IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 28, 2019, accepted May 22, 2019, date of publication June 3, 2019, date of current version June 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920578

Physical Layer Security in Uplink NOMA Multi-Antenna Systems With Randomly Distributed Eavesdroppers

GERARDO GOMEZ[1], FRANCISCO J. MARTIN-VEGA[2], F. JAVIER LOPEZ-MARTINEZ[1], (Senior Member, IEEE), YUANWEI LIU[3], (Senior Member, IEEE), AND MAGED ELKASHLAN[3]

[1]Departamento de Ingeniería de Comunicaciones, Universidad de Málaga, 29071 Málaga, Spain
[2]Keysight Technologies, 29590 Málaga, Spain
[3]Department of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K.

Corresponding author: Gerardo Gomez (ggomez@ic.uma.es)

This work was supported in part by the Spanish Government (Ministerio de Economía y Competitividad) under Grant TEC2016-80090-C2-1-R, and in part by the Universidad de Málaga.

ABSTRACT The physical layer security of uplink non-orthogonal multiple access (NOMA) is analyzed. A stochastic geometry approach is applied to analyze the coverage probability and effective secrecy throughput (EST) of the *kth* NOMA user, where a fixed or an adaptive transmission rate can be used. We consider a protected zone around the legitimate terminals to establish an eavesdropper-exclusion area. We assume that the channel state information associated with eavesdroppers is not available at the base station. We also consider that the base station is equipped with multiple antennas. The impact of imperfect successive interference cancellation is also taken into account in this paper. Our framework allows to compute, numerically, the wiretap code rates that maximize the EST. In addition, our framework also allows an optimum selection of other system parameters, such as the transmit power or the eavesdropper-exclusion radius.

INDEX TERMS Effective secrecy throughput (EST), non-orthogonal multiple access (NOMA), physical layer security, stochastic geometry.

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) has recently been introduced as a new feature intended to increase the spectrum efficiency in the fifth generation (5G) networks [1], [2]. This technique allows serving multiple users simultaneously using the same spectrum resources at the cost of increased intra-cell interferences [3]. NOMA may use the power domain jointly with interference cancellation techniques to separate signals, exploiting the path-loss differences among users.

In uplink (UL) NOMA, a set of users transmits simultaneously their signals to their associated base station (BS). As a consequence, the received signal of a particular user suffers from intra-cluster interference, which is a function of the channel statistics of other users. In order to minimize such interference, the BS may apply successive interference cancellation (SIC) to decode signals. SIC technique requires that different message signals arrive to the receiver (BS) with a sufficient power difference so that SIC may be successfully applied. This is typically achieved in the downlink (DL) by means of different weights at the transmitter. However, since the UL channel gains already provide sufficient distinctness between the received signals, such weights are not necessary. In fact, the conventional UL transmit power control intended to equalize the received signal powers of users is not recommended for UL NOMA transmissions since it may remove channel distinctness [3].

SIC technique in UL NOMA works as follows. The BS first decodes the strongest signal by considering the signals from other users as noise. However, the user with the weakest signal enjoys zero intra-cluster interference since the BS has previously canceled interfering signals (considering ideal conditions). If we consider the possibility of a SIC failure, the error is propagated to all remaining messages.

UL NOMA was firstly presented in [4], by considering the minimum mean squared error (MMSE)-based SIC

The associate editor coordinating the review of this manuscript and approving it for publication was Yong Zeng.

decoding at the BS. An interesting survey on NOMA for 5G networks is presented in [5], which provides a comprehensive overview of the latest NOMA research results and innovations. A novel dynamic power allocation scheme for DL and UL NOMA is proposed in [6]. The outage performance and the achievable sum data rate for UL NOMA is theoretically analyzed in [7]. In [8], a framework to analyze multi-cell UL NOMA with stochastic geometry is presented. In [9], the optimum received UL power levels using a SIC detector is determined analytically for any number of transmitters.

The possibility of having a secure communication in NOMA-based scenarios is also a current hot topic. The presence of eavesdroppers (EDs) is a classical problem in communication theory, ever since Wyner introduced the wiretap channel [10]. In the last years, the field of physical layer security over different scenarios has taken an important interest in the research community as a means to provide reliable secure communications, relaxing the complexity and complementing the performance of the required cryptographic technologies. For instance, the work in [11] considers the secure transmission of information over an ergodic fading channel in the presence of an ED. An extension of this work considering a multiple-input multiple-output (MIMO) wiretap channel is analyzed in [12]. In [13], an analysis is conducted on the probability of secrecy capacity for wireless communications over Rician fading channels. The communication between two legitimate peers in the presence of an external ED in the context of free-space optical (FSO) communications is analyzed in [14]. In [15], a comprehensive survey on various multiple-antenna techniques in physical layer security is provided, with an emphasis on transmit beamforming designs for multiple-antenna nodes. An overview on the state-of-the-art works on physical layer security technologies that can provide secure communications in wireless systems is given in [16].

In the particular field of physical layer security with NOMA, a small number of contributions are available. A simple scenario for a DL NOMA with just one ED (with single antenna configuration) in a single cell is addressed in [17]. An analysis of the optimal power allocation policy that maximizes the secrecy sum rate for a DL NOMA scenario is presented in [18]. In [19], a cooperative NOMA system with a single relay is analyzed assuming that NOMA users are affected by an ED. The work in [20] analyzes the secrecy outage probability (SOP) in a single-cell DL NOMA scenario in which the EDs are not part of the cellular system. Reference [21] extends previous work by proposing several mechanisms to enhance the SOP in a DL NOMA multi-antenna aided transmission. In [22], a DL NOMA scenario with multiple-input single-output (MISO) is addressed, proposing a secure beamforming transmission scheme. The secrecy performance of a two-user DL NOMA with transmit antenna selection schemes is analyzed in [23]. The work in [24] studies the secrecy performance of a downlink of multiple-input multiple-output (MIMO) scenario, focusing on the impact of a max-min transmit antenna selection strategy.

A. MOTIVATION AND CONTRIBUTIONS

As described before, most recent literature dealing with a physical layer security characterization of NOMA is focused on the DL [21]–[24]. Hence, its use on an UL setup is one of the novel contributions of this paper. To the best of the authors' knowledge, the only work dealing with this scenario [25] does not incorporate random spatial locations of EDs since locations are deterministic (i.e. it does not use a stochastic geometry approach) and does not consider the effect of the protection radius around the legitimate users (LUs).

The main technical differences and challenges on analyzing the physical layer security in UL NOMA from the existing studies for DL NOMA are the following:

- In the UL NOMA, the BS receives transmissions from all users simultaneously, and consequently, intra-cell interference to a given user is a function of the channel statistics of other users within the cell; however, in DL NOMA, the intra-cell interference to a user is a function of its own channel statistics [8].
- Intra-cluster interfering signals in the UL NOMA are also the desired signals; therefore, it is not possible to provide the benefits of SIC, i.e. enhance the Signal-to-Interference plus Noise Ratio (SINR) unequivocally for all users.
- In the UL NOMA, EDs are randomly positioned near the N legitimate transmitters, independently of the transmitters' location within the cell, whereas in the DL NOMA, the BS is the unique transmitter, thus simplifying the scenario.

In this work, we provide the following contributions:

1) We provide a detailed characterization of an UL NOMA scenario for a generic number of simultaneous users. The analysis is given both from a connection level perspective and from a physical layer security viewpoints. We provide new analytical expressions for UL NOMA at the BS with multiple antennas, random spatial locations of EDs and a protection radius around the LUs to enhance the secrecy metrics. This scenario has not been addressed yet to the best of the authors' knowledge.
2) We analyze the effective secrecy throughput (EST) for UL NOMA as a performance metric that captures the two key features of wiretap channels (reliability and secrecy). We provide analytical expressions for the EST, which captures explicitly the reliability constraint and secrecy constraint of wiretap channels. Our analysis allows determining numerically the wiretap code rates that achieve the maximum EST. Additionally, it also helps designing optimum values of the transmit power and the ED-exclusion radius in order to enhance the overall EST.

3) We analyze previous metrics under two different scenarios: fixed and adaptive transmission schemes from legitimate users (LUs). In the case of fixed transmission rate, our analysis includes the impact of an imperfect SIC during NOMA detection.

B. ORGANIZATION AND NOTATION

The remainder of this paper is organized as follows. The system model under analysis is introduced in Section II. The analysis of the SINR distributions for both LUs and EDs is presented in Section III. In Section IV, analytical expressions for the EST under different scenarios are derived. Numerical results are shown and described in Section V. Finally, we draw conclusions in Section VI.

Notation: Throughout this paper, $\mathbb{E}[\cdot]$ stands for the expectation operator and $\mathbb{P}$ for the probability measure. Random variables (RV) are represented with capital letters whereas lower case is reserved for deterministic values and parameters. If X is a RV, $f_X(\cdot)$, $F_X(\cdot)$, $\bar{F}_X(\cdot)$ and $\mathcal{L}_X(\cdot)$ represent its probability density function (pdf), cumulative distribution function (cdf), complementary cdf (ccdf) and Laplace transform of its pdf, respectively.

II. SYSTEM MODEL

We focus on the UL communication scenario in which LUs are connected to a BS centered at the origin, with an associated serving cell of radius r_c. We assume a single cell scenario, as considered in most previous studies related to NOMA [1], [6], [7], [9], [18], [20], [21], [26]. A number of EDs (EDs) are randomly distributed along the whole plane, attempting to intercept the communication between LUs and BS. The spatial distribution of EDs is modeled using a homogeneous Poisson Point Process (PPP) uniformly distributed in $\mathbb{R}^2$, which is denoted by Φ_e and associated with a density λ_e. The spatial distribution of EDs is modeled using a Poisson Point Process (PPP) distributed in $\mathbb{R}^2$, which is denoted by Φ_e and associated with a density λ_e. An ED-exclusion zone of radius r_p (in which no EDs are allowed to roam) is introduced around the LUs for improving the secrecy performance, as it is also considered in [21] for the DL. Hence, Φ_e can be considered as an inhomogeneous PPP with $\lambda_e > 0$ density outside the exclusion radius and $\lambda_e = 0$ inside that region. Fig. 1 shows the system model under analysis.

At each radio resource, the BS gives service to N simultaneous LUs (using NOMA), whose positions are random inside the cell. We assume a random scheduling, i.e. the BS selects randomly the set of N LUs to be scheduled in a given radio resource according to NOMA. The locations of the LUs that are scheduled in a single radio resource are assumed to be uniformly distributed in the cell. Hence, we consider that the resulting set of points (LUs) inside the disk $B(0, r_c)$ is a Binomial Point Process (BPP) Φ_B with N points, as it is normally assumed in the literature [7], [26]. The assumption of a BPP for LUs (instead of a PPP) is due to tractability issues, but at the same time, it provides the necessary spatial correlation between the nodes that are served by the BS.

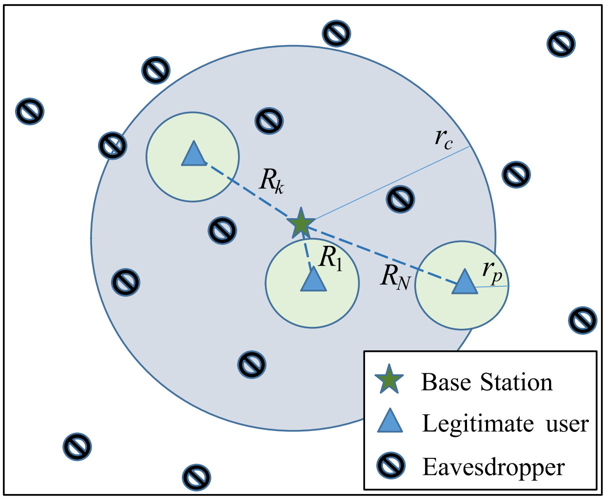

FIGURE 1. System model for secure transmission in UL NOMA.

We assume that both LUs and EDs are equipped with a single antenna each whereas the BS is equipped with M uncorrelated receive antennas and applies a Maximal Ratio Combining (MRC) reception. We also assume that LUs' channels and EDs' channels are subject to independent quasi-static Rayleigh fading with equal block length. UL transmit power control is not recommended as justified in the introduction section, and hence, it is not used.

We also consider that the EDs apply the same SIC method than the BS in order to separate the signals from each transmitter, so that they can technically compromise the communication from each user in the network (and specially if colluding EDs are considered, which is not the case in this paper). That is, the EDs measure the received signal power and first decodes the strongest signal by treating other signals as noise. Afterwards, it cancels the first decoded signal and continues decoding the second strongest signal, and so on. We consider the most detrimental ED scenario in order to simplify the code rate design.

As stated in [3], the impact of the path-loss factor is generally more dominant than channel fading effects. Hence, for tractability reasons, we assume that ordering of the received signal powers can be approximately achieved by ordering the distances of the users to their serving BS. Let R_k be the distance between the kth user and the BS, being $R_1 \leq R_k \leq R_N$. Power loss due to propagation is modeled using a standard path-loss model with $\alpha > 2$, whereas a Rayleigh model is assumed for small-scale fading. Hence, the received signal power at a distance R_k can be simply computed as $H_k {R_k}^{-\alpha}$, where H_k is the equivalent channel power gain for the kth user after multiple antenna processing at the receiver.

We consider a scenario in which EDs are not a part of the cellular system (passive eavesdropping) and therefore, the channel state information (CSI) associated with EDs' channel is not available at the BS. Note that LUs might be aware of the presence of a potential ED in their surrounding area, simply by a visual inspection, thus guaranteeing the ED-exclusion zone during their transmission.

Let R_s be the secrecy rate in a legitimate link, i.e. the rate of transmitted confidential information. This rate can be computed as:

$$R_s \triangleq R_b - R_e \geq 0, \tag{1}$$

where R_b represents the codeword rate from the LU to the BS, i.e. rate at which the codeword is transmitted, including the confidential message and redundancy; R_e quantifies the redundancy rate, i.e. rate associated with redundant information for providing physical layer security in the message transmission. Roughly, a larger R_e provides a higher secrecy level.

On the one hand, if we select a codeword rate such that $R_b \leq C_b$ (being C_b the capacity of the legitimate channel), a reliability constraint is ensured. On the other hand, if the redundancy rate is above the capacity of the ED's channel, i.e. $R_e > C_e$, a secrecy constraint is achieved.

Depending on whether the CSI of LU and ED links are available at the BS, such rates can be adapted to the channel or not. In that sense, we address two different cases regarding the LUs transmission mode:

- *Fixed transmission rate*: LUs transmit their information towards their BS at a fixed rate. In this scenario, we find the optimum values for the wiretap code rates, taking into account the reliability outage probability that occurs when the selected fixed rate exceeds the instantaneous channel capacity.
- *Adaptive transmission rate*: the BS enforces an adaptive secure transmission from LUs assuming a perfect channel estimation. In this scenario, we find the optimum value of the redundancy rate, R_e, that maximizes the secrecy performance.

Note that, although the fixed rate transmission is expected to achieve a worst performance compared to the adaptive transmission, it is here included as a baseline to evaluate the gain of the latter case. Additionally, our analysis could be also extended to other type of communications (sensor networks, etc.) in which the fixed rate case might be the best solution for a very simple device.

III. ANALYSIS OF THE SINR DISTRIBUTIONS

First, we analyze the connection related statistics of this scenario using a stochastic geometry approach. We assume that the BS applies SIC to detect the UL transmission from the nearest user first, and afterwards, it continues decoding the information from other users up to user N.

Let us denote the receive signal at the j^{th} antenna port

$$r_j = \sqrt{P_T R_k^{-\alpha}} g_j^{(k)} x_k + \sqrt{P_T} \sum_{i=k+1}^{N} \sqrt{R_i^{-\alpha}} g_j^{(i)} x_i + n_j \tag{2}$$

where $g_j^{(i)}$ indicates the amplitude fading channel coefficient between the i^{th} user transmitter and the j^{th} antenna port, x_i denote the message symbols from the i^{th} user with $\mathbb{E}\{|x_i|^2\} = 1$, n_j is the additive white Gaussian noise (AWGN) term, P_T is the transmit power, N is the number of users and $j = 1 \dots M$, with M being the number of receive antennas. According to the system model here considered, all fading channel coefficients are normalized Rayleigh RVs with $\mathbb{E}\{|g_j^{(i)}|^2\} = 1$.

Now, defining the vectors $g^i = [g_1^{(i)} \dots g_M^{(i)}]$ and $r = [r_1 \dots r_M]$, the output of the MRC combiner to decode the message x_k is given by [27, eq. (26)] as

$$y^{(k)} = g^{k^H} r = \sqrt{P_T R_k^{-\alpha}} \underbrace{\sum_{j=1}^{M} |g_j^{(k)}|^2}_{H_k} x_k + \sqrt{P_T} \sum_{i=k+1}^{N} \sum_{j=1}^{M} \sqrt{R_i^{-\alpha}} g_j^{(i)} g_j^{(k)*} x_i + n_{eq}, \tag{3}$$

where ^{H} denotes the Hermitian transpose, * the complex conjugate operation and n_{eq} is an equivalent noise term.

With these definitions, the received instantaneous SINR at the BS for the k^{th} user is defined as

$$\gamma_k = \frac{H_k R_k^{-\alpha}}{I + 1/\rho_b}, \tag{4}$$

where ρ_b represents the transmit signal-to-noise ratio (SNR) defined as $\rho_b = \frac{P_T}{\sigma_b^2}$, being σ_b^2 the noise power at the BS. In this equation, the term I represents the intra-cluster interference due to other NOMA users, which is related to the underlying amplitude fading coefficients as follows:

$$I = \sum_{i=k+1}^{N} \underbrace{H_i R_i^{-\alpha}}_{|v_i|^2}, \tag{5}$$

where the individual interference terms are given as

$$v_i = \sum_{j=1}^{M} \frac{g_j^{(i)} g_j^{(k)*}}{|g^k|} = \sum_{j=1}^{M} \frac{g_j^{(i)} g_j^{(k)*}}{\sqrt{H_k}}. \tag{6}$$

We note that according to [27, eq. (30)], it follows that v_i is a complex Gaussian RV (and notably, independent of H_k) if the individual gains are Rayleigh distributed, which is the case under consideration.

Note that, since we consider a MRC reception technique at the BS, the desired signal is given by the sum of M independent unit-mean exponentially distributed random variables, yielding a Gamma distribution with ccdf given by

$$\overline{F}_{H_k}(M, x) = e^{-x} \cdot \sum_{r=0}^{M-1} \frac{x^r}{r!} \tag{7}$$

Note that (4) represents the SINR associated with the decoding process of the message from user k subject to the correct decoding process from previous NOMA users (from user 1 to $k-1$) so that their intra-cluster interference has been successfully canceled. Also note that the SINR expression for the last user is simplified to $\gamma_N = \rho_b H_N R_N^{-\alpha}$ since the intra-cluster interference has been completely canceled.

A. DISTRIBUTION OF THE SINR OF LEGITIMATE USERS

In this section we compute the coverage probability of the LUs, i.e. the ccdf of their received SINR at the BS, which represents the probability for a user to have a SINR higher than a given threshold t.

Lemma 1: In the case of M antennas at the BS, the ccdf of the SINR for the kth user, $p_k(t)$, is given by

$$
\begin{aligned}
&\bar{F}_{\gamma_k}(t) \\
&= \int_0^{r_c} e^{-\psi/\rho_b} \sum_{r=0}^{M-1} \sum_{k=0}^{r} \frac{\psi^r (-1)^k}{(r-k)!k!\rho_b^{r-k}} \frac{d^k}{ds^k} \mathcal{L}_{I|r_k}(s)\,|_{s=\psi} \\
&\times \frac{2}{r_c} \frac{\Gamma\left(k+\frac{1}{2}\right)\Gamma(N+1)}{\Gamma(k)\Gamma\left(N+\frac{3}{2}\right)} \beta\left(\frac{r_k^2}{r_c^2}; k+\frac{1}{2}, N-k+1\right) dr_k
\end{aligned}
\tag{8}
$$

with $\psi = tr_k^\alpha$ and

$$
\mathcal{L}_{I|r_k}(s) = \left(\frac{2\left(r_c^{\alpha+2}\Omega\left(-\frac{r_c^\alpha}{tr_k^\alpha}\right) - r_k^{\alpha+2}\Omega\left(-\frac{1}{t}\right)\right)}{tr_k^\alpha\left(r_c^2 - r_k^2\right)(\alpha+2)}\right)^{N-k} \tag{9}
$$

where $\Omega(x) = {}_2F_1\left[1, \frac{\alpha+2}{\alpha}, 2+\frac{2}{\alpha}, x\right]$ being ${}_2F_1[\cdot,\cdot,\cdot,\cdot]$ the Gauss hypergeometric function defined in [28] (Ch. 15), $\Gamma(z) = \int_0^\infty t^{z-1}\mathrm{e}^{-t}\mathrm{d}t$ stands for the Euler Gamma function, $\beta(x; a, b)$ is the beta density function defined as $\beta(x; a, b) = (1/B(a, b))x^{a-1}(1 - x)^{b-1}$, being $B(a, b)$ the beta function, which is expressible in terms of Gamma functions as $B(a, b) = \Gamma(a)\Gamma(b)/\Gamma(a + b)$. Note that (8) just includes one finite integral, which can be also computed by the Gaussian-Chebyshev quadrature relationship [29].

Proof: See Appendix A. □

As mentioned before, due to the exclusion regions considered in the scenario, the locations of EDs have been modeled as an inhomegeneous PPP, where the exclusion regions are treated as a disk centered around the target LU. Taken into account this assumption, our theoretical analysis represents an approximation, since the analysis does not consider the exclusion regions from other LUs. This approximation actually represents an upper bound for the coverage probability since the distance between the LU and the EDs will be statistically higher if the exclusion regions from other LUs are taken into account.

Corollary 1: In the case of single antenna ($M = 1$) at the BS, the ccdf of the SINR for the kth user, $p_k(t)$, is simplified to

$$
\begin{aligned}
&\bar{F}_{\gamma_k}(t) \\
&= \int_0^{r_c} e^{-tr_k^\alpha/\rho_b} \\
&\times \left(\frac{2\left(r_c^{\alpha+2}\Omega\left(-\frac{r_c^\alpha}{tr_k^\alpha}\right) - r_k^{\alpha+2}\Omega\left(-\frac{1}{t}\right)\right)}{tr_k^\alpha\left(r_c^2 - r_k^2\right)(\alpha+2)}\right)^{N-k} \\
&\times \frac{2}{r_c} \frac{\Gamma\left(k+\frac{1}{2}\right)\Gamma(N+1)}{\Gamma(k)\Gamma\left(N+\frac{3}{2}\right)} \beta\left(\frac{r_k^2}{r_c^2}; k+\frac{1}{2}, N-k+1\right) dr_k
\end{aligned}
\tag{10}
$$

Corollary 2: In the case of single antenna ($M = 1$) at the BS, the coverage probability for the farthest user (N) is simplified to

$$
\bar{F}_{\gamma_N}(t) = \frac{2N}{\alpha r_c^{2N}}\left(\frac{t}{\rho_b}\right)^{-\frac{2N}{\alpha}} \left[\Gamma\left(\frac{2N}{\alpha}\right) - \Gamma\left(\frac{2N}{\alpha}, \frac{r_c^\alpha t}{\rho_b}\right)\right] \tag{11}
$$

where $\Gamma(\cdot,\cdot)$ stands for the upper incomplete Gamma function.

Proof: The farthest user (N) experiences no intra-cluster interference, so its coverage probability can be expressed as

$$
\begin{aligned}
\bar{F}_{\gamma_N}(t) &= \int_0^{r_c} e^{-tr_N^\alpha/\rho_b} f_{R_N}(r_N) dr_N \\
&= \int_0^{r_c} e^{-tr_N^\alpha/\rho_b} \frac{2N}{r_c}\left(\frac{r_N^2}{r_c^2}\right) dr_N
\end{aligned}
\tag{12}
$$

After minor manipulations, the proof is complete. □

B. DISTRIBUTION OF THE SNR OF EAVEDROPPERS

We address the worst-case scenario, in which EDs are assumed to have strong detection capabilities. Specifically, by applying multi-user detection techniques, the multi-user data stream received at the BS can be also distinguished by the EDs.

We consider the most detrimental ED, which is not necessarily the nearest one, but the one having the best channel to the LU that is transmitting towards the BS. Therefore, the instantaneous received SNR at the most detrimental ED (with respect with any LU) can be expressed as follows:

$$
\gamma_e = \max_{e\in\Phi_e}\left\{\rho_e H_e R_e^{-\alpha}\right\} \tag{13}
$$

where ρ_e represents the transmit SNR defined as $\rho_e = \frac{P_T}{\sigma_e^2}$, being P_T transmit power at the LU; σ_e^2 is the AWGN power received at the ED; H_e stands for the channel power gain received at the ED from the LU. Since both ED and LU are equipped with a single antenna, H_e follows an exponential distribution.

Lemma 2: Assuming an ED-exclusion zone of radius r_p around the LUs, the cdf of the SNR for the most detrimental ED can be computed as follows:

$$
F_{\gamma_e}\ (t) = \exp\left[-\frac{2\pi\lambda_e\Gamma\left(2/\alpha, r_p^\alpha t/\rho_e\right)}{\alpha(t/\rho_e)^{2/\alpha}}\right] \tag{14}
$$

Proof: Taking into account that EDs follow a PPP distribution, we can express the cdf of the SNR for the most detrimental ED as follows:

$$
\begin{aligned}
F_{\gamma_e}(t) &= 1 - p_e(t) = E_{\Phi_e}\left\{\prod_{e\in\Phi_e} F_{H_e}\left(tr_e^\alpha/\rho_e\right)\right\} \\
&\overset{(a)}{=} \exp\left[-\lambda_e \int_{R^2}\left(1 - F_{H_e}\left(tr_e^\alpha/\rho_e\right)\right) r_e dr_e\right]
\end{aligned}
$$

$$= \exp\left[-2\pi\lambda_e \int_{r_p}^{\infty} r_e e^{-t r_e^{\alpha}/\rho_e} dr_e\right] \tag{15}$$

where (a) comes from the Probability Generating Functional (PGFL) [30]. Solving the last integral, the proof is complete. □

In the particular case of no ED-exclusion zone, (14) is simplified to:

$$F_{\gamma_e}(t)\Big|_{r_p=0} = \exp\left[-\frac{2\pi\lambda_e\Gamma\left(2/\alpha\right)}{\alpha(t/\rho_e)^{2/\alpha}}\right] \tag{16}$$

IV. SECRECY RATE METRICS

Most of previous works on physical layer security compute the secrecy capacity as $C_s = [C_b - C_e]^+$, where $[x]^+ = \max\{0, x\}$ [31], although this definition implicitly requires that both C_b and C_e are available. In our scenario, this assumption is not realistic since EDs are not part of the cellular system. Subsequently, we do not use the typical information-theoretic formulation related to the secrecy capacity but a recent formulation of a new metric, referred to as the *effective secrecy throughput* (EST) [32], which captures both the reliability constraint and the secrecy constraint as independent terms.

In order to ensure secrecy, two different constraints are to be considered. On the one hand, a reliability constraint is based on the fact that the error probability at the receiver decreases with increasing code length; therefore, if we select a codeword rate such that $R_b \leq C_b$ (being C_b the capacity of the legitimate channel), the reliability constraint is ensured. On the other hand, a secrecy constraint is based on the fact that the fraction of information leakage to the ED decreases with increasing code length; therefore, if the redundancy rate is above the capacity of the ED's channel, i.e. $R_e > C_e$, the secrecy constraint is achieved.

The EST of a wiretap channel quantifies the average secrecy rate at which the messages are transmitted from the LUs to the BS without being leaked to the EDs, and can be defined as

$$\Phi(R_b, R_e) = (R_b - R_e)\left[1 - \mathcal{O}_r(R_b)\right]\left[1 - \mathcal{O}_s(R_e)\right] \tag{17}$$

where the term $(R_b - R_e)$ represents the rate of transmitted confidential information, i.e. R_s; and the term $[1 - \mathcal{O}_r(R_b)]$ $[1 - \mathcal{O}_s(R_e)]$ quantifies the probability that the information is securely transmitted from the LUs to the BSs, being $[1 - \mathcal{O}_r(R_b)]$ associated with the reliability constraint and $[1 - \mathcal{O}_r(R_e)]$ associated with the secrecy constraint. We assume a normalized bandwidth $W = 1$, and therefore, secrecy rate and capacity metrics are measured in bits/s.

We have chosen the EST as a secrecy performance metric in this paper as it allows for explicitly designing the wiretap code rates that satisfy certain reliability and secrecy constraints. This is not the case when using conventional secrecy metrics such as the Secrecy Outage Probability (SOP) $\mathcal{P}(C_s < R_s)$ (where R_s is defined as the threshold rate under which secure communication cannot be achieved) or the probability of strictly positive secrecy capacity $\mathcal{P}(C_s > 0)$. Besides, and despite being a relatively recent performance metric, the EST has been used in numerous recent works [25], [32]–[40]. Additionally, the evaluation of the SOP poses an additional challenge from an analytical perspective in this specific scenario, since it includes an additional infinite integral.

A. ADAPTIVE TRANSMISSION RATE

In this scenario, the BS enforces an adaptive transmission scheme from LUs in the UL.

Theorem 1: The EST for the NOMA kth user in case of adaptive transmission is given by

$$\Phi_k(R_e) = \left(\frac{1}{ln\,2}\int_{2^{R_e}-1}^{\infty}\frac{\bar{F}_{\gamma_k}(z)}{1+z}dz - F_{\gamma_k}(2^{R_e}-1)R_e\right)F_{\gamma_e}\left(2^{R_e}-1\right) \tag{18}$$

where $\bar{F}_{\gamma_k}(\cdot)$ and $F_{\gamma_e}(\cdot)$ were given in (10) and (14), respectively.

Proof: In case of adaptive transmission, R_b can be optimally chosen as $R_b = C_b$, and hence, the reliability constraint can be always guaranteed, i.e. the reliability outage probability is zero: $\mathcal{O}_r(R_b) = 0$. Therefore, the EST for the NOMA *kth* user can be defined as

$$\Phi_k(R_e) = (C_k - R_e)\left[1 - \mathcal{O}_s(R_e)\right] \tag{19}$$

where the term C_k represents the ergodic capacity for the *kth* user. Note that, in the adaptive transmission scheme, R_e is adjusted within the constraint $0 < R_e < C_k$. Since $R_b = C_b$, we need to guarantee that $C_b = log_2(1 + \gamma_b) > R_e$, that is, $\gamma_b > 2^{R_e} - 1$. Therefore, assuming a normalized channel bandwidth $W = 1$, the average capacity for the *kth* user, C_k, can be expressed as

$$C_k = \int_{2^{R_e}-1}^{\infty} \log_2\left(1+\gamma\right) f_{\gamma_k}(\gamma)d\gamma. \tag{20}$$

Using integration by parts with $u = \log_2(1+\gamma)$, $dv = f_{\gamma_k}(\gamma)$ and $v = -\left(1 - F_{\gamma_k}(\gamma)\right)$, the average capacity can be also expressed as

$$C_k = \bar{F}_{\gamma_k}(2^{R_e}-1)R_e + \frac{1}{ln\,2}\int_{2^{R_e}-1}^{\infty}\frac{\bar{F}_{\gamma_k}(z)}{1+z}dz \tag{21}$$

The secrecy outage probability term can be computed as

$$\begin{aligned}\mathcal{O}_s(R_e) &= \mathbb{P}(R_e < C_e) = \mathbb{P}(\gamma_e > 2^{R_e} - 1)\\ &= 1 - F_{\gamma_e}(2^{R_e} - 1).\end{aligned} \tag{22}$$

Substituting (22) and (21) into (19), the proof is complete. □

Remark 1 (Impact of EDs density, λ_e): In view of Theorem 1, it can be deduced that, for $\lambda_e = 0$, the term associated with the secrecy constraint, $\mathcal{O}_r(R_e)$, is null; hence, the EST is mainly determined by the capacity of the LU's link. On the other hand, the EST tends to zero as λ_e grows since

TABLE 1. Summary of secrecy metric expressions for different scenarios.

SCENARIO	RELIABILITY CONSTRAINT, $[1-\mathcal{O}_r(R_b)]$	SECRECY CONSTRAINT, $[1-\mathcal{O}_s(R_e)]$	EFFECTIVE SECRECY THROUGHPUT (EST), Φ_k
Adaptive rate	1	$F_{\gamma_e}\left(2^{R_e}-1\right)$	$\Phi_k(R_e)=\left(\frac{1}{\ln 2}\int_{2^{R_e}-1}^{\infty}\frac{\bar{F}_{\gamma_k}(z)}{1+z}\mathrm{d}z-F_{\gamma_k}(2^{R_e}-1)R_e\right)F_{\gamma_e}\left(2^{R_e}-1\right)$
Fixed rate with perfect SIC	$\bar{F}_{\gamma_k}(2^{R_b}-1)$	$F_{\gamma_e}\left(2^{R_e}-1\right)$	$\Phi_k^{(P)}(R_b,R_e)=(R_b-R_e)\bar{F}_{\gamma_k}\left(2^{R_b}-1\right)F_{\gamma_e}\left(2^{R_e}-1\right)$
Fixed rate with imperfect SIC	$\prod_{i=1}^{k}\bar{F}_{\gamma_i}\left(2^{R_b}-1\right)$	$F_{\gamma_e}\left(2^{R_e}-1\right)$	$\Phi_k^{(I)}(R_b,R_e)=(R_b-R_e)\prod_{i=1}^{k}\bar{F}_{\gamma_i}\left(2^{R_b}-1\right)F_{\gamma_e}\left(2^{R_e}-1\right)$

expression (18) always satisfies that $\lim_{\lambda_e\to\infty}\Phi_k(R_e)=0$, $\forall r_p\in[0,\infty)$; *this is due to the fact that the fading distribution introduces a non-null probability of having a higher instantaneous capacity for the ED than for the legitimate user.*

Remark 2 (Impact of ED-exclusion radius, r_p*): In view of expression (18), it can be noted that the only term that depends on* r_p *is the cdf of the SNR of the worst ED,* $F_{\gamma_e}\left(2^{R_e}-1\right)$*; for* $r_p=0$*, this term is simplified to (16), whereas for* $r_p\to\infty$*, this term satisfies that* $F_{\gamma_e}\left(2^{R_e}-1\right)|_{r_p\to\infty}=1$*, that is, EDs do not have any impact on the EST performance.*

B. FIXED TRANSMISSION RATE

In case the LUs use a fixed transmission rate, the reliability constraint cannot be always guaranteed, i.e. a reliability outage must be taken into account as

$$\mathcal{O}_r(R_b)=\mathbb{P}(R_b>C_b) \tag{23}$$

Therefore, an outage may occur whenever a message transmission is either unreliable or non secure.

Regarding the reliability constraint term, $\mathcal{O}_r(R_b)$, we address in our analysis the impact of imperfect SIC and detection probability for NOMA. Note that the signals from the intra-cluster interfering users may or may not be decoded perfectly; therefore, SIC may or may not be performed in a perfect fashion. As a consequence, we distinguish two cases: perfect and imperfect SIC.

The reliability constraint term for user k in the case of perfect SIC, named as $p_k^{(P)}$, is given by

$$\begin{aligned}p_k^{(P)}(R_b) &= 1-\mathcal{O}_{r_k}(R_b)=1-\mathbb{P}(R_b>C_k)\\ &=1-\mathbb{P}(\gamma_k<2^{R_b}-1)=\bar{F}_{\gamma_k}(2^{R_b}-1)\end{aligned} \tag{24}$$

That is, the reliability constraint term represents the detection probability for user k, whose expression was obtained in (10).

Finally, the EST for user k in case of perfect SIC can be expressed as

$$\Phi_k^{(P)}(R_b,R_e)=(R_b-R_e)\bar{F}_{\gamma_k}\left(2^{R_b}-1\right)F_{\gamma_e}\left(2^{R_e}-1\right) \tag{25}$$

However, in the case of imperfect SIC, the intra-cluster interference experienced by the *kth* user depends on whether the detection for the $k-1$ nearest users were successful or not, which complicates the model significantly. In this paper we assume the worst case of imperfect SIC, which considers that the decoding of the *kth* user is always unsuccessful whenever the decoding of his relative $k-1$ closest users is unsuccessful [8]. Therefore, the reliability constraint term for the worst-case detection probability of *kth* user is given by:

$$p_k^{(I)}(R_b)=\prod_{i=1}^{k}\bar{F}_{\gamma_i}\left(2^{R_b}-1\right) \tag{26}$$

Finally, the EST for user k in case of imperfect SIC can be expressed as

$$\Phi_k^{(I)}(R_b,R_e)=(R_b-R_e)\prod_{i=1}^{k}\bar{F}_{\gamma_i}\left(2^{R_b}-1\right)F_{\gamma_e}\left(2^{R_e}-1\right) \tag{27}$$

Note that the EST expression is the same for the first NOMA user independently of the SIC assumption, i.e. $\Phi_1^{(P)}=\Phi_1^{(I)}$, since potential detection errors occur from the second user up to the *Nth* user.

A summary of secrecy metric expressions for different scenarios is shown in Table 1.

TABLE 2. Main configuration parameters.

Parameter	Value
r_c (m)	500
α	3.8
ρ_b (dB)	110
ρ_e (dB)	90
λ_e (points/m^2)	1e-5

V. NUMERICAL RESULTS

In this section, analytical results are illustrated and validated with extensive Monte Carlo simulations in order to assess the physical layer security in UL NOMA. We conduct a thorough performance comparison between the adaptive and fixed rate transmission schemes in terms of EST. Main parameters are presented in Table 2 unless otherwise stated.

A. DETECTION PROBABILITY

In the case of fixed transmission rate, the reliability constraint term (or equivalently, the detection probability) plays an important role in NOMA performance. Let us analyze first this contribution separately.

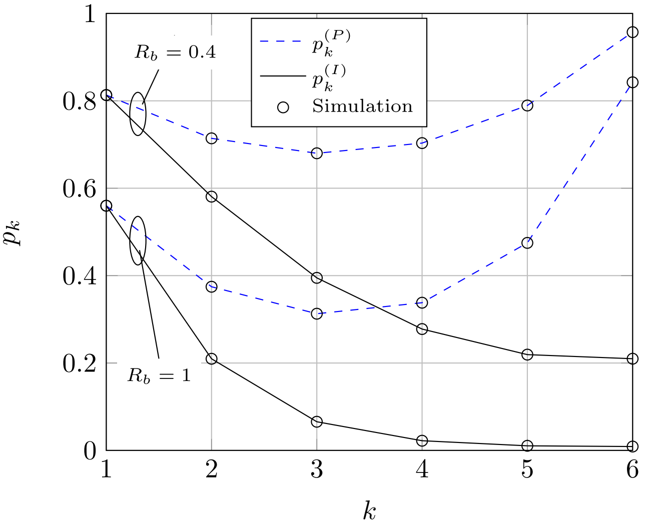

FIGURE 2. Detection probability for LUs with perfect and imperfect SIC for each user *k* with *N* = 6.

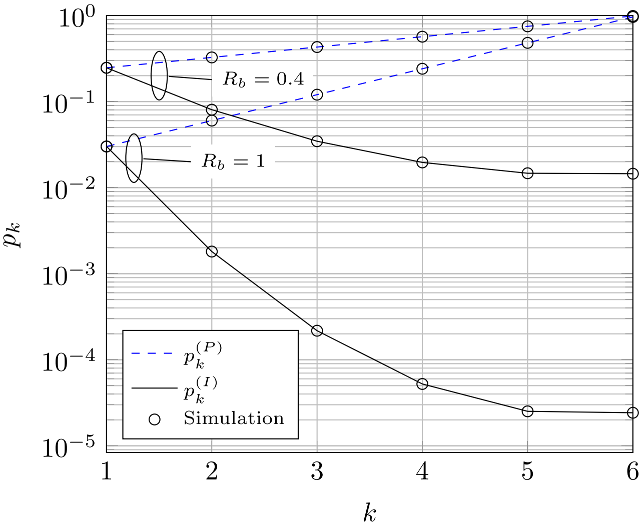

FIGURE 3. Detection probability for LUs with perfect and imperfect SIC for each user *k* with *N* = 6 (with fixed positions at $2r_c/3$).

Fig. 2 shows the detection probability results for LUs with perfect SIC, $p_k^{(P)}$, and imperfect SIC, $p_k^{(I)}$. In this case, we have considered a high number of simultaneous NOMA LUs ($N = 6$) randomly positioned according to a BPP in order to evaluate the performance as k grows. In the case of perfect SIC, results show that detection probability is not a monotonically decreasing function with k (i.e. with the distance from the *kth* user to the BS); instead, farthest LUs are boosted since the intra-cluster interference term has been partially (or totally) canceled. Note that the best result is achieved for the farthest user, $k = N = 6$, since perfect SIC assumes that intra-cluster interference is fully canceled. However, in the case of imperfect SIC, the intra-cluster interference experienced by the *kth* user depends on whether the detection for $k - 1$ nearer users were successful or not, thus providing a monotonically decreasing function with k. Note also that higher values of R_b lead to a lower detection probability.

In the case that all LUs are located at the same distance from the BS, then the theoretical analysis is simplified considerably as Eq. (28) step (a) is not conditioned on the distance r_k, leading to the following expression:

$$\bar{F}_{\gamma_k}(t)=e^{-\psi/\rho_b}\sum_{r=0}^{M-1}\sum_{k=0}^{r}\frac{\psi^r(-1)^k}{(r-k)!k!\rho_b^{r-k}}\frac{d^k}{ds^k}\left[\frac{1}{1+sr_k^{-\alpha}}\right]\Bigg|_{s=\psi}$$

with $\psi = tr_k^\alpha$, being r_k the deterministic distance from all LUs to the BS.

In the case of single antenna at the BS ($M = 1$), this expression is further simplified to:

$$\bar{F}_{\gamma_k}(t) = \frac{e^{-tr_k^{-\alpha}/\rho_b}}{(1+t)^{N-k}}$$

Note that although all the users are located at the same distance, the expression still depends on the index k, which represents the user that is being decoded iteratively.

Fig. 3 shows the detection probability results in case all LUs are located at the same distance from the BS, which has been set to $2r_c/3$. This is the average distance of random points within a disc of radius r_c. If we compare the results with previous figure, we can observe that in the case of perfect SIC, results show that detection probability is a monotonically increasing function with k; this is so because users that are decoded later experience lower intra-cluster interference as it has been previously canceled. However, in the case of imperfect SIC with all the users located at the same distance, the performance is very poor compared to the random case. Note that SIC technique requires that different message signals arrive to the BS with a sufficient power difference so that SIC may be successfully applied. In this case, this assumption is not satisfied, thus degrading significantly the performance, specially for the latest decoded users.

Fig. 4 shows the detection probability results for LUs with imperfect SIC, $p_k^{(I)}$, and for EDs, p_e, versus the SINR threshold $t = 2^{R_b} - 1$. Results for $p_k^{(I)}$ are obtained from (26) considering $N = 4$ NOMA LUs. The detection probability of EDs, p_e, is also shown for different values of the exclusion area radius, r_p. Since we consider the most detrimental ED, i.e. the one receiving the best channel quality from the LU, the detection probability results for the EDs may outperform the results for LUs as r_p is decreased, assuming a density of EDs of λ_e = 1e-5 points/m^2 (default value). The fact that the ED outperforms the LU in terms of detection probability is detrimental from a physical layer security perspective, although it may be compensated by increasing the exclusion area radius, as shown in the figure. Results also show the detection probability for LUs in case of different number of antennas at the BS, leading to an important improvement as M grows.

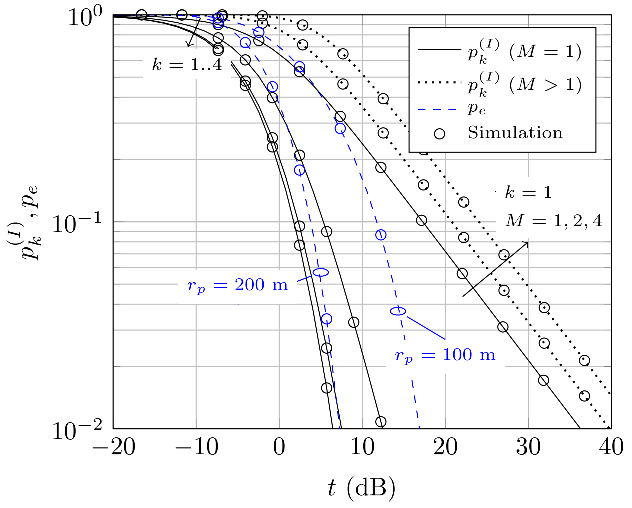

FIGURE 4. Detection probability for LUs with imperfect SIC, $p_k^{(I)}$, and for EDs, p_e, versus $t = 2^{R_b} - 1$, with $N = 4$ and M antennas.

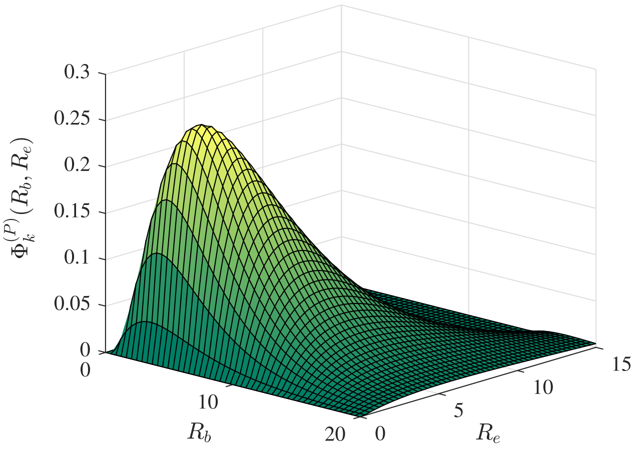

FIGURE 5. EST with perfect SIC for fixed transmission rate with $N = 2$, $k = 1$ and $r_p = 50$ m.

B. EST FOR FIXED TRANSMISSION RATE

In this section we provide EST performance results in case the BS uses a fixed transmission scheme.

Fig. 5 shows the EST for fixed rate transmission scheme and perfect SIC versus R_b and R_e, $\Phi_k^{(P)}(R_b, R_e)$. We observe that there is a unique pair of R_b and R_e that maximizes the EST. Note that EST results are zero for $R_e \geq R_b$, as defined in (1).

Fig. 6 shows the value of R_e that maximizes the EST, noted as $R_e^\dagger$, as a function of λ_e and R_b (being $R_e \leq R_b$), with $N = 2$, $k = 1$ and $r_p = 50$ m. Facing the impossibility of reaching an analytical expression of the optimum value of R_e, it has been determined numerically from (21). Note that the ratio between $R_e^\dagger$ and R_b is not linear. We also observe that a higher density of EDs requires a higher redundancy rate to optimize the EST.

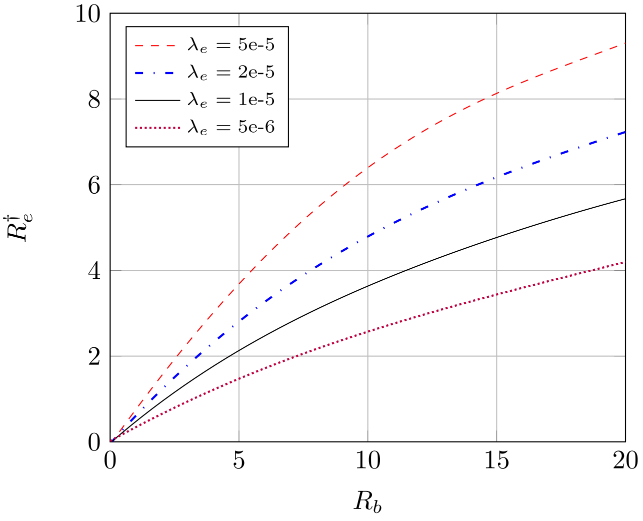

FIGURE 6. Optimum value of R_e that maximizes the EST as a function of R_b and λ_e, considering fixed transmission with $N = 2$, $k = 1$ and $r_p = 50$ m.

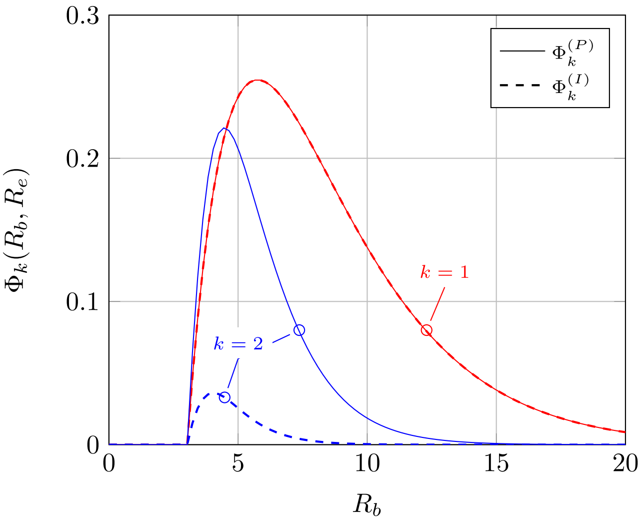

FIGURE 7. Comparison between the EST for fixed rate transmission scheme with perfect SIC and imperfect SIC, with $N = 2$, $R_e = 3$ and $r_p = 50$ m.

Fig. 7 shows a comparison between the EST for fixed rate transmission with perfect SIC, $\Phi_k^{(P)}$, and imperfect SIC, $\Phi_k^{(I)}$. EST results are shown for $N = 2$ NOMA users as a function of R_b, assuming a value of $R_e = 3$ bps and $r_p = 50$ m. We observe that the results for the first user ($k = 1$) are the same for perfect and imperfect SIC since imperfect SIC models the propagation of decoding errors from previous decoded users. We also observe that, in the case of perfect SIC, the maximum EST for the second user is not degraded significantly compared to the first user, as the larger distance to the BS is compensated by the fact that the second user does not experience (ideally) any intra-cluster interference. However, in the case of imperfect SIC, the second user is highly degraded compared to the first user due to SIC error

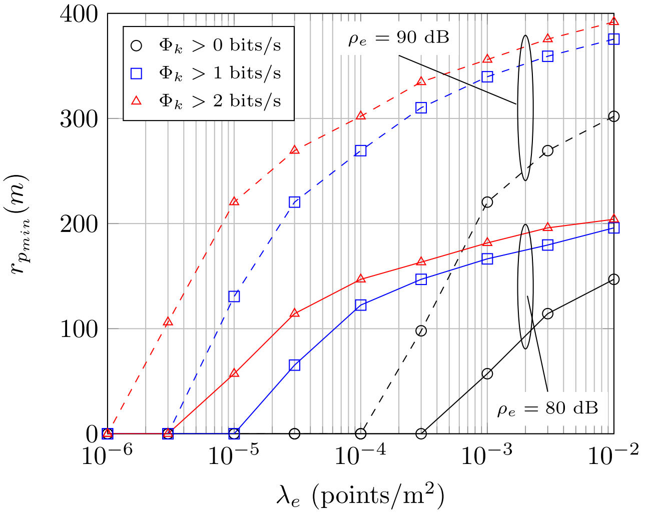

FIGURE 8. Minimum value of the ED-exclusion radius ($r_{p_{min}}$) that ensures a target EST (Φ_k) as a function of λ_e, for $N = 2$, $k = 1$ and $R_e = 1$.

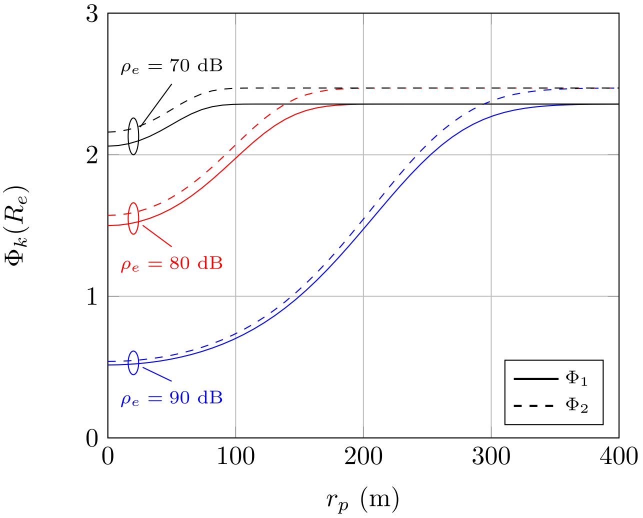

FIGURE 9. EST of the *kth* user versus r_p for adaptive transmission with $N = 2$ and $\rho_b = 110$ dB.

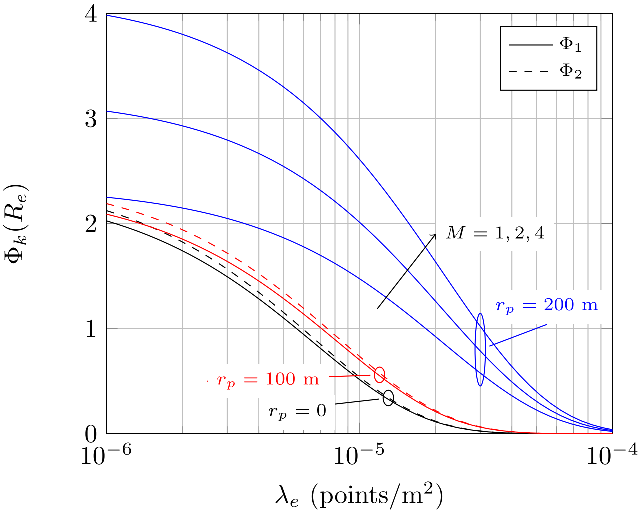

FIGURE 10. EST of the *kth* user versus λ_e for adaptive transmission with $N = 2$ and $R_e = 1$; number of antennas $M = 1, 2, 4$.

propagation from the previous decoded user. Note also that the value of R_b that maximizes the EST is different of each LU, so optimum code rate selection at the BS must be done per LU.

Fig. 8 shows the value of the minimum ED-exclusion radius ($r_{p_{min}}$) that ensures a certain EST value. Results are shown for the first user ($k = 1$), with $N = 2$, as a function of the ED density (λ_e). It is observed that a higher ED-exclusion radius is require to achieve the minimum EST target as λ_e or ρ_e is increased. It is also observed that for low λ_e values, there is no need to include an exclusion area to achieve the EST target.

C. EST FOR ADAPTIVE TRANSMISSION RATE

In this section we provide EST performance results in case the BS uses the CSI of LUs to enforce an adaptive transmission scheme.

The impact of the ED-exclusion radius on the EST is depicted in Fig. 9. We observe an increasing S-shape behavior as r_p grows, since the most detrimental ED reduces its detection capabilities for higher r_p values. Results match perfectly with Remark 2, which stated that for $r_p \to \infty$, EDs do not have any impact on the performance.

EST results as a function of the density of EDs, λ_e, is shown in Fig. 10. We observe an exponential decreasing behavior with λ_e. As stated in Remark 1, when λ_e tends to zero, the EST is mainly determined by the capacity of the LU's link; on the contrary, when λ_e tends to infinity, the EST is zero, although higher ED-exclusion radii lead to a slower EST degradation. Results also show the performance gain as the number of antennas M is increased.

Fig. 11 shows the EST for adaptive transmission for the *kth* user as a function of the transmission power (P_T) of the LU measured in dBm/Hz. We observe an optimum value of P_T, which depends on the specific values of ρ_e and k. We have considered an ED-exclusion radius of $r_p = 50$ m and an average noise power received at the BS of $\sigma_b^2 = -160$ dBm/Hz; note that the default value of $\rho_b = 110$ dB would give a value of $P_T = -50$ dBm/Hz, or equivalently, a $P_T = 23$ dBm for a bandwidth of 20 MHz, which is a typical power value for a micro-cell. Results show that very low P_T values lead to a very poor performance since the average SINR of the LUs is very low (reliability constraint); on the other hand, when the transmit power is increased, there is a optimum value above which the EST starts decreasing, since the EDs are also increasing their detecting capabilities (secrecy constraint). Results also show that higher values of $\rho_e = \frac{P_T}{\sigma_e^2}$ degrades considerably the EST. We also observe that the performance of the first and second LU differs significantly as ρ_e is increased. We must recall that in the adaptive transmission, the last user is ideally free of intra-cluster interference, and hence, its performance is limited by noise. Therefore, the second user is much more

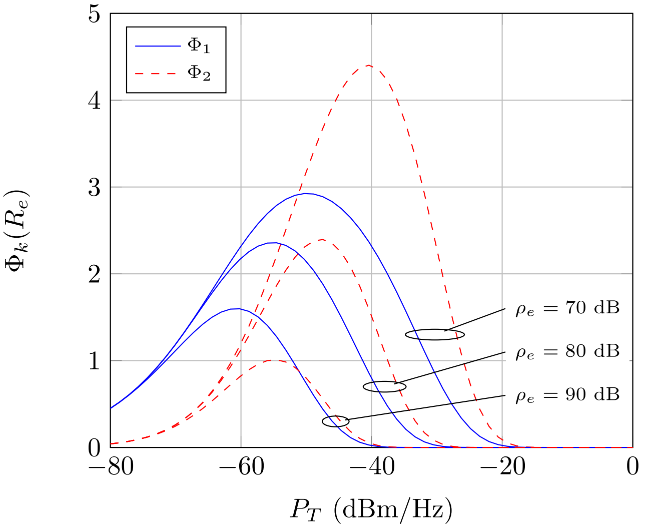

FIGURE 11. EST of the *kth* user versus the transmission power P_t for adaptive transmission as a function of ρ_e, with $N = 2$, $R_e = 1$, $r_p = 50$ m, $\lambda_e = 10^{-5}$ points/m^2 and $\sigma_b^2 = -160$ dBm/Hz.

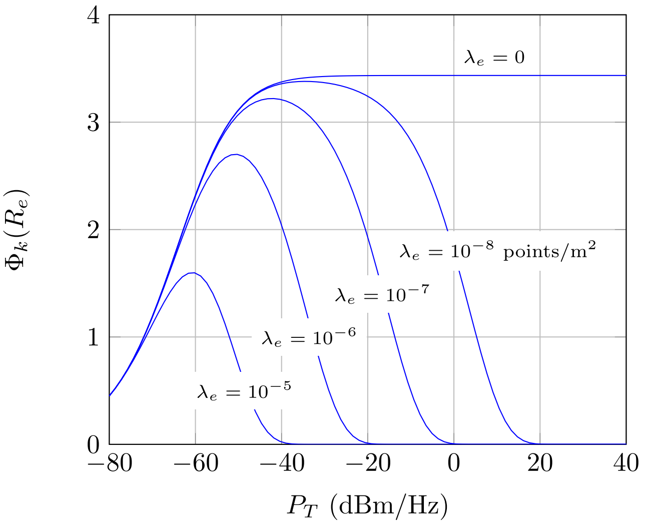

FIGURE 12. EST of the first NOMA user ($k = 1$) versus the transmission power P_t for adaptive transmission as a function of λ_e, with $N = 2$, $R_e = 1$, $\rho_e = 90$ dB, $r_p = 50$ m and $\sigma_b^2 = -160$ dBm/Hz.

affected by the value of ρ_e. In case of high noise power at EDs (low ρ_e) the second user is shown to outperform the first user despite being further from the BS.

Fig. 12 shows the EST of the first NOMA user ($k = 1$) versus the transmission power P_t for adaptive transmission as a function of the ED density, λ_e. We observe that the optimum transmit power value is very affected by λ_e. In fact, lower ED densities lead to higher EST, although an adjustment of the transmit power is critical to achieve such maximum. For the limit case of no EDs ($\lambda_e = 0$) there is no EST degradation for high P_T values, as the secrecy constraint is null.

Fig. 13 shows a comparison between the average EST for adaptive rate and fixed rate schemes as a function of ρ_b for different values of ρ_e. EST results have been obtained by considering optimum values of R_b (noted as $R_b^\dagger$) and R_e (noted as $R_e^\dagger$), showing that EST performance for the adaptive rate scheme is always superior to that of its fixed counterpart.

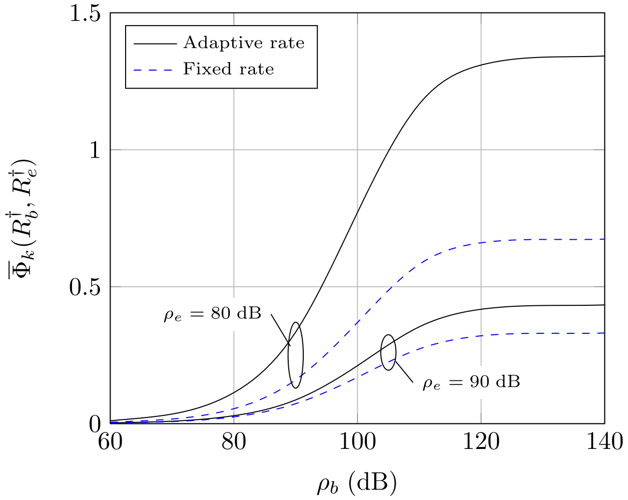

FIGURE 13. Comparison between the average EST for adaptive rate and fixed rate schemes as a function of ρ_b for different values of ρ_e.

VI. CONCLUSIONS

In this paper, we analyzed the performance of UL NOMA for a generic number of simultaneous users, both from a connection level perspective and from a physical layer security viewpoint. We considered a passive eavesdropping scenario in which the BS and LUs are not aware of their CSI, and different cases depending on whether the LUs use a fixed or an adaptive transmission scheme. We also considered the use of multiple antennas at the BS. Our analysis includes the impact of an imperfect SIC during NOMA detection and an ED-exclusion radius to enhance the secrecy metrics.

We obtained new analytical expressions for the coverage probability in the UL for LUs and EDs. In addition, we provide analytical expressions for the EST, which captures explicitly the reliability constraint and secrecy constraint of wiretap channels. Our analysis allows determining the wiretap code rates that achieve the maximum EST. Performance results also help designing optimum values of the transmit power (P_T) and the ED-exclusion radius (r_p) in order to enhance the overall EST.

Future work may include multiple antennas also at the transmitter side as well as the analysis of inter-cell interference.

APPENDIX A
PROOF OF LEMMA 1

The ccdf of the SINR for the *kth* user, $p_k(t)$, assuming M antennas at the BS, can be expressed as

$$\bar{F}_{\gamma_k}(t)$$
$$= \mathbb{P}[\gamma_k > t] \overset{(a)}{=} \int_0^{r_c} \mathbb{P}[\gamma_k > t|r_k] f_{R_k}(r_k) \mathrm{d}r_k$$
$$\overset{(b)}{=} \int_0^{r_c} \mathbb{P}\left[h_k > t(I + \rho_b^{-1}) r_k^\alpha | r_k\right] f_{R_k}(r_k) \mathrm{d}r_k$$

$$
\begin{aligned}
&= \int_0^{r_c} \mathbb{E}_I \left[\mathbb{P}\left[h_k > t(i+\rho_b^{-1}) r_k^{\alpha} | r_k, i \right]\right] f_{R_k}(r_k) \mathrm{d}r_k \\
&\overset{(c)}{=} \int_0^{r_c} e^{-t r_k^{\alpha}/\rho_b} \mathbb{E}_{I|r_k} \left[e^{-tIr_k^{\alpha}} \sum_{r=0}^{M-1} \frac{\left(t\left(I+\rho_b^{-1}\right) r_k^{\alpha}\right)^r}{r!} \middle| r_k \right] \\
&\qquad \times f_{R_k}(r_k) dr_k
\end{aligned} \tag{28}
$$

where (a) and (b) follow from the total probability theorem [41], while (c) follows from the fact that H_k has a Gamma distribution with ccdf given by (7).

Using the binomial expansion $(a+b)^r = \sum_{k=0}^{r} \binom{r}{k} a^{r-k} b^k$ and considering $\psi = t r_k^{\alpha}$, it yields

$$
\begin{aligned}
\bar{F}_{\gamma_k}(t) &= \int_0^{r_c} e^{-\psi/\rho_b} \\
&\quad \times \mathbb{E}_{I|r_k} \left[e^{-\psi I} \sum_{r=0}^{M-1} \sum_{k=0}^{r} \frac{\psi^r I^k}{(r-k)!k!} \left(\frac{1}{\rho_b}\right)^{r-k} \middle| r_k \right] \\
&\qquad \times f_{R_k}(r_k) dr_k \\
&= \int_0^{r_c} e^{-\psi/\rho_b} \sum_{r=0}^{M-1} \sum_{k=0}^{r} \frac{\psi^r}{(r-k)!k!} \left(\frac{1}{\rho_b}\right)^{r-k} \\
&\quad \times \left(\int_0^{\infty} e^{-\psi I} I^k f_I(I) dI \right) f_{R_k}(r_k) dr_k \\
&= \int_0^{r_c} e^{-\psi/\rho_b} \sum_{r=0}^{M-1} \sum_{k=0}^{r} \frac{\psi^r (-1)^k}{(r-k)!k!\rho_b^{r-k}} \\
&\quad \times \frac{d^k}{ds^k} \mathcal{L}_{I|r_k}(s) |_{s=\psi} f_{R_k}(r_k) dr_k
\end{aligned} \tag{29}
$$

The term $\mathcal{L}_{I|r_k}(s) = \mathbb{E}_{I|r_k}\left[\mathrm{e}^{I} | r_k\right]$ represents the Laplace transform of the intra-cluster interference conditioned on r_k, which can be expressed as

$$
\begin{aligned}
&\mathcal{L}_{I|r_k}(s) \\
&= \mathbb{E}_{r_j|r_k,h_j} \left[\exp\left(-s \sum_{j=k+1}^{N} h_j r_j^{-\alpha} \right) \right] \\
&= \mathbb{E}_{r_j|r_k,h_j} \left[\prod_{j=k+1}^{N} exp\left(-s h_j r_j^{-\alpha}\right) \right] \\
&\overset{(a)}{=} \prod_{j=k+1}^{N} \mathbb{E}_{r_j|r_k,h_j} \left[exp\left(-s h_j r_j^{-\alpha}\right) \right] = \mathbb{E}_{r_j|r_k} \left[\tfrac{1}{1+s r_j^{-\alpha}} \right]^{N-k} \\
&\overset{(b)}{=} \left(\int_{r_k}^{r_c} \frac{1}{1+s r_j^{-\alpha}} \frac{2r_j}{r_c^2 - r_k^2} dr_j \right)^{N-k} \\
&= \left(\frac{2\left(r_c^{\alpha+2} \Omega\left(-r_c^{\alpha}/s\right) - r_k^{\alpha+2} \Omega\left(-r_k^{\alpha}/s\right) \right)}{s\left(r_c^2 - r_k^2\right)(\alpha+2)} \right)^{N-k}
\end{aligned} \tag{30}
$$

being $\Omega(x) = {}_2F_1\left[1, \frac{\alpha+2}{\alpha}, 2+\frac{2}{\alpha}, x\right]$. Step (a) comes from the fact that the fading is independent of the BPP and, although *jth* users' location are correlated with *kth* user when their distances are ordered, the computation of the interference can be obtained considering that the $N-k$ NOMA interfering users are located within a disk whose inner radius is r_k and outer radius r_c. Step (b) comes from the fact that the pdf of the distance from a randomly located point within that disk is given by $f_{R_j|R_k}(r_j|r_k) = 2r_j / \left(r_c^2 - r_k^2\right)$. Note that the MRC combination does not change the distribution of the interference in our scenario, as stated in [27], [42].

In [43], the marginal pdf of the *kth* nearest point to the origin of a BPP is given. In particular, this work shows that, in a BPP consisting of N points randomly distributed in a 2-dimensional ball of radius r_c centered at the origin, the Euclidean distance R_k from the origin to its *kth* nearest point follows a generalized beta distribution

$$
f_{R_k}(r_k) = \frac{2}{r_c} \frac{\Gamma\left(k+\frac{1}{2}\right)\Gamma(N+1)}{\Gamma(k)\,\Gamma\left(N+\frac{3}{2}\right)} \beta\left(\frac{r_k^2}{r_c^2}; k+\frac{1}{2}, N-k+1 \right) \tag{31}
$$

Substituting (30) and (31) into (28) the proof is complete.

REFERENCES

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C.-L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[2] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 938–953, Apr. 2016.

[3] H. Tabassum, M. S. Ali, E. Hossain, M. J. Hossain, and D. I. Kim, "Non-orthogonal multiple access (NOMA) in cellular uplink and downlink: Challenges and enabling techniques," 2016, *arXiv:1608.05783*. [Online]. Available: https://arxiv.org/abs/1608.05783

[4] Y. Endo, Y. Kishiyama, and K. Higuchi, "Uplink non-orthogonal access with MMSE-SIC in the presence of inter-cell interference," in *Proc. Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2012, pp. 261–265.

[5] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[6] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7244–7257, Nov. 2016.

[7] N. Zhang, J. Wang, G. Kang, and Y. Liu, "Uplink nonorthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 458–461, Mar. 2016.

[8] H. Tabassum, E. Hossain, and J. Hossain, "Modeling and analysis of uplink non-orthogonal multiple access in large-scale cellular networks using poisson cluster processes," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3555–3570, Aug. 2017.

[9] F. A. Rabee, K. Davaslioglu, and R. Gitlin, "The optimum received power levels of uplink non-orthogonal multiple access (NOMA) signals," in *Proc. IEEE 18th Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2017, pp. 1–4.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[11] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[13] X. Liu, "Probability of strictly positive secrecy capacity of the Rician–Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[14] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.
[15] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.
[16] 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, 1st Quart., 2017.
[17] 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.
[18] 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.
[19] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.
[20] 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 *Proc. IEEE Int. Conf. Commun.*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[21] 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.
[22] 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, Jul. 2018.
[23] 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.
[24] H. Lei, J. Zhang, K. H. Park, P. Xu, Z. Zhang, G. Pan, and M. S. Alouini, "Secrecy outage of max–min TAS scheme in MIMO-NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.
[25] K. Jiang, T. Jing, Y. Huo, F. Zhang, and Z. Li, "SIC-based secrecy performance in uplink NOMA multi-eavesdropper wiretap channels," *IEEE Access*, vol. 6, pp. 19664–19680, 2018.
[26] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.
[27] A. Shah and A. M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1454–1463, Jul. 2000.
[28] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions*. New York, NY, USA: Dover, 1965.
[29] E. Hildebrand, *Introduction to Numerical Analysis*. New York, NY, USA: Dover, 1987.
[30] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications* (Wiley Series in Probability and Statistics). Hoboken, NJ, USA: Wiley, 2013.
[31] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.
[32] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.
[33] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2069–2072, Nov. 2015.
[34] H. Yu, S. Guo, Y. Yang, and B. Xiao, "Optimal target secrecy rate and power allocation policy for a swipt system over a fading wiretap channel," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3291–3302, Dec. 2018.
[35] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.
[36] M. Yang, B. Zhang, Y. Huang, N. Yang, D. B. da Costa, and D. Guo, "Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11394–11398, Dec. 2017.
[37] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, Mar. 2017.
[38] K. Jiang, T. Jing, F. Zhang, Y. Huo, and Z. Li, "ZF-SIC based individual secrecy in SIMO multiple access wiretap channel," *IEEE Access*, vol. 5, pp. 7244–7253, 2017.
[39] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum secrecy throughput of MIMOME FSO communications with outage constraints," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3487–3497, May 2018.
[40] D. Chen, Y. Cheng, W. Yang, J. Hu, and Y. Cai, "Physical layer security in cognitive untrusted relay networks," *IEEE Access*, vol. 6, pp. 7055–7065, 2017.
[41] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes* (McGraw-Hill Series in Electrical Engineering: Communications and Signal Processing). New York, NY, USA: McGraw-Hill, 2002.
[42] J. M. Romero-Jerez and A. J. Goldsmith, "Receive antenna array strategies in fading and interference: An outage probability comparison," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 920–932, Mar. 2008.
[43] S. Srinivasa and M. Haenggi, "Distance distributions in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.

GERARDO GOMEZ received the B.Sc. and Ph.D. degrees in telecommunication engineering from the University of Málaga, Spain, in 1999 and 2009, respectively. From 2000 to 2005, he was with Nokia Networks and Optimi Corporation (acquired by Ericsson), leading the area of quality of service (QoS) for 2G and 3G cellular networks. In 2005, he joined the University of Málaga, where he is currently an Associate Professor and the Deputy Director of the Communications Engineering Department. His research interests include the field of mobile communications, especially physical layer security, stochastic geometry, interference management, and QoS/QoE evaluation for multimedia services.

FRANCISCO J. MARTIN-VEGA is currently pursuing the Ph.D. degree in wireless engineer with Keysight Technologies. From 2011 to 2017, he was an Associate Researcher with the University of Málaga, Spain, where he participated in contracts with several industry partners related to cellular and satellite communications. His research activity has focused on the mathematical modeling of communication systems. He has been awarded with the best Master's and Ph.D. Theses by the Spanish Official Telecommunication Engineering School (COIT), in 2012 and 2018.

F. JAVIER LOPEZ-MARTINEZ (SM'17) received the M.Sc. and Ph.D. degrees in telecommunication engineering from the Universidad de Málaga, Spain, in 2005 and 2010, respectively.

In 2005, he joined the Communication Engineering Department, Universidad de Málaga, as an Associate Researcher. He was a Marie Curie Postdoctoral Fellow with the Wireless Systems Laboratory, Stanford University, from 2012 to 2014, and the Universidad de Málaga, from 2014 to 2015. Since 2015, he has been an Assistant Professor with the Communication Engineering Department, Universidad de Málaga. He has been a Visiting Researcher with University College London, since 2010, and Queen's University Belfast, since 2018. His research interests include the diverse set of topics in the wide areas of communication theory and wireless communications: stochastic processes, wireless channel modeling, random matrix theory, physical layer security, and wireless powered communications. He received several research awards, including the Best Paper Award in the Communication Theory Symposium at IEEE Globecom 2013, the IEEE Communications Letters Exemplary Reviewer Certificate, in 2014, and the IEEE Transactions on Communications Exemplary Reviewer Certificate, in 2015 and 2017. He is also an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, in the area of wireless communications.

YUANWEI LIU (S'13–M'16–SM'19) received the B.S. and M.S. degrees from the Beijing University of Posts and Telecommunications, in 2011 and 2014, respectively, and the Ph.D. degree in electrical engineering from the Queen Mary University of London, U.K., in 2016.

He was with the Department of Informatics, King's College London, from 2016 to 2017, where he was a Postdoctoral Research Fellow. He has been a Lecturer (Assistant Professor) with the School of Electronic Engineering and Computer Science, Queen Mary University of London, since 2017. His research interests include 5G and beyond wireless networks, the Internet of Things, machine learning, and stochastic geometry. He has served as a TPC Member for many IEEE conferences, such as GLOBECOM and ICC. He has served as the Publicity Co-Chair for VTC2019-Fall. He received the Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters, in 2015, the IEEE Transactions on Communications, in 2016 and 2017, and the IEEE Transactions on Wireless Communications, in 2017. He has been serving on the Editorial Board as an Editor of the IEEE Transactions on Communications, IEEE Communications Letters, and IEEE Access. He also serves as the Guest Editor for the IEEE JSTSP special issue on Signal Processing Advances for Non-Orthogonal Multiple Access in Next Generation Wireless Networks.

MAGED ELKASHLAN received the Ph.D. degree in electrical engineering from The University of British Columbia, Canada, in 2006.

From 2007 to 2011, he was with the Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During that time, he held visiting appointments at the University of New South Wales and the University of Technology Sydney. In 2011, he joined the School of Electronic Engineering and Computer Science, Queen Mary University of London, U.K. His research interests include the broad areas of communication theory and statistical signal processing. He received the Best Paper Awards at the IEEE Vehicular Technology Conference (VTC-Spring), in 2013, the IEEE International Conference on Communications (ICC), in 2014 and 2016, and the International Conference on Communications and Networking in China (CHINACOM), in 2014. He currently serves as an Editor for the IEEE Transactions on Wireless Communications and IEEE Transactions on Vehicular Technology.