\mu = 3$, $a = 0.3$, $b_1 = 0.1$, and $c = 0.1$. In these first results, the fading channel affecting both users have the same κ and μ parameters. Observe that the SOP decreases as the E_s/N_0 increases, with is an expected result, except for the scenario $b_2 = 0.1$. In this case, the residual interference for the eavesdropper is low, and it can easily decode the information of the trusted as the SNR increases. Thus, notice that the SOP decreases for low SNR values, but it increases for high SNR values. On the other hand, when b_2 increases ($b_2 > 0.1$), the residual interference for the eavesdropper increases, and consequently, it cannot successfully decode the information of U_1. In this sense, it is desirable that the residual interference for U_2 is high for protecting the information transmitted by U_1. However, if in the NOMA network it is also desirable that U_2 decodes his information properly, additional mechanisms must be considered by the BS in order to protect the trusted user information and ensure that both users correctly decode his own information.

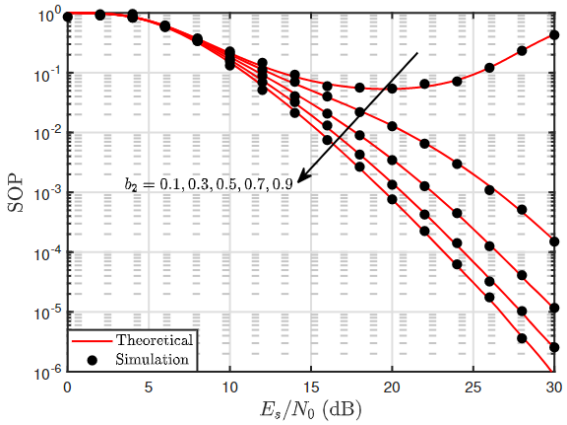

Figure 2. SOP as a function of the SNR, parameterized by b2, considering $\kappa = 0.6$, $\mu = 3$, a = 0.3, $b1 = 0.1$, and $c = 0.1$.

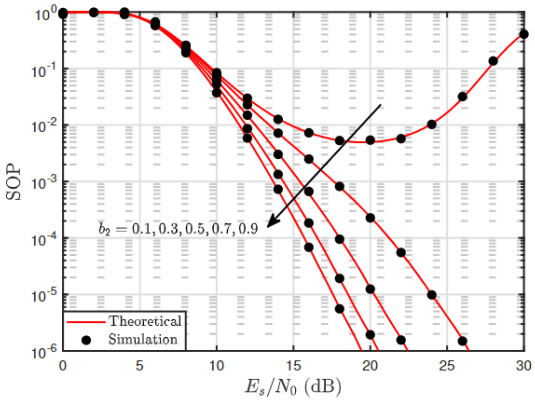

Figure 3. SOP as a function of the SNR, parameterized by b2, considering $\kappa = 1.2$, $\mu = 6$, $a = 0.3$, $b1 = 0.1$, and $c = 0.1$.

Fig. 3 is similar to Fig. 2, but in this case the parameters κ = 1.2, and μ = 6 are employed. When comparing both figures, it is noticed that a lower SOP is obtained in the last scenario, i.e, a higher security is guaranteed when the parameters κ and μ increase. Consequently, the SOP decays faster as the Es/N0 increases. From this, the fading channel parameters play a fundamental role in the security level of the trusted user. Thus, in practical scenarios where some radio resources are available in each cell, the BS could guarantee a given SOP for trusted users by assigning them radio channels where the κ and μ fading parameters are high. Obviously, this depends on the location of the users with respect to the BS and a proper channel estimation process is required.

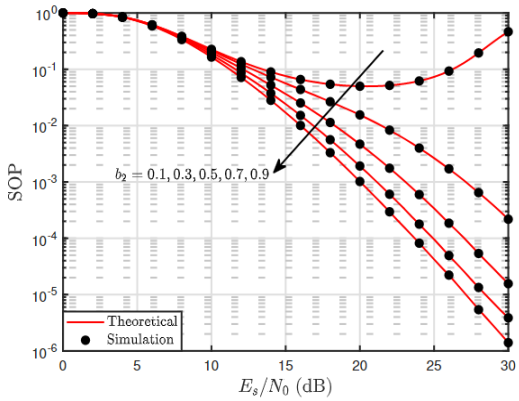

Figure 4. SOP as a function of the SNR, parameterized by b2, considering $\kappa 1$ = 0.3, $\kappa 2$ = 1.1, $\mu 1$ = 3, $\mu 2$ = 6, a = 0.3, $b1$ =0.1 and c = 0.1.

In the following, we evaluate a scenario where the users are affected by fading channels with different κ and μ parameters. Fig. 4 shows the SOP as a function of the E_s/N_0, parameterized by b_2, considering κ_1 = 0.3, κ_2 = 1.1, μ_1 = 3, μ_2 = 6, a = 0.3, b_1 = 0.1 and c = 0.1. Moreover, Fig. 5 shows the SOP as a function of the E_s/N_0, parameterized by b_2, considering κ_1 = 1.3, κ_2 = 0.2, μ_1 = 6, μ_2 = 3, a = 0.3, b_1 = 0.1 and c = 0.1. Notice that in Fig. 4 the parameters κ and μ are higher for the fading channel that affects U_2 and the opposite occurs in Fig. 5. When comparing the curves of both figures, it is clearly observed that when the trusted user is affected by a fading channel in which the κ and μ parameters are greater than those of the eavesdropper, then the SOP decays more rapidly as the SNR increases, which implies a scenario with more information security for the trusted user.

Fig. 6 shows the SOP as a function of the power allocation parameter, a, parameterized by b1, considering κ = 3.2 and μ = 3 for both users, it is also assumed Es/N0 = 20 dB, $b2$ = 0.3, and c = 0.1. In the figure, notice that when U_1 has a low SIC imperfection level ($0.05 \leq b1 \leq 0.2$) and as more power is allocated to this user, i.e., as a increases, the SOP decreases since U_1 can decode his signal more easily. However, notice that if a is increases too much, then the SOP slightly increases. This is because high values of a help the eavesdropper to decode the trusted user signal, which increases the eavesdropper capacity.

In addition, observe that as b_1 increases, the SOP also increases because the residual interference increases in the receiver of the trusted user, which reduces its rate, that is given by Eq. (11).

Finally, Fig. 7 is similar to Fig. 6, but in this case, the parameter c = 0.4 is used. When comparing these figures, notice that the SOP worsens as c increases. In particular, as c increases, we can assume that the eavesdropper gets closer to the BS, which allows him to receive the trusted user's signal with greater power, and therefore, U_2 decodes it more easily, which is translated into a higher SOP.

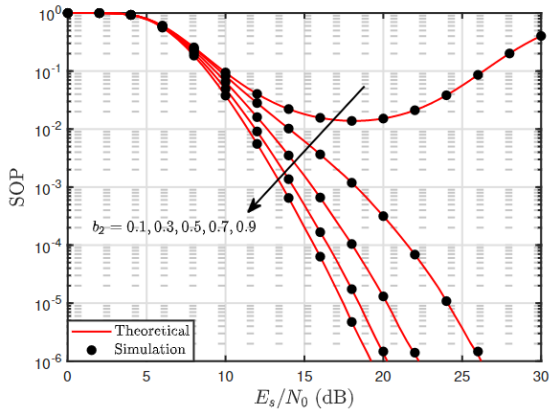

Figure 5. SOP as a function of the SNR, parameterized by b2, considering $\kappa 1$ = 1.3, $\kappa 2$ = 0.2, $\mu 1$ = 6, $\mu 2$ = 3, a = 0.3, $b1$ = 0.1 and c = 0.1.

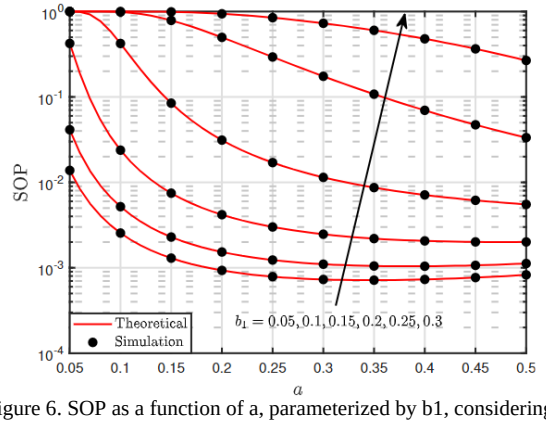

Figure 6. SOP as a function of a, parameterized by b1, considering Es/N0 = 20 dB, $b2$ = 0.3, c = 0.1, κ = 3.2, and μ = 3.

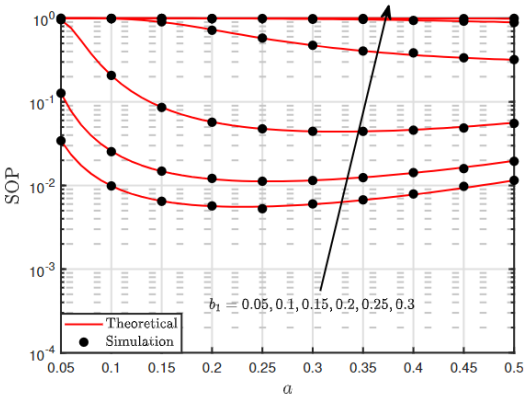

Figure 7. SOP as a function of a, parameterized by b1, considering Es/N0 = 20 dB, $b2$ = 0.3, c = 0.4, κ = 3.2, and μ = 3.

Another aspect to ensure security for the trusted user is related with the amount of power allocated to each user. Thus, a high power allocated to the trusted user can

become beneficial for the eavesdropper, who can decodes the trusted user's information in a more reliable way, which translates into a higher SOP. Therefore, it is important that the BS assigns the trusted user a radio channel in which κ and μ fading parameters allow guaranteeing an adequate SOP without increasing the power assigned to this user too much.

Finally, there are other generalized distributions in the literature to model the fading phenomenon in millimeter wave scenarios like α–μ or η–μ [22]. Thus, these distributions can also be considered for future research.

VI. Conclusion

In this work, we analyze the secrecy performance of downlink NOMA systems in presence of imperfect SIC at the receivers of two users over a generalized κ-μ fading channel. For this, we obtain expressions to evaluate the achievable rates of a trusted user near to the BS and an eavesdropper farther away from the BS. With these results, an expression to evaluate the SOP for the trusted user is obtained.

Numerical results show that the information of the trusted user is decoded more effectively by the eavesdropper when it has low imperfect SIC levels. However, as the imperfect SIC levels at the eavesdropper receiver increase, the SOP decays more rapidly as the SNR increases since the transmission capacity of the eavesdropper decreases due to high residual interference. Moreover, it is observed that when the trusted user is affected by a fading channel in which κ and μ parameters are greater than those of the eavesdropper, the SOP decays more rapidly as the SNR increases. Therefore, this is an easy user matching strategy which can be employed by the BS in NOMA systems for guaranteeing security to users who are close to the BS.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, H. Carvajal and N. Orozco; methodology, H. Carvajal and N. Orozco; software, H. Carvajal, A. Arias, L. Huera and B. Rueda; validation, H. Carvajal, N. Orozco and F. Almeida; formal analysis, H. Carvajal, A. Arias, L. Huera and B. Rueda; investigation, H. Carvajal, N. Orozco, A. Arias, L. Huera, B. Rueda and F. Almeida; data curation, H. Carvajal and N. Orozco; writing—original draft preparation, H. Carvajal, N. Orozco, A. Arias, L. Huera, B. Rueda and F.A.; writing—review and editing, H. Carvajal, N. Orozco, A. Arias, L. Huera, B. Rueda and F. Almeida; visualization, H. Carvajal and N. Orozco; supervision, H. Carvajal; project administration and funding acquisition, H. Carvajal All authors have read and agreed to the published version of the manuscript.

References

[1] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A survey on IOT and 5G network," presented at Int. Conf. on Smart City and Emerg. Technology, Mumbai, India, Jan. 2018.

[2] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16-32, Jan. 2020.

[3] A. Mir, M. F. Zuhairi, S. Musa, T. A. Syed, and A. Alrehaili, "A Survey of security challenges with 5G-IoT," in *Proc. First Int. Conf. of Smart Systems and Emerging Technologies*, Riyadh, Nov. 2020, pp. 249-250.

[4] A. Dutta and E. Hammad, "5G security challenges and opportunities: a system approach," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India, Sep. 2020, pp. 109-114.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679-695, Apr. 2018.

[6] Y. Choi, J. Kim, and N. Park, "Revolutionary direction for 5G mobile core network architecture," in *Proc. Int. Conf. on Information and Comm. Tech. Convergence (ICTC)*, Jeju, South Korea, Oct. 2016, pp. 992-996.

[7] M. K. Hasan, *et al.*, "The role of deep learning in NOMA for 5G and Beyond Communications," Int. Conf. on Artificial Intelligence in Information and Communication (ICAIIC), pp. 303-307, Fukuoka, Japan, Apr. 2020.

[8] C. Frison, H. Carvajal, and C. D. Almeida, "MC-CDMA and SCMA performance evaluation in 100% and 200% load factor scenarios," presented at IEEE Fourth Ecuador Technical Chapters Meeting (ETCM), Guayaquil, Ecuador, Nov. 2019.

[9] M. Hassan, M. Singh, and K. Hamid, "Survey on NOMA and spectrum sharing techniques in 5G," presented at IEEE Int. Conf. on Smart Information Systems and Technologies, Nur-Sultan, Kazakhstan, Jun. 2020.

[10] H. T Madan and I. B. Prabhugoud, "Reliable and secrecy aware cooperative framework for cognitive radio non-orthogonal multiple access (NOMA) Networks," *Journal of Communications*, vol. 17, no. 2, pp. 125-133, Feb. 2022.

[11] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700-714, Jun. 2019.

[12] Z. Xiang, X. Tong, and Y. Cai, "Secure transmission for NOMA systems with imperfect SIC," *China Communications*, vol. 17, no. 11, pp. 67-78, Nov. 2020.

[13] F. J. ElHalawany, *et al.*, "Performance Analysis of downlink NOMA systems over κ-μ shadowed fading channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1046-1050, Jan. 2020.

[14] P. Sharma, A. Kumar, and M. Bansal, "Performance analysis of downlink NOMA over η–μ and κ–μ fading channels," *IET Commun.*, vol. 14, no 3, pp. 522-531, Feb. 2020.

[15] M. Sfredo, E. M. Garcia, and H. Carvajal, "Physical layer security in power-domain NOMA using improper Gaussian signals," presented at IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, Dec. 2021.

[16] M. A. Ahmed, A. Baz, and C. C. Tsimenidis, "Performance analysis of NOMA systems over rayleigh fading channels with successive-interference cancellation," *IET Commun.*, vol. 14, no 6, pp. 1065-1072, Apr. 2020.

[17] M. W. Baidas, E. Alsusa, and K. A. Hamdi, "Performance analysis of downlink NOMA networks over Rayleigh fading channels," presented at IEEE Wireless Comm. and Networking Conf., Barcelona, Spain, Jun. 2018.

[18] B. Panda and P. Singh, "Performance analysis of NOMA systems in rayleigh and Rician fading channels," *Advanced Comm. Technologies and Signal Processing (ACTS)*, Dec. 2021.

[19] D. Do, and M. Van Nguyen, "Exploring secrecy outage probability of AF-NOMA and AF-OMA networks," *Journal of Communications*, vol. 14, no. 7, pp. 538-543, Feb. 2019.

[20] P. Noren *et al.*, "Measurement and diagnostics of millimeter waves 5G enabled devices," presented at IEEE Conf. on Antenna Measurements & Applications (CAMA), Sweden, Nov. 2018.

[21] M. H. Mahmud, M. M. Hossain, A. A. Khan, S. Ahmed, M. A. Mahmud, and M. H. Islam, "Performance analysis of OFDM, W-OFDM and F-OFDM under rayleigh fading channel for 5G wireless communication," presented at 3rd Int. Conf. on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, Dec. 2020.
[22] T. R. R. Marins *et al*., "Fading evaluation in the mm-wave band," *IEEE Trans. Commun*, vol. 67, no. 12, pp. 8725-8738, Dec. 2019.
[23] J. Kibiłda, Y. J. Chun, F. Firyaguna, S. K. Yoo, L. A. DaSilva, and S. L. Cotton, "Performance evaluation of millimeter-wave networks in the context of generalized fading," presented at IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, Dec. 2018.
[24] M. D. Yacoub, "The κ−μ distribution and the η−μ distribution," *IEEE Antennas and Propagation Magazine*, vol. 49, no. 1, pp. 68-81, Feb. 2007.
[25] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, "Enhancing physical layer security with artificial noise in large-scale NOMA networks," *IEEE Trans. Veh. Technol*., vol. 70, no. 3, pp. 2349-2361, Mar. 2021.
[26] S. Huang, M. Xiao, and H. V. Poor, "On the Physical layer security of millimeter wave NOMA networks," *IEEE Trans. Veh. Technol*., vol. 69, no. 10, pp. 11697-11711, Oct. 2020.
[27] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347-376, Aug. 2016.
[28] 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.
[29] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks," presented at Proc. IEEE GLOBECOM Wkshps, Singapore, Dec. 2017.
[30] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol*., vol. 67, no. 7, pp. 6700-6705, Mar. 2018.
[31] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 210-222, Apr. 2019.
[32] P. Patel, "Improving of physical layer insecurity of the non orthogonal multiple access system," *Int. Journal of Scientific and Technology Research*, vol. 9, issue 04, Apr. 2020.
[33] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," presented at IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, Dec. 2018.
[34] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G noma systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13005-13017, Aug. 2020.
[35] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over non-small-scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326-1339, Ma. 2016.
[36] K. Cao *et al.*, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930-2943, Mar. 2020.
[37] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," presented at IEEE Int. Conf. on Comm. (ICC), Kuala Lumpur, Malaysia, Jul. 2016.
[38] N. Yang, X. Zhou, J. Lee, and D. Gyeongbuk, "Safeguarding the 5G Era and beyond with physical layer wireless security," presented at IEEE Int. Conf. on Comm. (ICC), Tutorial, Daegu, South Korea, May 2019.
[39] D. Lee, "Secrecy outage probability of MIMO diversity schemes over integer and real-valued Nakagami fading channels," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 727-731, Apr. 2022.
[40] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.
[41] M. Abramowitz, and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, New York: Dover: Wiley-IEEE Press, 1972.
[42] I. A. Mahady *et al*., "Sum-rate maximization of NOMA systems under imperfect successive interference cancellation," *IEEE Commun. Lett*, vol. 23, no. 3, pp. 474-477, Mar. 2019.

Adrian S. Arias is an engineer in Electronics and Information Networks graduated from Universidad de las Américas (UDLA), Ecuador, in 2022, where he was part of various scientific dissemination projects as well as being immersed in competitions in which he demonstrated his passion for technological innovation. He is currently an IT Analyst and Developer at Tata Consultancy Services (TCS). His research interests are the applications of Artificial Intelligence as well as the development of systems that use these tools.

Brandon S. Rueda is an engineer in Electronics and Information Networks from the Universidad de Las Américas (UDLA). Ecuador, in 2022. He was engineer in PON technologies in MEGADATOS enterprise, Ecuador, 2022. He currently works as a backoffice in PROSOLUTIONS enterprise in Ecuador. He has worked on several projects related to telecommunications networks, mainly focused on the deployment of GPON networks. His research interests include digital communications (optical and wireless) and strategies to improve their performance and security.

Leidy C. Huera received the B.Sc. degree in Electronics and Information Networks at Universidad de Las Américas (UDLA), Ecuador, in 2022. She is currently working as an OnSite Information Security Analyst at SecureSoft, Ecuador. She has been part of several research and innovation projects related to electronics, telecommunications, and information technologies. Her research interests include IT developments oriented to improve the security of communication networks.

Henry R. Carvajal and received the B.Sc. degree in electronics and telecommunications engineering from the Armed Forces University-ESPE, Ecuador, with honors in 2009, and the M.Sc. and Ph.D. degrees in electrical engineering from the School of Electrical and Computer Engineering (FEEC), University of Campinas (UNICAMP), Brazil, in 2014 and 2018, respectively. He was Director of the technology transfer area in the Education, Science and Technology Secretariat (SENESCYT), Ecuador, 2018. He obtained the HCIA-5G certification from Huawei in 2020. He is currently Assistant Professor at Universidad de Las Américas (UDLA), Ecuador. His research interests are fading channels, diversity-combining systems, orthogonal and non-orthogonal multiple access, multiuser detection, MIMO, physical-layer security, 5G, and B5G technologies.

Nathaly V. Orozco received the Electronic and Telecommunications Engineering degree from Armed Forces University-ESPE, Sangolquí, Ecuador, in 2011, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Campinas (UNICAMP), Brazil, in 2014 and 2018, respectively. She is currently a Full Professor with the Universidad de Las Américas (UDLA), Quito, Ecuador. Her research interests include digital communications with specific emphasis on orthogonal and non-orthogonal multiple access, fading channels, MIMO, cognitive systems, opportunistic transmissions, and 5G and 6G technologies.

Fernando D. Almeida received the B.Sc. degree in electronics and telecommunications engineering from the Armed Forces University-ESPE, Quito, Ecuador, in 2012, and the M.Sc. and Ph.D. degrees in electrical engineering from the School of Electrical and Computer Engineering (FEEC), University of Campinas (UNICAMP), SP, Brazil, in 2015 and 2021, respectively. From 2014 to 2020, he worked together with Bradar Indústria S.A., a branch of Embraer Defense and Security, in the development of innovative radar signal processing techniques. Since 2021, he is a postdoctoral fellow with the Wireless Technology Laboratory (WissTek) at FEEC-UNICAMP. His research interests include radar systems, wireless communications, channel modeling, and digital signal processing.