Imperfect jamming cancellation on NOMA networks with randomly located eavesdroppers

G. M. da Silva*, D. P. Moya Osorio†, and M. Latva-aho†
*Department of Electrical Engineering, Federal University of São Carlos. São Carlos, Brazil
gustavomarques@estudante.ufscar.br
†Centre for Wireless Communications, University of Oulu. Oulu, Finland
[diana.moyaosorio, matti.latva-aho]@oulu.fi

***Abstract*—This paper addresses the secrecy performance of the downlink of a non-orthogonal multiple access network in the presence of multiple randomly located eavesdroppers. The network consists of a base station and a near receiver that are located inside a protected zone, free of eavesdroppers, while a far user is located outside. Herein, it is considered that the source transmits a superposed jamming signal to enhance the secrecy performance. In this sense, imperfections on the removal of the jamming signal by the legitimate receivers are also investigated. Integral-form exact and closed-form approximate expressions for the secrecy outage probability are derived by employing stochastic geometry tools. The expressions are corroborated via Monte Carlo simulations.**

***Index Terms*—Intentional jamming, non-orthogonal multiple access, physical layer security, stochastic geometry, successive interference cancellation.**

I. Introduction

THE emerging of sophisticated and stringent services for 5G and beyond (5GB) networks has imposed a huge necessity on the exploration of novel multiple-access techniques. Thus, non-orthogonal multiple access (NOMA), in power and code domain, have been proposed as interesting solutions for the challenges of 5GB [1]. Particularly, the power-domain NOMA allows to serve multiple users at the same resource block, thus attaining superior capacity than orthogonal multiple access (OMA) techniques. For that purpose, power-domain NOMA employs super-position coding (SC) techniques at the transmitter side and successive interference cancellation (SIC) at the receiver side [2].

Moreover, the massive deployments of new applications with heterogeneous devices makes 5GB networks more prone to security attacks. In this sense, novel solutions for safeguarding 5GB networks are of paramount importance. Recently, physical layer security (PLS) techniques have shown a great potential to complement cryptography-based solutions by efficiently exploiting the random characteristics of wireless channels in order to prevent the leakage of information to malicious nodes [3]. Different PLS techniques were tackled for the most diverse scenarios [4], [5]. For instance, the use of beamforming to maximise the security of a multiple-input-single-output (MISO) system was investigated in [4], by introducing the concept of protected zone as a form of preventing near eavesdroppers and for power saving purposes. Furthermore, in [5], a scheme was proposed in order to superpose a jamming signal with the information signal to improve the ergodic secrecy sum rate (ESSR) of an untrusted relay network.

Regarding NOMA systems, PLS techniques have been addressed in a number of works [6]–[9]. Particularly in [6], the SOP of the downlink of a NOMA network is derived by assuming a protected zone around the base station and randomly located legitimate users and eavesdroppers. The authors in [7] analyzed the effective secrecy throughput of the uplink in a NOMA system by considering randomly located legitimate users and eavesdroppers. On the other hand, jamming techniques were investigated in [8] and [9]. Specifically, a cooperative NOMA network is investigated in [8], where cooperative relays broadcast intentional jamming, simultaneously with the desired signal sent by the base station, in order to maximise the achievable secrecy rate. The authors in [9] derived the secrecy rate of a NOMA network, where the strong user serves as a relay to help the base station forward the weak user's signal, in the presence of an eavesdropper. Therein, it was considered that the base station broadcasts intentional jamming during the relay forwarding phase in order to increase the secrecy performance.

Herein, we analyze the secrecy outage probability in the downlink of a power-domain NOMA network. For this purpose, it is considered a base station trying to communicate with two legitimate users, while randomly located non-colluding eavesdroppers attempt to decode the information. Inspired by [4], it is assumed a protected zone around the source, free of eavesdroppers, where the nearest user is located. This assumption is aligned with practical deployments, where exists a restrict-access area, so that no eavesdropper can be located in that zone. Furthermore, it is considered that the base station is capable to allocate part of its power for the transmission of information and the rest of its power is employed for the transmission of intentional jamming, similar to the case in [5]. In this context, our goal is to evaluate the impact of an imperfect cancellation of the jamming signal at the legitimate

This work was partially supported by the Academy of Finland 6Genesis Flagship under Grant 318927 and FAITH project under Grant 334280, and by the São Paulo Research Foundation (FAPESP) under Grant 2019/14168-7

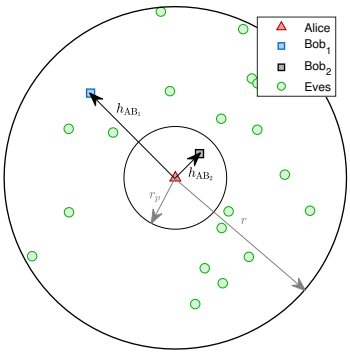

Fig. 1. System model for the NOMA network.

receivers. For the proposed system, integral-form exact and closed-form approximate expressions for the secrecy outage probability are derived by employing stochastic geometry tools and validated via Monte Carlo simulations.

Along the paper, the probability density function (PDF) and the cumulative distribution function (CDF) of a random variable (RV) X will be denoted as $f_X(x)$ and $F_X(x)$, respectively. Also, $\mathrm{E}\{\cdot\}$ denotes the expectation operator, $\Gamma(a,x) = \int_x^\infty t^{a-1}e^{-t}\mathrm{d}t$ denotes the incomplete gamma function, and $[z]^+ = \max\{z, 0\}$.

II. System Model

Consider the system illustrated in Fig. 1, where a base station so-called Alice (A) tries to communicate with two legitimate NOMA users so-called Bob_1 and Bob_2 (B_1 and B_2), so that B_1 is the user located far away from Alice and, consequently, B_2 is located near to Alice, inside a controlled geographical area of radius r_p, so-called protected zone, in which the probability of an eavesdropper located inside is null. Thus, randomly located and non-colluding eavesdroppers so-called Eves (E_i) are distributed by a homogeneous Poisson point process (hPPP) in a ring between r_p and r, where the hPPP is denoted by Φ_λ, with λ being the density of the process and $i \in \Phi_\lambda$. It is considered that the legitimate receivers operate in a NOMA basis, and all channels undergo independent Rayleigh block fading and additive white Gaussian noise (AWGN) with mean power N_0. Therefore, the channel coefficients are denoted by $h_{\mathrm{A}j} \sim \mathcal{CN}(0, \Omega_{\mathrm{A}j})$, and the channel gains by $g_{\mathrm{A}j} = |h_{\mathrm{A}j}|^2$, with $\Omega_{\mathrm{A}j} = \mathrm{E}\{g_{\mathrm{A}j}\} = d_{\mathrm{A}j}^{-\beta}$ being the average channel gain, $d_{\mathrm{A}j}$ is the distance between the respective nodes, β is the pathloss exponent, and $j \in \{\mathrm{B}_1, \mathrm{B}_2, \mathrm{E}_i\}$.

For the communication process, A first broadcasts, simultaneously, the information messages intended to B_1 and B_2, by considering a power-domain NOMA scheme, together with an intentional jamming signal, intended to improve the secrecy performance as in [5]. Thus that the transmitted signal at time t is given by

$$x(t) = \sqrt{\alpha\theta P}\; x_1(t) + \sqrt{(1-\alpha)\theta P}\; x_2(t) + \sqrt{(1-\theta)P}\; x_J(t), \tag{1}$$

where $x_1(t)$, $x_2(t)$ and $x_J(t)$ denote the information signals to B_1, B_2 and the intentional jamming signal, respectively. P is the total transmitting power at A, $0.5 < \alpha < 1$ is the power allocation factor according to NOMA scheme, and $\theta \in [0,1]$ is the power allocation factor for jamming and information signals. Then, the received signal at time t in node $j \in \{\mathrm{B}_1, \mathrm{B}_2, \mathrm{E}_i\}$ can be expressed as

$$y_j(t) = h_{\mathrm{A}j}\underbrace{\sqrt{\alpha\theta P}x_1(t)}_{\mathrm{B}_1\text{'s Signal}} + \underbrace{\sqrt{(1-\alpha)\theta P}x_2(t)}_{\mathrm{B}_2\text{'s Signal}} + \underbrace{\sqrt{(1-\theta)P}x_J(t)}_{\text{Jamming Signal}} + \underbrace{n_0}_{\text{Noise}}. \tag{2}$$

Herein, the jamming is generated by a pseudorandom noise generator, [10] then the jamming signal can be replicated at the legitimate receivers, giving them the ability of cancel the jamming. However, in this paper we consider that the users might fail on perfectly remove the intentional jamming, due to decoding errors and channel specifcs, causing a remaining residual interference (RI) at the user's received signal. Therefore, the instantaneous received signal-to-interference-plus-noise ratio (SINR) at B_1 is expressed as

$$\gamma_1 = \frac{\alpha\theta\gamma_p\; g_{\mathrm{AB}_1}}{(1-\alpha)\theta\gamma_p\; g_{\mathrm{AB}_1} + (1-\theta)\xi\gamma_p\; g_{\mathrm{AB}_1} + 1}, \tag{3}$$

where $\gamma_p = \frac{P}{N_0}$ is the transmit SNR and $\xi \in [0,1]$ is the RI level, i.e., the perfect intentional jamming cancellation occurs when $\xi = 0$.

On the other hand, B_2 employs SIC to first decode the information intended to B_1's, then it is able to decode its own information. Therefore, the corresponding instantaneous received SINRs γ_{21} relative to B_1's information and γ_{22} relative to B_2's information are, respectively, given by

$$\gamma_{21} = \frac{\alpha\theta\gamma_p\; g_{\mathrm{AB}_2}}{(1-\alpha)\theta\gamma_p\; g_{\mathrm{AB}_2} + (1-\theta)\xi\gamma_p\; g_{\mathrm{AB}_2} + 1}, \tag{4}$$

$$\gamma_{22} = \frac{(1-\alpha)\theta\gamma_p\; g_{\mathrm{AB}_2}}{(1-\theta)\xi\gamma_p\; g_{\mathrm{AB}_2} + 1}. \tag{5}$$

For the eavesdroppers, it is assumed that they perform SIC, but are unable to remove the jamming signal, so that the instantaneous received SINRs at E_i are denoted as $\gamma_{\mathrm{E}_i 1}$ relative to B_1's information and $\gamma_{\mathrm{E}_i 2}$ relative to B_2's information. Regarding that the eavesdroppers do not collude, we are interested on the instantaneous received SINRs of the eavesdropper with best channel conditions, which are, respectively, given by

$$\gamma_{\mathrm{E}1} = \max_{i\in\Phi_\lambda}[\gamma_{\mathrm{E}_i 1}] = \max_{i\in\Phi_\lambda}\left[\frac{\alpha\theta\gamma_p\; g_{\mathrm{AE}_i}}{\gamma_p\; g_{\mathrm{AE}_i}\left[(1-\alpha)\theta + (1-\theta)\right] + 1}\right], \tag{6}$$

$$\gamma_{\mathrm{E}2} = \max_{i\in\Phi_\lambda}[\gamma_{\mathrm{E}_i 2}] = \max_{i\in\Phi_\lambda}\left[\frac{(1-\alpha)\theta\gamma_p\; g_{\mathrm{AE}_i}}{(1-\theta)\gamma_p\; g_{\mathrm{AE}_i} + 1}\right]. \tag{7}$$

Considering this, the corresponding CDFs for the RVs expressed in (3), (4) and (5) can be obtained straightforwardly by isolating the respective channel gain from each equation, which follow an exponential distribution.

The CDF of γ_{E1} can be obtained from (6) as

$$\begin{aligned}
F_{\gamma_{\mathrm{E1}}}(\tau) &= \Pr\left(\gamma_{\mathrm{E1}} \leq \tau\right), \\
&= \Pr\left(\max_{i\in\Phi_\lambda}[g_{\mathrm{AE}_i}] \leq \tfrac{\tau}{\gamma_p[\alpha\theta-\tau(1-\alpha\theta)]}\right), \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_\lambda}\left[\prod_{i\in\Phi_\lambda}\left(1-e^{-\frac{\tau}{\gamma_p[\alpha\theta-\tau(1-\alpha\theta)]d_{\mathrm{AE}_i}^{-\beta}}}\right)\right] \\
&\overset{(b)}{=} \exp\left(-\lambda\int_0^{2\pi}\int_{r_p}^{r} e^{-\frac{\tau}{\gamma_p[\alpha\theta-\tau(1-\alpha\theta)]\rho^{-\beta}}}\,\rho\;\mathrm{d}\rho\mathrm{d}\phi\right), \\
&= \exp\left[-2\pi\lambda\left(\int_0^{r} e^{-k\rho^\beta}\,\rho\;\mathrm{d}\rho - \int_0^{r_p} e^{-k\rho^\beta}\,\rho\;\mathrm{d}\rho\right)\right], \\
&\overset{(c)}{=} \exp\left[-\tfrac{2\pi\lambda}{\beta}k^{-\frac{2}{\beta}}\left[\Gamma\left(\tfrac{2}{\beta},kr_p^\beta\right)-\Gamma\left(\tfrac{2}{\beta},kr^\beta\right)\right]\right], \quad (8)
\end{aligned}$$

where $k=\frac{\tau}{\gamma_p[\alpha\theta-\tau(1-\alpha\theta)]}$ and (a) is obtained considering that all g_{AE_i} are independent and identically distributed, hence it becomes a multiplication. Finally, we obtain the expectation of the hPPP.

Also, (b) is obtained by considering the following variable change $\rho{=}d_{\mathrm{AE}_i}$ and [11, Theo. 4.9].

Finally, (c) is obtained after mathematical manipulations and by considering [12, Eq. 3.326.4].

By defining $\Upsilon(k) = e^{-\frac{2\pi\lambda}{\beta}k^{-\frac{2}{\beta}}\left[\Gamma\left(\frac{2}{\beta},kr_p^\beta\right)-\Gamma\left(\frac{2}{\beta},kr^\beta\right)\right]}$ and following the above mentioned steps to find the CDF of the RV γ_{E2}, we can express the CDFs of γ_{E1} and γ_{E2} respectively, as

$$F_{\gamma_{\mathrm{E1}}}(\tau)=\Upsilon\left(\tfrac{\tau}{\gamma_p(\alpha\theta-\tau(1-\alpha\theta))}\right), 0<\tau<\tfrac{\alpha\theta}{1-\alpha\theta}, \quad (9)$$

$$F_{\gamma_{\mathrm{E2}}}(\tau)=\Upsilon\left(\tfrac{\tau}{\gamma_p(\theta(1-\alpha)-\tau(1-\theta))}\right), 0<\tau<\tfrac{\theta(1-\alpha)}{1-\theta}. \quad (10)$$

III. Secrecy Outage Probability

Given the definition of secrecy capacity [3] as the difference between the capacities of the legitimate and eavesdropping links, i.e. $C_{\mathrm{S}}=[C_B-C_{\mathrm{E}}]^+$, the secrecy outage probability (SOP) is traditionally defined as the probability of C_{S} being less than a target secrecy rate $R_{\mathrm{S}}>0$. However, this metric does not give a direct indication of the security level in the system, thus Zhou et al. proposed a new definition for SOP in [13], by conditioning the SOP to the likelihood of a successful transmission. Thus, given that exists a feedback from B to A, A can decide to transmit only when the legitimate link is reliable, i.e. γ_k exceeds some SNR threshold μ, where $\mu\geq 2^{R_{\mathrm{S}}}-1$. Taken this definition of SOP into consideration and defining $\tau_{\mathrm{S}}{=}2^{R_{\mathrm{S}}}$ as the security threshold, the SOP at B_1 and B_2 can be, respectively, formulated as

$$\mathrm{SOP}_1=\Pr\left(\frac{1+\gamma_1}{1+\gamma_{\mathrm{E1}}}<\tau_{\mathrm{S}}|\gamma_1>\mu\right), \quad (11)$$

$$\mathrm{SOP}_2=\Pr\left(\frac{1+\gamma_{22}}{1+\gamma_{\mathrm{E2}}}<\tau_{\mathrm{S}}|(\gamma_{21}>\mu\cap\gamma_{22}>\mu)\right). \quad (12)$$

In the following, we perform an exact derivation for (11) and (12), and an approximation is also proposed.

A. Exact Analysis

Theorem 1. The conditioned SOP at B_1 and B_2 under imperfect intentional jamming cancellation are, respectively, given by

$$\mathrm{SOP}_1=\begin{cases}\Psi_{\gamma_1}\left(\frac{\gamma_1-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\mu,\frac{\alpha\theta+\tau_{\mathrm{S}}-1}{1-\alpha\theta}\right), & I_a^1\\ \Psi_{\gamma_1}\left(\frac{\gamma_1-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\mu,\frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}\right), & I_b^1,\end{cases} \quad (13)$$

$$\mathrm{SOP}_2=\begin{cases}\Psi_{\gamma_{22}}\left(\frac{\gamma_{22}-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\mu,\frac{\tau_{\mathrm{S}}(1-\alpha\theta)}{1-\theta}-1\right), & I_a^2\\ \Psi_{\gamma_{22}}\left(\frac{\gamma_{22}-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\mu,\frac{(1-\alpha)\theta}{(1-\theta)\xi}\right), & I_b^2\\ \Psi_{\gamma_{22}}\left(\frac{\gamma_{22}-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\frac{\mu(1-\alpha)}{\alpha-\mu(1-\alpha)},\frac{\tau_{\mathrm{S}}(1-\alpha\theta)}{1-\theta}-1\right), & I_c^2\\ \Psi_{\gamma_{22}}\left(\frac{\gamma_{22}-\tau_{\mathrm{S}}+1}{\tau_{\mathrm{S}}},\frac{\mu(1-\alpha)}{\alpha-\mu(1-\alpha)},\frac{(1-\alpha)\theta}{(1-\theta)\xi}\right), & I_d^2.\end{cases} \quad (14)$$

where $I_a^1\triangleq\{1<\tau_{\mathrm{S}}\leq\frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)},\tau_{\mathrm{S}}{-}1\leq\mu<\frac{\alpha\theta+\tau_{\mathrm{S}}-1}{1-\alpha\theta}\}$, $I_b^1\triangleq\{\frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)}<\tau_{\mathrm{S}}<\frac{\xi+\theta(1-\xi)}{\xi+\theta(1-\alpha-\xi)},\tau_{\mathrm{S}}-1\leq\mu<\frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}\}$, $I_a^2\triangleq\{0<\mu\leq\frac{\alpha}{1-\alpha}-1,\frac{\mu\xi}{1-\alpha+\mu\xi}<\theta<1,0<\xi<\frac{\theta(1-\alpha)}{\tau_{\mathrm{S}}(1-\alpha\theta)+\theta-1}\}$, $I_b^2\triangleq\{0<\mu\leq\frac{\alpha}{1-\alpha}{-}1,\frac{\mu\xi}{1-\alpha+\mu\xi}<\theta<1,\frac{\theta(1-\alpha)}{\tau_{\mathrm{S}}(1-\alpha\theta)+\theta-1}\leq\xi<1\}$, $I_c^2\triangleq\{\frac{\alpha}{1-\alpha}-1<\mu<\frac{\alpha}{1-\alpha},\frac{\mu\xi}{\alpha-\mu(1-\alpha-\xi)}<\theta<1,0<\xi<\frac{\theta(1-\alpha)}{\tau_{\mathrm{S}}(1-\alpha\theta)+\theta-1}\}$ and $I_d^2\triangleq\{\frac{\alpha}{1-\alpha}{-}1<\mu<\frac{\alpha}{1-\alpha},\frac{\mu\xi}{\alpha-\mu(1-\alpha-\xi)}<\theta<1,\frac{\theta(1-\alpha)}{\tau_{\mathrm{S}}(1-\alpha\theta)+\theta-1}\leq\xi<1\}$. Also $\Psi_{\gamma_1}(k,a,b)$ and $\Psi_{\gamma_{22}}(k,a,b)$ are defined as

$$\Psi_{\gamma_1}(k,a,b)\triangleq\frac{\int_a^b[1-F_{\gamma_{\mathrm{E1}}}(k)]\;f_{\gamma_1}(\gamma_1)\;\mathrm{d}\gamma_1}{1-F_{\gamma_1}(a)}, \quad (15)$$

$$\Psi_{\gamma_{22}}(k,a,b)\triangleq\frac{\int_a^b[1-F_{\gamma_{\mathrm{E2}}}(k)]\;f_{\gamma_{22}}(\gamma_{22})\;\mathrm{d}\gamma_{22}}{1-F_{\gamma_{22}}(a)}. \quad (16)$$

Proof. The proof is provided in appendix A. □

B. Approximate Analysis

By considering the approximation of the gamma function $\Gamma(a,b)\simeq\Gamma(a)-b^a\Gamma(a)/\Gamma(a+1)$ for $b\to 0$ as in [14], closed-form approximate expressions for the SOP at B_1 and B_2 can be obtained by approximating the gamma functions in (9) and (10) for $\gamma_p\to\infty$. The approximations are respectively shown in (17) and (18) at the top of the next page.

IV. Numerical Results and Discussions

In this section, our analytical expressions are validated by Monte Carlo simulations through some illustrative samples. For the sake of illustration, we consider the pathloss exponent $\beta=4$ (urban scenario), all the positions are normalized by a maximum radius $r=1$, and A is positioned at the center of the disc. Furthermore, we consider the target secrecy rate $R_{\mathrm{S}}=1$ and $\mu=2^{R_{\mathrm{S}}}-1$ (worst-case scenario).

Fig. 2 illustrates the secrecy outage probability versus transmit SNR, γ_p, for different configurations of power allocation factor for NOMA, α and power allocation factor for information, θ. It can be observed that the approximation obtained for SOP is tight from medium-to-high SNR. Also, note that by allocating more power to jamming (lower θ) the SOP is improved, especially for B_2, since it has a privileged position. For B_1, the most crucial parameter is α since the quality of channel of B_1 presents less quality; therefore, it is necessary to allocate more power for signal for decoding to get a better performance. Note that there is no SOP_2 for

$$\mathrm{SOP}_1 \approx \begin{cases} \left[1-e^{-\pi\lambda\left(r^2-r_p^2\right)}\right]\left[1-e^{-\frac{\alpha\theta[\tau_{\mathrm{S}}-(\mu+1)(1-\alpha\theta)]}{\Omega_{\mathrm{AB}_1}\gamma_p[(1-\alpha\theta)(\theta+\xi(1-\theta))-\tau_{\mathrm{S}}(\theta(1-\alpha)+\xi(1-\theta))][\alpha\theta-\mu(\xi+\theta(1-\alpha-\xi))]}}\right], & I_a^1 \\ 1-e^{-\pi\lambda\left(r^2-r_p^2\right)}, & I_b^1, \end{cases} \tag{17}$$

$$\mathrm{SOP}_2 \approx \begin{cases} \left[1-e^{-\pi\lambda\left(r^2-r_p^2\right)}\right]\left[1-e^{-\frac{(1-\alpha)\theta[\tau_{\mathrm{S}}(1-\alpha\theta)-(1-\theta)(\mu+1)]}{\Omega_{\mathrm{AB}_2}\gamma_p(1-\theta)[\xi\tau_{\mathrm{S}}(1-\alpha\theta)-\theta(1-\alpha-\xi)-\xi][\mu\xi-\theta(1-\alpha+\mu\xi)]}}\right], & I_a^2 \\ \left[1-e^{-\pi\lambda\left(r^2-r_p^2\right)}\right]\left[1-e^{-\frac{\alpha\theta(1-\theta-\tau_{\mathrm{S}}(1-\alpha\theta))+(1-\alpha)\theta\tau_{\mathrm{S}}\mu(1-\alpha\theta)}{\Omega_{\mathrm{AB}_2}\gamma_p(1-\theta)[\xi\tau_{\mathrm{S}}(1-\alpha\theta)-\theta(1-\alpha-\xi)-\xi][\alpha\theta-\mu(\theta(1-\alpha-\xi)+\xi)]}}\right], & I_c^2 \\ 1-e^{-\pi\lambda\left(r^2-r_p^2\right)}, & I_b^2 \cup I_d^2. \end{cases} \tag{18}$$

$\alpha = 0.6$ and $\theta = 0.25$, which is mathematically expected, since the parameters set do not fit in any interval, and it represents a case of strong secrecy for B_2.

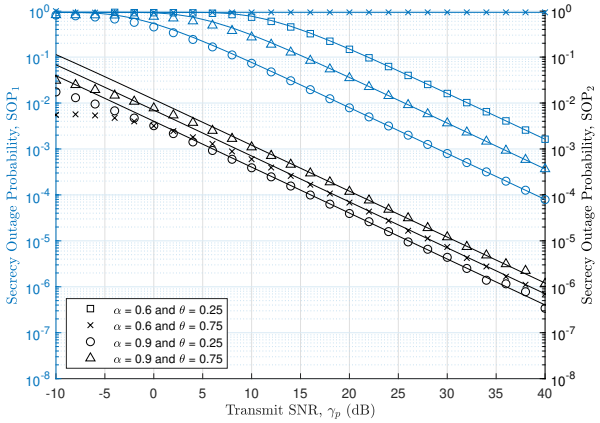

Fig. 2. SOP versus transmit SNR γ_p, for distances $d_{\mathrm{AB}_1} = 0.7$ and $d_{\mathrm{AB}_2} = 0.2$, radius of protected zone $r_p = 0.3$, eavesdropper density $\lambda = 1$ eavesdropper/area unit and RI interference level $\xi = 0$. The lines denote the approximate expressions and markers indicate simulated results.

Fig. 3 shows SOP versus the radius of protected zone, r_p, for different λ, and $d_{\mathrm{AB}_1} = 0.95$ and $d_{\mathrm{AB}_2} = 0.15$, so that the protected zone varies from B_2's position to B_1's position. It can be observed that the SOP decreases more sharply beyond $r_p \approx 0.5$; indeed, as higher the density, a higher r_p is required to have a significant decrease. Also, a lower eavesdropper density leads to a lower SOP, as expected, and it can be noted that this impact is similar for both users.

Fig. 4 illustrates SOP versus power allocation factor for information signals, θ, for different values of RI level, ξ and power allocation factor for NOMA, α. Observe that for the perfect jamming cancellation case, ($\xi = 0$), a better secrecy outage can be attained by allocating more power for intentional jamming. However, with some level of residual interference, lower values of θ will lead to a lost of secrecy, and there is an optimum value of for θ, for which the best performance of each user can be obtained.

Fig. 5 shows SOP versus RI level, ξ, for distinct values of power allocation factor for NOMA, α, and power allocation factor for information, θ. It can be observed that the level of RI may drastically decrease the secrecy performance in both users. Moreover, regarding B_2, for a fixed value of ξ,

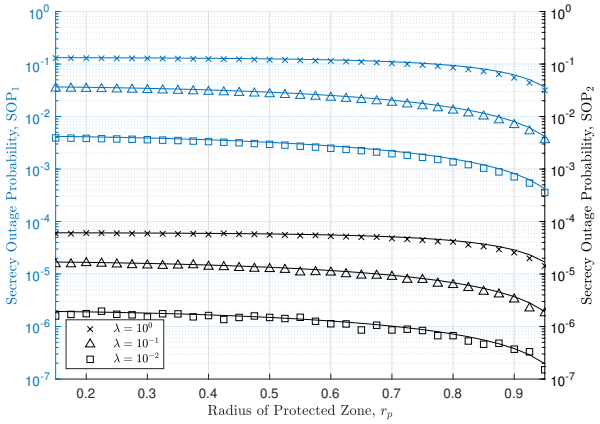

Fig. 3. SOP versus radius of protected zone r_p, for distances $d_{\mathrm{AB}_1} = 0.95$ and $d_{\mathrm{AB}_2} = 0.15$, power allocation factor for information signals $\theta = 0.25$, power allocation factor for NOMA $\alpha = 0.9$, transmit SNR $\gamma_p = 15$ dB and RI interference level $\xi = 0$.

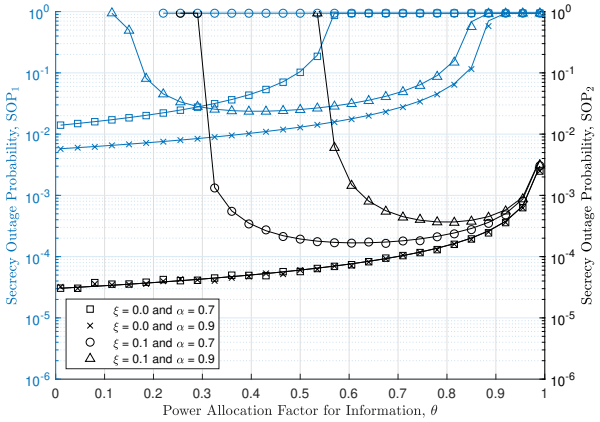

Fig. 4. SOP versus power allocation factor for information signals θ, for distances $d_{\mathrm{AB}_1} = 0.7$ and $d_{\mathrm{AB}_2} = 0.2$, radius of protected zone $r_p = 0.3$, eavesdropper density $\lambda = 1$ eavesdropper/area unit and transmit SNR $\gamma_p = 20$ dB.

the SOP is significantly lower if less power is allocated to B_1 information.

Fig. 6 shows SOP versus target secrecy rate, R_{S}, for distinct values of power allocation factor for NOMA, α, power allocation factor for information, θ, and RI level, ξ. It can be observed that, in general, SOP increases as the target secrecy rate, and the impact of RI interference level is crucial for

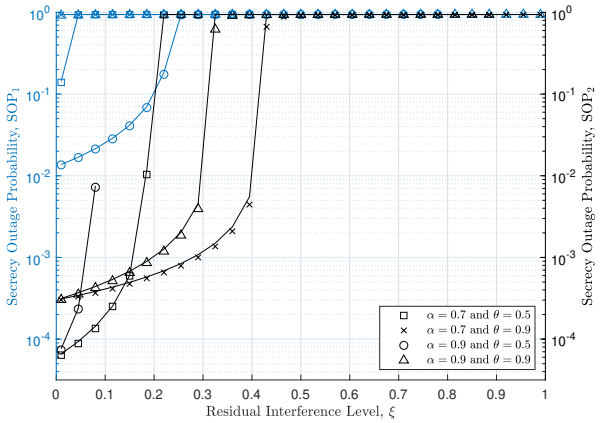

Fig. 5. SOP versus RI level ξ, for distances $d_{\mathrm{AB}_1} = 0.7$ and $d_{\mathrm{AB}_2} = 0.2$, protected radius $r_p = 0.3$, eavesdropper density $\lambda = 1$ eavesdropper/area unit and transmit SNR $\gamma_p = 20$ dB.

lower θ, i.e., for more power allocated to intentional jamming. It is important to remark that $\mu = 2^{R_\mathrm{S}} - 1$ is considered the SNR threshold for reliability, then for $\theta = 0.75$ and $\alpha = 0.7$ the transmission attempts become scarce as the secrecy rate increases, but since there is quality enough to transmit, the secrecy is guaranteed by the high level of power allocated to the strong user, hence the SOP decreases due the scarcity of transmission.

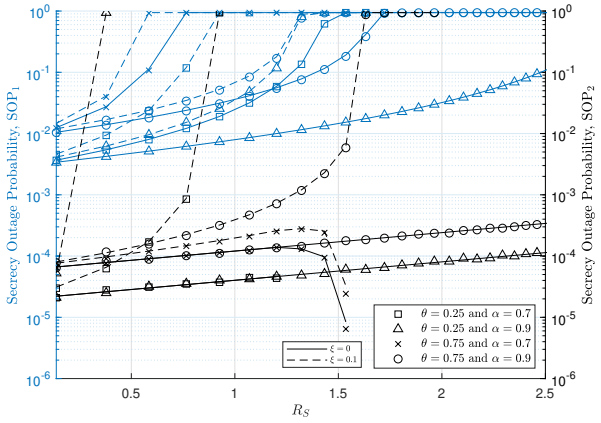

Fig. 6. SOP versus target secrecy rate R_S, for distances $d_{\mathrm{AB}_1} = 0.7$ and $d_{\mathrm{AB}_2} = 0.2$, protected radius $r_p = 0.3$, eavesdropper density $\lambda = 1$ eavesdropper/area unit and transmit SNR $\gamma_p = 20$ dB.

V. Conclusions

We derived integral-form exact and closed-form approximate expressions for the secrecy outage probability of a PD-NOMA network consisting of two legitimate users and multiple eavesdroppers. It was considered the use of intentional jamming for improving the secrecy performance, and the case of imperfect jamming cancellation was evaluated. Results showed that secrecy transmissions are feasible as long as the residual interference level from jamming remains low. Future works can possibly focus on a network of colluding eavesdroppers and/or techniques to guarantee a low RI level due the imperfect jamming cancellation.

Appendix A

The following steps are taken to obtain the SOP at B_1. From (11), let A as the event of $\frac{\gamma_1+1}{\gamma_{\mathrm{E}1}+1} < \tau_\mathrm{S}$ and B as the event of $\gamma_1 > \mu$, by the definition of conditional probability

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}. \tag{19}$$

Considering the constraints described into sections II and III: (i) $\mu \geq \tau_\mathrm{S} - 1$, (ii) $\tau_\mathrm{S} > 1$, (iii) $0.5 < \alpha < 1$, (iv) $0 < \theta < 1$, (v) $0 \leq \xi \leq 1$ and the following limits (vi) $0 < \gamma_1 < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}$ and (vii) $0 < \gamma_{\mathrm{E}1} < \frac{\alpha\theta}{1-\alpha\theta}$, the integration region and parameters ranges can be found by the steps bellow.

Step 1 - Replacing (vi) into event B we have $\mu < \gamma_1 < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}$, that only holds if $\mu < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}$. Using (i) into this result, we obtain $\tau_\mathrm{S} < \frac{\xi+\theta(1-\xi)}{\xi+\theta(1-\alpha-\xi)}$.

Step 2 - The event A can be rewritten as $\gamma_1 < \gamma_{\mathrm{E}1}\tau_\mathrm{S} + \tau_\mathrm{S} - 1$. From (vii), $\gamma_{\mathrm{E}1} < \frac{\alpha\theta}{1-\alpha\theta}$ multiplying τ_S on both sides of this inequality and adding $\tau_\mathrm{S} - 1$, also in both sides, we obtain $\gamma_{\mathrm{E}1}\tau_\mathrm{S} + \tau_\mathrm{S} - 1 < \frac{\tau_\mathrm{S}-1+\alpha\theta}{1-\alpha\theta}$. Therefore, we have that $\gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}$.

Step 3 - From (vi) we have $\gamma_1 < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}$, from the results of step 2, we have $\gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}$, and from the results of step 1, we have $\tau_\mathrm{S} < \frac{\xi+\theta(1-\xi)}{\xi+\theta(1-\alpha-\xi)}$. We can rewrite the event $\left(\gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta} \cap \gamma_1 < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}\right)$ as the event of $\gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}$, if $1 < \tau_\mathrm{S} \leq \frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)}$ or as the event of $\gamma_1 < \frac{\alpha\theta}{(1-\alpha)\theta+(1-\theta)\xi}$, if $\frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)} < \tau_\mathrm{S} < \frac{\xi+\theta(1-\xi)}{\xi+\theta(1-\alpha-\xi)}$.

Step 4 - We can rewrite the event A as the event $\gamma_{\mathrm{E}1} > \frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}}$, from (vii) we have $\gamma_{\mathrm{E}1} > 0$. From (i) we know that $0 < \frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}}$ always holds, so the event $\left(\gamma_{\mathrm{E}1} > \frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}} \cap \gamma_{\mathrm{E}1} > 0\right)$ can be simplified as the event of $\gamma_{\mathrm{E}1} > \frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}}$.

Step 5 - Finally, we can combine the results from steps 1 and 3, and the constraint (i) to verify that the event $(A \cap B)$ will occur for two differen cases: case 1 if $1 < \tau_\mathrm{S} \leq \frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)}$ and $\tau_\mathrm{S} - 1 \leq \mu < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}$, and case 2 if $\frac{(1-\alpha\theta)(\xi+\theta(1-\xi))}{\xi+\theta(1-\alpha-\xi)} < \tau_\mathrm{S} < \frac{\xi+\theta(1-\xi)}{\xi+\theta(1-\alpha-\xi)}$ and $\tau_\mathrm{S} - 1 \leq \mu < \frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}$. Each case will be analyzed separately below.

- **Case 1:** Considering the parameters range in this case, the event $(A \cap B)$ will occur if $\left(\mu < \gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}\right)$ and $\left(\frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}} < \gamma_{\mathrm{E}1}\right)$. Therefore, in this case, the SOP will be defined as

$$\begin{aligned}\mathrm{SOP}_1 &= \frac{\Pr\left(\mu < \gamma_1 < \frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}, \frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}} < \gamma_{\mathrm{E}1}\right)}{\Pr\left(\mu < \gamma_1\right)} \\ &= \frac{\int_\mu^{\frac{\alpha\theta+\tau_\mathrm{S}-1}{1-\alpha\theta}} \left[1 - F_{\gamma_{\mathrm{E}1}}\left(\frac{\gamma_1-\tau_\mathrm{S}+1}{\tau_\mathrm{S}}\right)\right] f_{\gamma_1}(\gamma_1)\mathrm{d}\gamma_1}{1 - F_{\gamma_1}(\mu)} \\ &= \Psi_{\gamma_1}\left(\frac{\gamma_1 - \tau_\mathrm{S} + 1}{\tau_\mathrm{S}}, \mu, \frac{\alpha\theta + \tau_\mathrm{S} - 1}{1 - \alpha\theta}\right),\end{aligned} \tag{20}$$

where $\Psi_{\gamma_1}(k, a, b)$ is defined in (15).

- **Case 2:** Considering the parameters range of this case, the event $(A \cap B)$ will occur if $\left(\mu < \gamma_1 < \frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}\right)$ and $\left(\frac{\gamma_1-\tau_S+1}{\tau_S} < \gamma_{E1}\right)$. Therefore, in this case the SOP will be defined as

$$\begin{aligned}\mathrm{SOP}_1 &= \frac{\Pr\left(\mu < \gamma_1 < \frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}, \frac{\gamma_1-\tau_S+1}{\tau_S} < \gamma_{E1}\right)}{\Pr\left(\mu < \gamma_1\right)} \\ &= \frac{\int_{\mu}^{\frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}} \left[1 - F_{\gamma_{E1}}\left(\frac{\gamma_1-\tau_S+1}{\tau_S}\right)\right] f_{\gamma_1}(\gamma_1)\mathrm{d}\gamma_1}{1 - F_{\gamma_1}(\mu)} \\ &= \Psi_{\gamma_1}\left(\frac{\gamma_1-\tau_S+1}{\tau_S}, \mu, \frac{\alpha\theta}{\xi+\theta(1-\alpha-\xi)}\right). \quad (21)\end{aligned}$$

A similar process can be followed to obtain the SOP at B_2, by replacing the respective parameters, constraints, and CDFs.

REFERENCES

[1] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5g and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, 2017.

[2] A. Tregancini, E. E. B. Olivo, D. P. M. Osorio, C. H. M. de Lima, and H. Alves, "Performance analysis of full-duplex relay-aided noma systems using partial relay selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 622–635, 2020.

[3] D. P. Osorio, J. D. Sánchez, and H. Alves, "Physical-layer security for 5g and beyond," in *Wiley 5G Ref*, 2019, pp. 1–19.

[4] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "Phy layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, 2013.

[5] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: A noma-inspired jamming and relaying approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3191–3205, 2019.

[6] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *IEEE International Conference on Communications*, 2016, pp. 1–6.

[7] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink noma multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70 422–70 435, 2019.

[8] 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, 2020.

[9] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, and P. Zhang, "Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2682–2696, 2019.

[10] S. S. Saab, J. G. Hobeika, and I. E. Ouaiss, "A novel pseudorandom noise and band jammer generator using a composite sinusoidal function," *IEEE Transactions on Signal Processing*, vol. 58, no. 2, pp. 535–543, 2010.

[11] M. Haenggi, *Stochastic Geometry for Wireless Networks*, 1st ed. USA: Cambridge University Press, 2012.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, Amsterdam, 2007.

[13] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, 2011.

[14] D. P. Moya Osorio, E. E. Benitez Olivo, D. B. da Costa, and J. C. Silveira Santos Filho, "Distributed link selection in multirelay multiuser networks," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 7, pp. 939–951, 2016.