Enhancing the Physical Layer Security of Non-orthogonal Multiple Access in Large-scale Networks

Yuanwei Liu, *Student Member, IEEE,* Zhijin Qin, *Student Member, IEEE,*
Maged Elkashlan, *Member, IEEE,* Yue Gao, *Senior Member, IEEE,* and
Lajos Hanzo, *Fellow, IEEE*

Abstract

This paper investigates the physical layer security of non-orthogonal multiple access (NOMA) in large-scale networks with invoking stochastic geometry. Both single-antenna and multiple-antenna aided transmission scenarios are considered, where the base station (BS) communicates with randomly distributed NOMA users. In the single-antenna scenario, we adopt a protected zone around the BS to establish an eavesdropper-exclusion area with the aid of careful channel-ordering of the NOMA users. In the multiple-antenna scenario, artificial noise is generated at the BS for further improving the security of a beamforming-aided system. In order to characterize the secrecy performance, we derive new exact expressions of the security outage probability for both single-antenna and multiple-antenna aided scenarios. To obtain further insights, 1) for the single antenna scenario, we perform secrecy diversity order analysis of the selected user pair. The analytical results derived demonstrate that the secrecy diversity order is determined by the specific user having the worse channel condition among the selected user pair; and 2) for the multiple-antenna scenario, we derive the asymptotic secrecy outage probability, when the number of transmit antennas tends to infinity. The results derived indicate that the channels of the eavesdroppers are independent of the number of transmit antennas for sufficiently large antenna arrays. Monte Carlo simulations are provided for verifying the analytical results derived and to show that: i) The security performance of the NOMA networks can be improved by invoking the protected zone and by generating artificial noise at the BS; and ii) The asymptotic secrecy outage probability is close to the exact secrecy outage probability, when the number of antennas at the BS is around 20.

Index Terms

Artificial noise, physical layer security, non-orthogonal multiple access, stochastic geometry

Y. Liu, Z. Qin, M. Elkashlan, and Y. Gao are with Queen Mary University of London, London, UK (email:{yuanwei.liu, z.qin, maged.elkashlan, yue.gao}@qmul.ac.uk).

L. Hanzo is with University of Southampton, Southampton, UK (email:lh@ecs.soton.ac.uk).

I. INTRODUCTION

The unprecedented expansion of new Internet-enabled smart devices, applications and services is expediting the development of the fifth generation (5G) networks, which aim for substantially increasing the throughput of the fourth generation (4G) networks. In addition to the key technologies such as large-scale multiple-input multiple-output (MIMO) solutions, heterogeneous networks and millimeter wave, as well as novel multiple access (MA) techniques should be invoked for improving the spectral efficiency [1]. Non-orthogonal multiple access (NOMA), which has been recently proposed for 3GPP Long Term Evolution (LTE) [2], is expected to have a superior spectral efficiency. It has also been pointed out that NOMA has the potential to be integrated with existing MA paradigms, since it exploits the new dimension of the power domain. The key idea of NOMA is to ensure that multiple users can be served within a given resource slot (e.g., time/frequrecy/code), by applying successive interference cancellation (SIC).

Hence NOMA techniques have received remarkable attention both in the world of academia and industry [3–7]. Ding *et al.* [3] investigated the performance of the NOMA downlink for randomly roaming users. It was shown that NOMA is indeed capable of achieving a better performance than their traditional orthogonal multiple access (OMA) counter parts. By considering the user fairness of a NOMA system, a user-power allocation optimization problem was addressed by Timotheou and Krikidis [4]. A cooperative simultaneous wireless power transfer (SWIPT) aided NOMA protocol was proposed by Liu *et al.* [5], where a NOMA user benefitting from good channel conditions acts as an energy harvesting source in order to assist a NOMA user suffering from poor channel conditions. To further improve the performance of NOMA systems, multiple antennas were introduced in [6, 7]. More particularly, the application of multiple-input single-output (MISO) solution to NOMA was investigated by Choi *et al.* [6], where a two-stage beamforming strategy was proposed. Power optimization was invoked by Sun *et al.* [7] for maximizing the ergodic capacity of MIMO aided NOMA systems.

Given the broadcast nature of wireless transmissions, the concept of physical (PHY) layer security (PLS), which was proposed by Wyner as early as 1975 from an information-theoretical perspective [8], has sparked of wide-spread recent interest. To elaborate, PLS has been considered from a practical perspective in [9–13]. Specifically, robust beamforming transmission was conceived in conjunction with applying artificial noise (AN) for mitigating the impact of imperfect channel state information (CSI) in MIMO wiretap channels was proposed by Mukherjee and Swindlehurst [9]. Ding *et al.* [10] invoked relay-aided cooperative diversity for increasing the capacity of the desired link. More particularly, the impact of eavesdroppers on the diversity and multiplexing gains was investigated both in single-antenna and multiple-antenna scenarios. Additionally, the tradeoffs between secure performance and reliability in the presence of eavesdropping attacks was identified by Zou *et al.* [12]. Furthermore, the physical layer security of D2D communication in large-scale cognitive radio networks was investigated by Liu *et al.* [13] with invoking a wireless power transfer model, where the positions of the power beacons, the legitimate and the eavesdropping nodes were modeled using stochastic geometry.

Recently, various PHY layer techniques, such as cooperative jamming [14] and AN [15] aided solutions were proposed for improving the PLS, even if the eavesdroppers have better channel conditions than the legitimate receivers. A popular technique is to generate AN at the transmitter for degrading the eavesdroppers' reception, which was proposed by Goel and Negi in [15]. In contrast to the traditional view, which regards noise and interference as a detrimental effect, generating AN at the transmitter is capable of improving the security, because it degrades the channel conditions of eavesdroppers without affecting those of the legitimate receivers. An AN-based multi-antenna aided secure transmission scheme affected by colluding eavesdroppers was considered by Zhou and McKay [16] for the scenarios associated both with perfect and imperfect CSI at both the transmitter and receiver. As a further development, the secrecy enhancement achieved in wireless Ad Hoc networks was investigated by Zhang *et al.* [17], with the aid of both beamforming and sectoring techniques.

A. Motivation and Contribution

As mentioned above, PLS has been studied in various scenarios, but not in NOMA, which motivates this contribution. In this paper, we specifically consider the scenario of large-scale networks, where a base station (BS) supports randomly roaming NOMA users. In order to avoid sophisticated high-complexity message detection at the receivers, a user pairing technique is adopted for ensuring that only two users share a specific orthogonal resource slot, which can be readily separated by low-complexity SIC. A random number of eavesdroppers are randomly positioned on an infinite two-dimensional plane according to a homogeneous Poisson point process (PPP). An eavesdropper-exclusion zone is introduced around the BS for improving the secrecy performance of the large-scale networks considered in which no eavesdroppers are allowed to roam. This ‘disc’ was referred to as a protected zone in [17–19]. Specifically, we consider both a single-antenna scenario and a multiple-antenna scenario at the base station (BS). 1) For the single-antenna scenario, M NOMA users are randomly roaming in an finite disc (user zone) with the quality-order of their channel conditions known at the BS. For example, the m-th NOMA user is channel-quality order of m. In this case, the m-th user is paired with the n-th user for transmission within the same resource slot; 2) For the multiple-antenna scenario, we invoke beamforming at the BS for generating AN. In order to reduce the complexity of channel ordering of MISO channels for NOMA, we partitioned the circular cell of Fig. 1 into an an internal disc and an external ring. We select one user from the internal disc and another from the external ring to be paired together for transmission within the same resource slot using a NOMA protocol. The primary contributions of this paper are as follows:

- We investigate the secrecy performance of large-scale NOMA networks both for a single-antenna aided and a multiple-antenna assisted scenario at the BS. A protected zone synonymously referred to as the eavesdropper-exclusion area, is invoked in both scenarios for improving the PLS. Additionally, we propose to generate AN at the BS in the multiple-antenna aided scenario for further enhancing the secrecy performance.
- For the single-antenna scenario, we derive the exact analytical expressions of the secrecy outage probability (SOP) of the selected pair of NOMA users, when relying on channel ordering. We then further extend on the secrecy diversity analysis and derive the expressions of asymptotic SOP. The results derived confirm that: 1) for the selected pair, the m-th user is capable of attaining a secrecy diversity order of m; 2) the secrecy diversity order is determined by the one associated with the worse channel condition between the paired users.
- For the multiple-antenna scenario, we derive the exact analytical expressions of the SOP in conjunction with AN generated at the BS. To gain further insights, we assume having a large antenna array and derive the expressions of SOP, when the number of antennas tends to infinity. The results derived confirm that increasing the number of antennas has no effect on the received signal-to-interference-plus-noise ratio (SINR) at the eavesdroppers, when the BS is equipped with a large antenna array.

- It is shown that: 1) the SOP can be reduced both by extending the protected zone and by generating AN at the BS; 2) the asymptotic SOP results of our large antenna array analysis is capable of closely approximating the exact secrecy outage provability; 3) there is an optimal desired signal-power and AN power sharing ratio, which minimizes the SOP in the multi-antenna scenario.

B. Organization

The rest of the paper is organized as follows. In Section II, a single-antenna transmission scenario is investigated in random wireless networks, where channel ordering of the NOMA users is relied on. In Section III, a multiple-antenna transmission scenario is investigated, which relies on generating AN at the BS. Our numerical results are presented in Section IV for verifying our analysis, which is followed by our conclusions in Section V.

II. PHYSICAL LAYER SECURITY IN RANDOM WIRELESS NETWORKS WITH CHANNEL ORDERING

As shown in Fig. 1, we focus our attention on a secure downlink communication scenario. In the scenario considered, a BS communicates with M legitimate users (LUs) in the presence of eavesdroppers (Es). We assume that the M users are divided into $M/2$ orthogonal pairs. For each pair, the NOMA transmission protocol is invoked. It is assumed that BS is located at the center of a disc, denoted by $\mathcal{D}$, which has a coverage radius of R_D (which is defined as the user zone for NOMA [3]). The M randomly roaming LUs are uniformly distributed within the disc. A random number of Es is distributed in an infinite two-dimensional plane. The spatial distribution of all Es is modeled using a homogeneous PPP, which is denoted by Φ_e associated with the density λ_e. It is assumed that the Es can be detected, provided that they are close enough to BS. Therefore, an E-exclusion area having a radius of r_p is introduced. Additionally, all channels are assumed to impose quasi-static Rayleigh fading, where the channel coefficients are constant for each transmission block, but vary independently between different blocks.

Without loss of generality, it is assumed that all the channels between the BS and LUs obey $|h_1|^2 \leq \cdots |h_m|^2 \leq \cdots |h_n|^2 \leq \cdots |h_M|^2$. Both the the small-scale fading and the path loss are incorporated into the ordered channel gain. Again, we assume that the m-th user and the n-th user ($m < n$) are paired for transmission in the same resource slot. With loss of generality, we

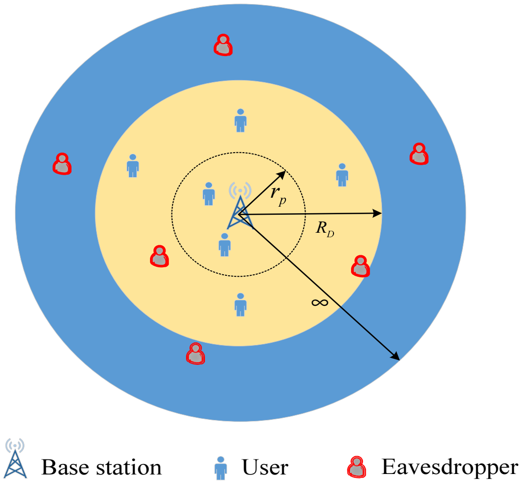


Fig. 1: Network model for secure NOMA transmission in single-antenna scenario.

focus our attention on a single selected pair of users in the rest of the paper. In the NOMA transmission protocol, more power should be allocated to the user suffering from worse channel condition [1, 2]. Therefore, the power allocation coefficients satisfy the conditions that $a_m \geq a_n$ and $a_m + a_n = 1$. SIC is invoked for detecting the stronger user first. Based on the aforementioned assumptions, the instantaneous SINR of the m-th user and the signal-to-noise ratio (SNR) of the n-th user can be written as:

$$\gamma_{B_m} = \frac{a_m |h_m|^2}{a_n |h_m|^2 + \frac{1}{\rho_b}}, \tag{1}$$

$$\gamma_{B_n} = \rho_b a_n |h_n|^2, \tag{2}$$

respectively. We introduce the convenient concept of transmit SNR $\rho_b = \frac{P_T}{\sigma_b^2}$, where P_T is the transmit power at the BS and σ_b^2 is the variance of the additive white Gaussian noise (AWGN) at the LUs, noting that this is not a physically measurable quantity owing to their geographic separation. In order to ensure that the m-th user can successfully decode the message of the n-th user, the condition of $a_m \geq \left(2^{R_m} - 1\right) a_n$ should be satisfied. Additionally, a bounded path loss model is used for guaranteeing that there is a practical path-loss, which is higher than one even for small distances.

We consider the worst-case scenario of large-scale networks, in which the Es are assumed to have strong detection capabilities. Specifically, by applying multiuser detection techniques, the multiuser data stream received from BS can be distinguished by the Es. In the scenario considered, all the downlink CSIs are assumed to be known at BS. Under this assumption, the most detrimental E is not necessarily the nearest one, but the one having the best channel to BS. Therefore, the instantaneous SNR of detecting the information of the m-th user and the n-th user at the most detrimental E can be expressed as follows:

$$\gamma_{E_\kappa} = \rho_e a_\kappa \max_{e \in \Phi_e, d_e \geq r_p} \left\{ |g_e|^2 L\left(d_e\right) \right\}. \tag{3}$$

It is assumed that $\kappa \in \{m, n\}$, $\rho_e = \frac{P_A}{\sigma_e^2}$ is the transmit SNR with σ_e^2 being the variance of the AWGN at Es. Additionally, g_e is defined as the small-scale fading coefficient associated with $g_e \sim \mathcal{CN}(0,1)$, $L\left(d_e\right) = \frac{1}{d_e^\alpha}$ is the path loss, and d_e is the distance from Es to BS. Note that due to the existence of the E-exclusion area (we assume $r_p > 1$), it is not required to bound the path loss for Es since d_e will always be larger than one.

A. New Channel Statistics

In this subsection, we derive several new channel statistics for LUs and Es, which will be used for deriving the secrecy outage probability in the next subsection.

Lemma 1. Assuming M randomly located NOMA users in the disc of Fig. 1, the cumulative distribution function (CDF) $F_{\gamma_{B_n}}$ of the n-th LU is given by

$$F_{\gamma_{B_n}}\left(x\right) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \sum_{\tilde{S}_n^p} \binom{n+p}{q_0+\cdots+q_K} \left(\prod_{K=0}^{K} b_k^{q_k} \right) e^{-\sum\limits_{k=0}^{K} q_k c_k \frac{x}{\rho_b a_n}}, \tag{4}$$

where K is a complexity-vs-accuracy tradeoff parameter, $b_k = -\omega_K \sqrt{1-\phi_k^2}\left(\phi_k+1\right)$, $b_0 = -\sum\limits_{k=1}^{K} b_k$, $c_k = 1 + \left[\frac{R_D}{2}\left(\phi_k+1\right)\right]^\alpha$, $\omega_K = \frac{\pi}{K}$, *and* $\phi_k = \cos\left(\frac{2k-1}{2K}\pi\right)$,
$\tilde{S}_n^p = \left\{ (q_0, q_1, \cdots, q_K) | \sum\limits_{i=0}^{K} q_i = n+p \right\}$, $\binom{n+p}{q_0+\cdots+q_K} = \frac{(n+p)!}{q_0!\cdots q_K!}$ and $\varphi_n = \frac{M!}{(M-n)!(n-1)!}$.

Proof: See Appendix A . ■

Lemma 2. Assuming M randomly positioned NOMA users in the disc of Fig. 1, the CDF $F_{\gamma_{B_m}}$

of the m-th LU is given in (5)

$$\begin{aligned} F_{\gamma_{B_m}}(x) =& U\left(x-\frac{a_m}{a_n}\right)+U\left(\frac{a_m}{a_n}-x\right)\varphi_m \\ & \times \sum_{p=0}^{M-m}\binom{M-m}{p}\frac{(-1)^p}{m+p}\sum_{\tilde{S}_m^p}\binom{m+p}{q_0+\cdots+q_K}\left(\prod_{k=0}^{K}b_k^{q_k}\right)e^{-\sum\limits_{k=0}^{K}q_k c_k\frac{x}{(a_m-a_n x)\rho_b}}. \end{aligned} \quad (5)$$

where $U(x)=\begin{cases}1, x>0\\ 0, x\le 0\end{cases}$ is the unit step function , and $\tilde{S}_m^p=\left\{(q_0,q_1,\cdots,q_K)\middle|\sum\limits_{i=0}^{K}q_i=m+p\right\}$.

Proof: Based on (1)*, the CDF of* $F_{\gamma_{B_m}}(x)$ *can be expressed as*

$$F_{\gamma_{B_m}}(x)=\begin{cases}\underbrace{\Pr\left\{|h_m|^2<\frac{x}{(a_m-a_n x)\rho_b}\right\}}_{\Phi_m}, x<\frac{a_m}{a_n}\\ 1, x\ge\frac{a_m}{a_n}\end{cases}. \quad (6)$$

To derive the CDF of $F_{\gamma_{B_m}}(x)$*,* Φ_m *can be expressed as* $\Phi_m=F_{|h_m|^2}\left(\frac{x}{(a_m-a_n x)\rho_b}\right)$*. Based on* (A.5)*, interchanging the parameters* $m\to n$ *and applying* $y=\frac{x}{(a_m-a_n x)\rho_b}$*, we obtain*

$$\Phi_m=\varphi_m\sum_{p=0}^{M-m}\binom{M-m}{p}\frac{(-1)^p}{m+p}\sum_{\tilde{S}_m^p}\binom{m+p}{q_0+\cdots+q_K}\left(\prod_{k=0}^{K}b_k^{q_k}\right)e^{-\sum\limits_{k=0}^{K}q_k c_k\frac{x}{(a_m-a_n x)\rho_b}}. \quad (7)$$

By substituting (7) *into* (6)*, with the aid of the unit step function, the CDF of* $F_{\gamma_{B_m}}(x)$ *can be obtained. The proof is completed.* ■

Lemma 3. Assuming that the eavesdroppers obey the PPP distribution and the E-exclusion zone has a radius of r_p, the probability density function (PDF) $f_{\gamma_{E_\kappa}}$ of the most detrimental E *(where* $\kappa\in\{m,n\}$ *)* is given by

$$f_{\gamma_{E_\kappa}}(x)=\mu_{\kappa 1}e^{-\frac{\mu_{\kappa 1}\Gamma(\delta,\mu_{\kappa 2}x)}{x^\delta}}\left(\frac{\mu_{\kappa 2}^{\delta}e^{-\mu_{\kappa 2}x}}{x}+\frac{\delta\Gamma(\delta,\mu_{\kappa 2}x)}{x^{\delta+1}}\right), \quad (8)$$

where $\mu_{\kappa 1}=\delta\pi\lambda_e(\rho_e a_\kappa)^\delta, \mu_{\kappa 2}=\frac{r_p^\alpha}{\rho_e a_\kappa}$, $\delta=\frac{2}{\alpha}$ and $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function.

Proof: To derive the PDF of $f_{\gamma_{E_\kappa}}(x)$*, we have to compute the CDF of* $F_{\gamma_{E_\kappa}}$ *firstly as*

$$F_{\gamma_{E_\kappa}}(x) = E_{\Phi_e}\left\{ \prod_{e\in\Phi_e, d_e\geq r_p} F_{|g_e|^2}\left(\frac{x d_e^\alpha}{\rho_e a_\kappa}\right)\right\}. \tag{9}$$

By applying the generating function [20], (9) *can be rewritten as*

$$F_{\gamma_{E_\kappa}}(x) = \exp\left[-\lambda_e \int_{R^2}\left(1 - F_{|g_e|^2}\left(\frac{x d_e^\alpha}{\rho_e a_\kappa}\right)\right) r dr\right] = \exp\left[-2\pi\lambda_e \int_{r_p}^{\infty} r e^{-\frac{x}{\rho_e a_\kappa} r^\alpha} dr\right]. \tag{10}$$

By applying [21, Eq. (3.381.9)], we arrive at:

$$F_{\gamma_{E_\kappa}}(x) = e^{-\frac{\delta\pi\lambda_e(\rho_e a_\kappa)^\delta \Gamma\left(\delta, \frac{x r_p^\alpha}{\rho_e a_\kappa}\right)}{x^\delta}}. \tag{11}$$

By taking the derivative of the CDF $F_{\gamma_{E_\kappa}}(x)$ *in* (11)*, we obtain the PDF* γ_{E_κ} *in* (8)*. The proof is completed.* ■

B. Secrecy Outage Probability

In the networks considered, the capacity of the LU's channel for the κ-h user ($\kappa \in \{m, n\}$) is given by $C_{B_\kappa} = \log_2(1 + \gamma_{B_\kappa})$, while the capacity of the E's channel for the κ-th user is quantified by $C_{E_\kappa} = \log_2(1 + \gamma_{E_\kappa})$. It is assumed that the length of the block is sufficiently high for facilitating the employment of capacity-achieving codes within each block. Additionally, the fading block length of the main channel and of the eavesdropper's channel are assumed to be the same. As such, according to [22], the secrecy rate of the m-th and of the n-th user can be expressed as

$$I_m = [C_{B_m} - C_{E_m}]^+, \tag{12}$$

$$I_n = [C_{B_n} - C_{E_n}]^+, \tag{13}$$

for $C_{B_m} > C_{E_m}$ and $C_{B_n} > C_{E_n}$, respectively, where we have $[x]^+ = \max\{x, 0\}$. Here, the secrecy rates of LUs are strictly positive [23]. Recall that the Es' CSIs are not known at the BS, hence the BS can only send information to LUs at a constant rate. Considering the κ-th user as an example, if $R_\kappa < I_\kappa$, the information with a rate of R_κ is conveyed in perfect secrecy. By contrast, for the case of $R_\kappa > I_\kappa$ the information-theoretic security is compromised. Motivated by this, the secrecy outage probability is used as our secrecy performance metric in this paper.

Given the expected secrecy rate R_κ of the κ-th user, a secrecy outage event is declared, when the secrecy rate I_κ drops below R_κ. As such, based on (12) and according to [23], the SOP for the m-th user is given by

$$P_m\left(R_m\right) = \int_0^\infty f_{\gamma_{E_m}}\left(x\right) F_{\gamma_{B_m}}\left(2^{R_m}\left(1+x\right)-1\right) dx. \tag{14}$$

Based on the assumption of $a_m \geq \left(2^{R_m}-1\right) a_n$, we consider the SOP under the condition that the connection between BS and LUs can be established. Upon using the results of **Lemma 2** and **Lemma 3**, as well as substituting (5) and (8) into (14), after some further mathematical manipulations, we can express the SOP of the m-th user according to the following theorem:

Theorem 1. Assuming that the LUs position obeys the PPP for the ordered channels of the LUs, the SOP of the m-th user is given by (15)

$$\begin{aligned} P_m\left(R_m\right) =& 1 - e^{-\frac{\mu_{m1}\Gamma\left(\delta,\tau_m\mu_{m2}\right)}{{\tau_m}^{\delta}}} + \varphi_m \sum_{p=0}^{M-m} \binom{M-m}{p} \frac{(-1)^p}{m+p} \sum_{\tilde{S}_m^p} \binom{m+p}{q_0+\cdots+q_K} \left(\prod_{k=0}^{K} b_k^{q_k}\right) \\ & \times \int_0^{\tau_m} \mu_{m1}\left(\frac{\mu_{m2}^{\delta} e^{-\mu_{m2}x}}{x} + \frac{\delta\Gamma\left(\delta,\mu_{m2}x\right)}{x^{\delta+1}}\right) e^{-\frac{\mu_{m1}\Gamma\left(\delta,\mu_{m2}x\right)}{x^{\delta}} - \sum\limits_{k=0}^{K} q_k c_k \frac{2^{R_m}(1+x)-1}{\left(a_m - a_n\left(2^{R_m}(1+x)-1\right)\right)\rho_b}} dx. \end{aligned} \tag{15}$$

where we have $\tau_m = \frac{1}{2^{R_m}(1-a_m)} - 1$.

In this treatise, we consider the SOP under the condition that the connection between the BS and LUs can be established. As such, the SIC has been assumed to be successfully performed at the n-th user. Based on (13), the SOP is given by

$$P_n\left(R_n\right) = \int_0^\infty f_{\gamma_{E_n}}\left(x\right) F_{\gamma_{B_n}}\left(2^{R_n}\left(1+x\right)-1\right) dx. \tag{16}$$

Upon using the results of **Lemma 1** and **Lemma 3**, and substituting (4) and (8) into (16), after some further mathematical manipulations, we can express the SOP of the n-th user with the aid of the following theorem:

Theorem 2. Assuming that the LUs position obeys the PPP for the ordered channels of the LUs, the SOP of the n-th user is given by

$$P_n\left(R_n\right) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \sum_{\tilde{S}_n^p} \binom{n+p}{q_0+\cdots+q_K} \left(\prod_{K=0}^{K} b_k^{q_k}\right) \times \int_0^\infty \mu_{n1} \left(\frac{\mu_{n2}^\delta e^{-\mu_{n2}x}}{x} + \frac{\delta\Gamma\left(\delta, \mu_{n2}x\right)}{x^{\delta+1}}\right) e^{-\frac{\mu_{n1}\Gamma(\delta,\mu_{n2}x)}{x^\delta} - \sum\limits_{k=0}^{K} q_k c_k \frac{2^{R_n}(1+x)-1}{\rho_b a_n}} dx. \tag{17}$$

In this paper, we consider the secrecy outage occurs in the m-th user and the n-th user are independent. In other words, the SOP of the m-th user has on effect on the SOP of the n-th user and vice versa. As a consequence, we define the SOP for the selected user pair as that of either the m-th user or the n-th user outage. Hence, based on (15) and (17), the SOP of the selected user pair is given by

$$P_{mn} = 1 - \left(1 - P_m\right)\left(1 - P_n\right). \tag{18}$$

C. Secrecy Diversity Order Analysis

In order to derive the secrecy diversity order to gain further insights into the system's operation in the high-SNR regime, the following new analytical framework is introduced. Again, as the worst-case scenario, we assume that Es have a powerful detection capability. The asymptotic behavior is analyzed, usually when the SNR of the channels between the BS and LUs is sufficiently high, i.e., when the BS's transmit SNR obeys $\rho_b \to \infty$, while and the SNR of the channels between BS and Es is set to arbitrary values. It is noted that for the E-transmit SNR of $\rho_e \to \infty$, the probability of successful eavesdropping will tend to unity. The secrecy diversity order can be defined as follows:

$$d_s = -\lim_{\rho_b \to \infty} \frac{\log P^\infty}{\log \rho_b}, \tag{19}$$

where P^∞ is the asymptotic SOP. We commence our diversity order analysis by characterizing the CDF of the LUs $F_{\gamma_{B_m}}^\infty$ and $F_{\gamma_{B_n}}^\infty$ in the high-SNR regime. When $y \to 0$, based on (A.3) and the approximation of $1 - e^{-y} \approx y$, we obtain the asymptotic unordered CDF of $\left|\tilde{h}_n\right|^2$ as follows:

$$F_{\left|\tilde{h}_n\right|^2}^\infty(y) \approx \frac{2y}{R_D^2} \int_0^{R_D} \left(1 + r^\alpha\right) r dr = y\ell, \tag{20}$$

where $\ell = 1 + \frac{2R_D^\alpha}{\alpha+2}$.

Substituting (20) into (A.2), the asymptotic unordered CDF of $\left|\tilde{h}_n\right|^2$ is given by

$$F_{|h_n|^2}^{\infty}(y) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} (y\ell)^{n+p} \approx \frac{\varphi_n}{n} (y\ell)^n. \tag{21}$$

Similarly, based on (A.1), we can obtain $F_{\gamma_{B_n}}^{\infty}(x) \approx \frac{\varphi_n}{n}\left(\frac{x\ell}{\rho_b a_n}\right)^n$. Based on Φ_m and (21), we can arrive at:

$$\Phi_m^{\infty} \approx \frac{\varphi_m}{m}\left(\frac{x\ell}{(a_m - a_n x)\,\rho_b}\right)^m. \tag{22}$$

Substituting (22) into (6), the asymptotic CDF of γ_{B_m} can be expressed as

$$F_{\gamma_{B_m}}^{\infty}(x) = U\left(x - \frac{a_m}{a_n}\right) + U\left(\frac{a_m}{a_n} - x\right)\Phi_m^{\infty}, \tag{23}$$

where Φ_m^{∞} is given in (22).

Based on (16), we can replace the CDF of $F_{\gamma_{B_n}}$ by the asymptotic $F_{\gamma_{B_n}}^{\infty}$. After some manipulations, we arrive at the asymptotic SOP of the n-th user formulated by the following theorem.

Theorem 3. Assuming that the LUs position obeys the PPP for the ordered channels of the LUs, the asymptotic SOP of the n-th user is given by

$$P_n^{\infty}(R_n) = G_n(\rho_b)^{-D_n} + o\left(\rho_b^{-D_n}\right), \tag{24}$$

where we have $Q_1 = \int_0^\infty \mu_{n1} e^{-\frac{\mu_{n1}\Gamma(\delta,\mu_{n2}x)}{x^\delta}} \left(\frac{\mu_{n2}^\delta e^{-\mu_{n2}x}}{x} + \frac{\delta\Gamma(\delta,\mu_{n2}x)}{x^{\delta+1}}\right)\left(\frac{\left(2^{R_n}(1+x)-1\right)\ell}{a_n}\right)^n dx$, $G_n = \frac{\varphi_n Q_1}{n}$, and $D_n = n$.

Similarly, based on (14), we can replace the CDF of $F_{\gamma_{B_m}}$ by the asymptotic $F_{\gamma_{B_m}}^{\infty}$ of (23). Additionally, we can formulate the asymptotic SOP of the m-th user by the following theorem.

Theorem 4. Assuming that the LUs position obeys the PPP for the ordered channels of the LUs, the asymptotic SOP for the m-th user is given by

$$P_m^{\infty}(R_n) = G_m(\rho_b)^{-D_m} + o\left(\rho_b^{-D_m}\right), \tag{25}$$

where we have $Q_2 = \int_0^{\tau_m} \mu_{m1} e^{-\frac{\mu_{m1}\Gamma(\delta,\mu_{m2}x)}{x^\delta}} \left(\frac{\mu_{m2}^\delta e^{-\mu_{m2}x}}{x} + \frac{\delta\Gamma(\delta,\mu_{m2}x)}{x^{\delta+1}}\right)\left(\frac{\left(2^{R_m}(1+x)-1\right)\ell}{\left(a_m - a_n\left(2^{R_m}(1+x)-1\right)\right)}\right)^m dx$, $G_m = \frac{\varphi_m Q_2}{m}$ and $D_m = m$.

Substituting (24) and (25) into (18), the asymptotic SOP for the user pair can be expressed as

$$P_{mn}^{\infty} = P_m^{\infty} + P_n^{\infty} - P_m^{\infty} P_n^{\infty} \approx P_m^{\infty} G_m (\rho_b)^{-D_m}. \tag{26}$$

Based on **Theorem 4** and **Theorem 3**, and upon substituting (24) and (25) into (19), we arrive at the following proposition.

Proposition 1. For $m < n$, the secrecy diversity order can be expressed as

$$d_s = -\lim_{\rho_b \to \infty} \frac{\log \left(P_m^{\infty} + P_n^{\infty} - P_m^{\infty} P_n^{\infty} \right)}{\log \rho_b} = m. \tag{27}$$

Remark 1. *The results of* (27) *indicate that the secrecy diversity order and the asymptotic SOP for the user pair considered are determined by the* m*-th user.*

Remark 1 provides insightful guidelines for improving the SOP of the networks considered by invoking user pairing among of the M users. Since the SOP of a user pair is determined by that of the one having a poor channel, it is efficient to pair the user having the best channel and the second best channel for the sake of achieving an increased secrecy diversity order.

III. ENHANCING SECURITY WITH THE AID OF ARTIFICIAL NOISE

In addition to single antenna scenario [24], for further improving the secrecy performance, let us now consider the employment of multiple antennas at BS for generating AN in order to degrade the Es' SNR. More particularly, the BS is equipped with N_A antennas, while all LUs and Es are equipped with a single antenna each. We mask the superposed information of NOMA by superimposing AN on Es with the aid of the BS. It is assumed that the CSI of LUs are known at BS. Since the AN is in the null space of the intended LU's channel, it will not impose any effects on LUs. However, it can significantly degrade the channel and hence the capacity of Es. More precisely, the key idea of using AN as proposed in [25] can be described as follows: an orthogonal basis of C^{N_A} is generated at BS for user κ, (where $\kappa \in \{m, n\}$) as a $(N_A \times N_A)$–element precoding matrix $\mathbf{U}_\kappa = [\mathbf{u}_\kappa, \mathbf{V}_\kappa]$, where we have $\mathbf{u}_\kappa = {\mathbf{h}_\kappa^\dagger}/{\|\mathbf{h}_\kappa\|}$, and $\mathbf{V}_\kappa$ is of size $N_A \times (N_A - 1)$. Here, $\mathbf{h}_\kappa$ is denoted as the intended channel between the BS and user κ. It is noted that each column of $\mathbf{V}_\kappa$ is orthogonal to $\mathbf{u}_\kappa$. Beamforming is applied at the BS for generating AN. As such, the transmitted superposed information, which is masked by AN

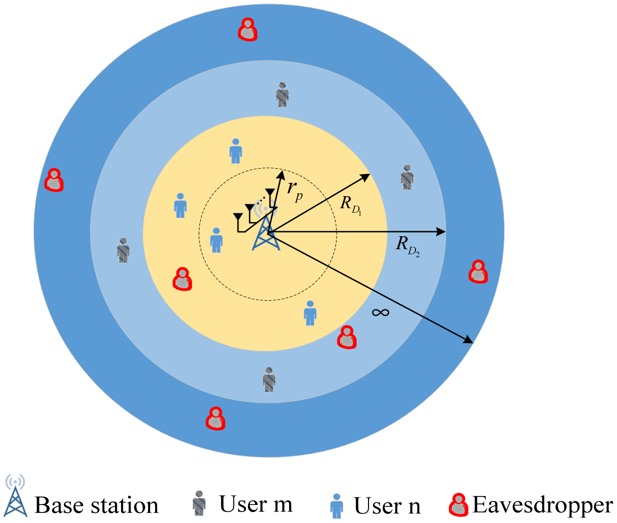


Fig. 2: Network model for secure NOMA transmission using AN in multiple-antenna scenario.

at the BS is given by

$$\sum_{\kappa\in\{m,n\}} \sqrt{a_\kappa}\mathbf{x}_\kappa = \sum_{\kappa\in\{m,n\}} \sqrt{a_\kappa}\left(s_\kappa\mathbf{u}_\kappa + \mathbf{t}_\kappa\mathbf{V}_\kappa\right), \tag{28}$$

where s_κ is the information-bearing signal with a variance of σ_s^2, and $\mathbf{t}_\kappa$ is the AN. Here the (N_A-1) elements of $\mathbf{t}_\kappa$ are independent identically distributed (i.i.d.) complex Gaussian random variables with a variance of σ_a^2. As such, the overall power per transmission is $P_T = P_S + P_A$, where $P_S = \theta P_T = \sigma_s^2$ is the transmission power of the desired information-bearing signal, while $P_A = (1-\theta)\,P_T = (N_A-1)\,\sigma_a^2$ is the transmission power of the AN. Here θ represents the power sharing coefficients between the information-bearing signal and AN. To reduce the complexity of channel ordering in this MISO system when applying the NOMA protocol, as shown in Fig. 2, we divide the disc D into two regions, namely, D_1 and D_2, respectively. Here, D_1 is an internal disc with radius R_{D_1}, and the group of user n is located in this region. D_2 is an external ring spanning the radius distance from R_{D_1} to R_{D_2}, and the group of user m is located in this region. In this scenario, channel ordering is unnecessary at the BS, since in this case the path loss is the dominant channel impairment. For simplicity, we assume that user n and user m are the selected user from each group in the rest of this paper. The cell-center user n is assumed to be capable of cancelling the interference of the cell-edge user m using SIC techniques. User n and user m are randomly selected in each region for pairing them for NOMA. The combined signal at user m is given by

$$\mathbf{y}_m = \underbrace{\frac{\sqrt{a_m} s_m \mathbf{h}_m}{\sqrt{1+d_m^{\alpha}}}}_{\textbf{Signal part}} + \underbrace{\frac{\sqrt{a_n} s_n \mathbf{h}_m \mathbf{u}_n}{\sqrt{1+d_m^{\alpha}}} + \frac{\sqrt{a_n} \mathbf{h}_m \mathbf{t}_n \mathbf{V}_n}{\sqrt{1+d_m^{\alpha}}} + \mathbf{n}_m}_{\textbf{Interference and noise part}}, \tag{29}$$

where $\mathbf{n}_m$ is a Gaussian noise vector at user m, while d_m is the distance between the BS and user m. Substituting (28) into (29), the received SINR at user m is given by

$$\gamma_{B_m}^{AN} = \frac{a_m \sigma_s^2 \|\mathbf{h}_m\|^2}{a_n \sigma_s^2 \left|\mathbf{h}_m \frac{\mathbf{h}_n^{\dagger}}{\|\mathbf{h}_n\|}\right|^2 + a_n \sigma_a^2 \|\mathbf{h}_m \mathbf{V}_n\|^2 + 1 + d_m^{\alpha}}, \tag{30}$$

where the variance of $\mathbf{n}_m$ is normalized to unity. As such, we can express the transmit SNR at BS as $\rho_t = P_T$.

Since SIC is applied at user n, the interference arriving from user m can be detected and subtracted firstly. The aggregate signal at user n is given by

$$\mathbf{y}_n = \underbrace{\frac{\mathbf{h}_n \sqrt{a_n} s_n}{\sqrt{1+d_n^{\alpha}}}}_{\textbf{Signal part}} + \underbrace{\frac{\mathbf{h}_n \sqrt{a_m} \mathbf{t}_m \mathbf{V}_m}{\sqrt{1+d_n^{\alpha}}} + \mathbf{n}_n}_{\textbf{Interference and noise part}}, \tag{31}$$

where $\mathbf{n}_n$ is the Gaussian noise at user n, while d_n is the distance between the BS and user n. The received SINR at user n is given by

$$\gamma_{B_n}^{AN} = \frac{a_n \sigma_s^2 \|\mathbf{h}_n\|^2}{a_m \sigma_a^2 \|\mathbf{h}_n \mathbf{V}_m\|^2 + 1 + d_n^{\alpha}}, \tag{32}$$

where the variance of $\mathbf{n}_n$ is normalized to unity. The signal observed by Es is given by

$$\mathbf{y}_e = \sum_{\kappa \in \{m,n\}} \sqrt{a_\kappa} \mathbf{x}_\kappa \frac{\mathbf{h}_e}{\sqrt{d_e^{\alpha}}} + \mathbf{n}_e, \tag{33}$$

where $\mathbf{n}_e$ is the Gaussian noises at Es, while $\mathbf{h}_e \in \mathrm{C}^{1 \times N_A}$ is the channel vector between the BS and Es. Similar to the single-antenna scenario, again, we assume that the Es have a strong detection capability and hence they unambiguously distinguish the messages of user m and user n. The received SINR of the most detrimental E associated with detecting user κ is given by

$$\gamma_{E_\kappa}^{AN} = a_\kappa \sigma_s^2 \max_{e \in \Phi_e, d_e \geq r_p} \left\{ \frac{X_{e,\kappa}}{I_e^{AN} + d_e^{\alpha}} \right\}, \tag{34}$$

where the variance of $\mathbf{n}_e$ is normalized to unity, and we have $X_{e,\kappa} = \left|\mathbf{h}_e \frac{\mathbf{h}_\kappa^\dagger}{\|\mathbf{h}_\kappa\|}\right|^2$ as well as $I_e^{AN} = a_m \sigma_a^2 \|\mathbf{h}_e \mathbf{V}_m\|^2 + a_n \sigma_a^2 \|\mathbf{h}_e \mathbf{V}_n\|^2$.

A. New Channel Statistics

In this subsection, we derive several new channel statistics for LUs and Es in the presence of AN, which will be used for deriving the SOP in the next subsection.

Lemma 4. Assuming that user m is randomly positioned in the ring D_2 of Fig. 2, for the case of $\theta \neq \frac{1}{N_A}$, the CDF of $F_{B_m}^{AN}$ is given by

$$F_{B_m}^{AN}(x) = 1 - e^{-\frac{\nu x}{a_n}} \sum_{p=0}^{N_A-1} \frac{(\nu x)^p}{p!} \sum_{q=0}^{p} \binom{p}{q} a_n^{q-p} \underbrace{a_1 \left(\frac{\Gamma(q+1)}{\left(\nu x + \frac{1}{P_S}\right)^{q+1}} - \sum_{l=0}^{N_A-2} \frac{\left(\frac{N_A-1}{P_A} - \frac{1}{P_S}\right)^l}{\frac{l!\left(\nu x + \frac{N_A-1}{P_A}\right)^{q+l+1}}{\Gamma(q+l+1)}} \right)}_{\mathrm{I}(\theta)} \times$$

$$\sum_{u=0}^{p-q} \binom{p-q}{u} \frac{\gamma\left(u+\delta, \frac{\nu x}{a_n} R_{D_2}^\alpha\right) - \gamma\left(u+\delta, \frac{\nu x}{a_n} R_{D_1}^\alpha\right)}{\left(\frac{\nu x}{a_n}\right)^{u+\delta}}, \tag{35}$$

where $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function, $\Gamma(\cdot)$ is the Gamma function, $a_1 = \delta \left(1 - \frac{P_A}{(N_A-1)P_S}\right)^{1-N_A} / \left(\left(R_{D_2}^2 - R_{D_1}^2\right) P_S\right)$, and $\nu = \frac{a_n}{a_m P_S}$.

For the case of $\theta = \frac{1}{N_A}$, the CDF of $F_{B_m}^{AN}$ is given by (35) upon substituting $\mathrm{I}(\theta)$ by $\mathrm{I}^*(\theta)$, where we have $\mathrm{I}^*(\theta) = \frac{a_2 \Gamma(q+N_A)}{\left(\nu x + \frac{1}{P_S}\right)^{q+N_A}} \sum\limits_{u=0}^{p-q} \binom{p-q}{u}$ and $a_2 = \frac{\delta}{\left(R_{D_2}^2 - R_{D_1}^2\right) {P_S}^{N_A} (N_A-1)!}$.

Proof: See Appendix B . ∎

Lemma 5. Assuming that user n is randomly positioned in the disc D_1 of Fig. 2, the CDF of $F_{B_n}^{AN}$ is given by

$$F_{B_n}^{AN}(x) = 1 - b_2 e^{-\frac{\vartheta x}{a_m}} \sum_{p=0}^{N_A-1} \frac{\vartheta^p x^p}{p!} \sum_{q=0}^{p} \binom{p}{q} \times$$

$$\frac{\Gamma(N_A - 1 + q)}{\left(\vartheta x + \frac{N_A-1}{P_A}\right)^{N_A-1+q} a_m^{p-q}} \sum_{u=0}^{p-q} \binom{p-q}{u} \frac{a_m^{u+\delta} \gamma\left(u+\delta, \frac{\vartheta x}{a_m} R_{D_1}^\alpha\right)}{(\vartheta x)^{u+\delta}}, \tag{36}$$

where we have $b_2 = \frac{\delta}{R_{D_1}^2 \Gamma(N_A-1) \left(\frac{P_A}{N_A-1}\right)^{N_A-1}}$ and $\vartheta = \frac{a_m}{a_n P_S}$.

Proof: See Appendix C. ∎

Lemma 6. Assuming that the distribution of Es obeys a PPP and that the E-exclusion zone has a radius of r_p, the PDF of $f_{\gamma_{E_\kappa}^{AN}}$ (where $\kappa \in \{m, n\}$) is given by

$$f_{\gamma_{E_\kappa}^{AN}}(x) = -e^{\Theta_\kappa \Psi_{\kappa 1}} \left(\frac{\left(\mu_{\kappa 2}^{AN}\right)^{\delta} e^{-x\mu_{\kappa 2}^{AN}}}{x} \Psi_{\kappa 1} + \frac{\delta \Theta_\kappa \Psi_{\kappa 1}}{x} + \Theta_\kappa \Psi_{\kappa 2} \right), \tag{37}$$

where $\Theta_\kappa = \frac{\Gamma\left(\delta, x\mu_{\kappa 2}^{AN}\right)}{x^\delta}$, $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function, $\Psi_{\kappa 1} = \Omega \frac{1}{\left(\frac{x}{a_\kappa P_S} + \tau_i\right)^j}$, $\Psi_{\kappa 2} = \Omega \frac{1}{\left(\frac{x}{a_\kappa P_S} + \tau_i\right)^j} \left(\frac{j}{\left(\frac{x}{a_\kappa P_S} + \tau_i\right)} \frac{1}{a_\kappa P_S} \right)$, $\Omega = (-1)^{N_A} \mu_{\kappa 1}^{AN} \prod\limits_{i=1}^{2} \tau_i^{N_A - 1} \sum\limits_{i=1}^{2} \sum\limits_{j=1}^{N_A - 1} a_{N_A - j, N_A - 1} (2\tau_i - L)^{j - (2N_A - 2)}$, $L = \tau_1 + \tau_2$, $\tau_1 = \frac{N_A - 1}{a_m P_A}$, $\tau_2 = \frac{N_A - 1}{a_n P_A}$, $a_{N_A - j, N_A - 1} = \binom{2N_A - j - 3}{N_A - j - 1}$, $\mu_{\kappa 1}^{AN} = \pi \lambda_e \delta (a_\kappa P_S)^\delta$, and $\mu_{\kappa 2}^{AN} = \frac{r_p^\alpha}{a_\kappa P_S}$.

Proof: See Appendix D. ■

B. Secrecy Outage Probability

In this subsection, we investigate the SOP of a multiple-antenna aided scenario relying on AN. Using the results of **Lemma 4** and **Lemma 6**, based on (14), we expressed the SOP of user m using the following theorem:

Theorem 5. Assuming that the LUs and Es distribution obey PPPs and that AN is generated at the BS, for the case $\theta \neq \frac{1}{N_A}$, the SOP of user m is given by

$$\begin{aligned} P_m^{AN}(R_m) = &\int_0^\infty -e^{\Theta_m \Psi_{m1}} \left(\frac{\left(\mu_{m2}^{AN}\right)^\delta e^{-x\mu_{m2}^{AN}}}{x} \Psi_{m1} + \frac{\delta \Theta_m \Psi_{m1}}{x} + \Theta_m \Psi_{m2} \right) \\ &\times \underbrace{\left(1 - a_1^* \sum_{p=0}^{N_A - 1} \frac{\iota_m^p}{p!} \sum_{q=0}^{p} \binom{p}{q} a_n^q \left(\frac{\Gamma(q+1)}{\left(a_n \iota_{m*} + \frac{1}{P_S}\right)^{q+1}} - \sum_{l=0}^{N_A - 2} \frac{\frac{1}{l!}\left(\frac{N_A - 1}{P_A} - \frac{1}{P_S}\right)^l \Gamma(q + l + 1)}{\left(a_n \iota_{m*} + \frac{N_A - 1}{P_A}\right)^{q+l+1}} \right) \mathrm{T}_1^* \right)}_{\mathrm{K}(\theta)} dx, \end{aligned} \tag{38}$$

where we have $a_1^* = \frac{\delta e^{-\iota_{m*}} \left(1 - \frac{P_A}{(N_A - 1) P_S}\right)^{1 - N_A}}{\left(R_{D_2}^2 - R_{D_1}^2\right) P_S}$, $\mathrm{T}_1^* = \sum\limits_{u=0}^{p-q} \binom{p-q}{u} \frac{\gamma\left(u + \delta, \iota_{m*} R_{D_2}^\alpha\right) - \gamma\left(u + \delta, \iota_{m*} R_{D_1}^\alpha\right)}{\iota_{m*}^{u+\delta}}$, and $\iota_{m*} = \frac{\nu\left(2^{R_m}(1+x) - 1\right)}{a_n}$.

For the case of $\theta = \frac{1}{N_A}$, the SOP for user m is given by (38) upon substituting $\mathrm{K}(\theta)$ with $\mathrm{K}^*(\theta)$, where $\mathrm{K}^*(\theta) = 1 - a_2^* \sum\limits_{p=0}^{N_A - 1} \frac{\iota_{m*}^p}{p!} \sum\limits_{q=0}^{p} \binom{p}{q} \frac{\Gamma(q + N_A) a_n^q}{\left(a_n \iota_{m*} + \frac{1}{P_S}\right)^{q + N_A}} \sum\limits_{u=0}^{p-q} \binom{p-q}{u} \mathrm{T}_1^*$, and $a_2^* = \frac{\delta e^{-\iota_{m*}}}{\left(R_{D_2}^2 - R_{D_1}^2\right) {P_S}^{N_A} (N_A - 1)!}$.

Similarly, using the results of **Lemma 5** and **Lemma 6**, as well as (16), we expressed the SOP of user n by the following theorem:

Theorem 6. Assuming that the LUs and Es distribution obey PPPs and that AN is generated at the BS, the SOP of user n is given by

$$\begin{aligned} P_n^{AN}\left(R_n\right) = & \int_0^\infty -e^{\Theta_n \Psi_{n1}} \left(\frac{\left(\mu_{n2}^{AN}\right)^\delta e^{-x\mu_{n2}^{AN}}}{x} \Psi_{n1} + \frac{\delta \Theta_n \Psi_{n1}}{x} + \Theta_n \Psi_{n2} \right) \\ & \times \left(1 - b_2 e^{-\iota_n} \sum_{p=0}^{N_A-1} \frac{\iota_{n*}}{p!} \sum_{q=0}^{p} \binom{p}{q} \frac{\Gamma\left(N_A - 1 + q\right) a_m^q}{\left(a_m \iota_{n*} + \frac{N_A-1}{P_A}\right)^{N_A-1+q}} \sum_{u=0}^{p-q} \binom{p-q}{u} \frac{\gamma\left(u+\delta, \iota_{n*} R_{D_1}^\alpha\right)}{\iota_{n*}^{u+\delta}} \right) dx, \end{aligned} \tag{39}$$

where $\iota_{n*} = \frac{\vartheta\left(2^{R_n}(1+x)-1\right)}{a_m}$.

Based on (38) and (39), the SOP for the selected user pair can be expressed as

$$P_{mn}^{AN} = 1 - \left(1 - P_m^{AN}\right)\left(1 - P_n^{AN}\right). \tag{40}$$

C. Large Antenna Array Analysis

In this subsection, we investigate the system's asymptotic behavior when the BS is equipped with large antenna arrays. It is noted that for the exact SOP derived in (38) and (39), as N_A increases, the number of summations in the equations will increase exponentially, which imposes an excessive complexity. Motivated by this, we seek good approximations for the SOP associated with a large N_A. With the aid of the theorem of large values, we have the following approximations: $\lim\limits_{N_A\to\infty} \left\|\mathbf{h}_n\right\|^2 \to N_A$, $\lim\limits_{N_A\to\infty} \left\|\mathbf{h}_m\right\|^2 \to N_A$, $\lim\limits_{N_A\to\infty} \left\|\mathbf{h}_n\mathbf{V}_m\right\|^2 \to N_A - 1$, and $\lim\limits_{N_A\to\infty} \left\|\mathbf{h}_m\mathbf{V}_n\right\|^2 \to N_A - 1$.

We first derive the asymptotic CDF of user n for $N_A \to \infty$. Based on (32), we can express the asymptotic CDF of $F_{B_n,\infty}^{AN}$ as $F_{B_n,\infty}^{AN}(x) = \Pr\left\{\frac{a_n P_S N_A}{a_m P_A + 1 + d_n^\alpha} \le x\right\}$.

After some further mathematical manipulations, we can obtain the CDF of $F_{B_n,\infty}^{AN}$ for large antenna arrays in the following lemma.

Lemma 7. Assuming that user n is randomly located in the disc D_1 of Fig. 2 and $N_A \to \infty$, the CDF of $F_{B_n,\infty}^{AN}$ is given by

$$F_{B_n,\infty}^{AN}(x) = \begin{cases} 0, x < \zeta_n \\ 1 - \frac{\left(\frac{a_n P_S N_A}{x} - a_m P_A - 1\right)^{\delta}}{R_{D_1}^2}, \zeta_n \le x \le \xi_n \\ 1, x \ge \xi_n \end{cases}, \tag{41}$$

where we have $\zeta_n = \frac{a_n P_S N_A}{R_{D_1}^{\alpha} + a_m P_A + 1}$ and $\xi_n = \frac{a_n P_S N_A}{a_m P_A + 1}$.

Similarly, based on (30),the CDF of the asymptotic $F_{B_m,\infty}^{AN}$ is given by

$$F_{B_m,\infty}^{AN}(x) = \Pr\left\{ \frac{a_m P_S N_A}{a_n P_S \left| \mathbf{h}_m \frac{\mathbf{h}_n^{\dagger}}{\|\mathbf{h}_n\|} \right|^2 + a_n P_A + 1 + d_m^{\alpha}} \le x \right\}. \tag{42}$$

After some further mathematical manipulations, we obtain the CDF of $F_{B_m,\infty}^{AN}$ for large antenna arrays using the following lemma.

Lemma 8. Assuming that user m is randomly located in the ring D_2 of Fig. 2 and $N_A \to \infty$, the CDF of $F_{B_m,\infty}^{AN}$ is given by

$$F_{B_m,\infty}^{AN}(x) = \begin{cases} 1, x \ge \zeta_{m1} \\ \frac{R_{D_2}^2 - t_m^2 + b_1 e^{-\frac{a_m P_S N_A}{x a_n P_S}}}{R_{D_2}^2 - R_{D_1}^2} \int_{R_{D_1}}^{t_m} r e^{\frac{r^{\alpha}}{a_n P_S}} dr, \zeta_{m2} < x \le \zeta_{m1} \\ \frac{b_1 e^{-\frac{a_m P_S N_A}{x a_n P_S}}}{R_{D_2}^2 - R_{D_1}^2} \int_{R_{D_1}}^{R_{D_2}} r e^{\frac{r^{\alpha}}{a_n P_S}} dr, x < \zeta_{m2} \end{cases}, \tag{43}$$

where $b_1 = 2e^{\frac{a_n P_A + 1}{a_n P_S}}$, $t_m = \sqrt[\alpha]{\frac{a_m P_S N_A}{x} - a_n P_A - 1}$, $\zeta_{m1} = \frac{a_m P_S N_A}{R_{D_1}^{\alpha} + a_n P_A + 1}$, $\zeta_{m2} = \frac{a_m P_S N_A}{R_{D_2}^{\alpha} + a_n P_A + 1}$, and $\xi_m = \frac{a_m P_S N_A}{a_n P_A + 1}$.

Let us now turn our attention to the derivation of the Es' PDF in a large-scale antenna scenario. Using the theorem of large values, we have $\lim\limits_{N_A \to \infty} I_{e,\infty}^{AN} = a_m \sigma_a^2 \|\mathbf{h}_e \mathbf{V}_m\|^2 + a_n \sigma_a^2 \|\mathbf{h}_e \mathbf{V}_n\|^2 \to P_A$. The asymptotic CDF of $F_{\gamma_{E_\kappa,\infty}^{AN}}$ associated with $N_A \to \infty$ is given by

$$F_{\gamma_{E_\kappa,\infty}^{AN}}(x) = \Pr\left\{ \max_{e \in \Phi_e, d_e \ge r_p} \left\{ \frac{a_\kappa P_S X_{e,\kappa}}{I_{e,\infty}^{AN} + d_e^{\alpha}} \right\} \le x \right\} = E_{\Phi_e}\left\{ \prod_{e \in \Phi_e, d_e \ge r_p} F_{X_{e,\kappa}}\left(\frac{(P_A + d_e^{\alpha})\, x}{a_\kappa P_S} \right) \right\}. \tag{44}$$

Following the procedure used for deriving (10), we apply the generating function and switch to polar coordinates. Then with the help of [21, Eq. (3.381.9)], (44) can be expressed as

$$F_{\gamma_{E_\kappa,\infty}^{AN}}(x) = \exp\left[-\frac{\mu_{\kappa 1}^{AN}\Gamma\left(\delta, \mu_{\kappa 2}^{AN}x\right)}{x^\delta} e^{-\frac{P_A x}{a_\kappa P_S}}\right]. \tag{45}$$

Taking derivative of (45), we obtain the PDF of $f_{\gamma_{E_\kappa,\infty}^{AN}}$ in the following lemma.

Lemma 9. Assuming that the Es distribution obeys a PPP and that AN is generated at the BS, the E-exclusion zone has a radius of r_p, and $N_A \to \infty$, the PDF of $f_{\gamma_{E_\kappa,\infty}^{AN}}$ is given by

$$f_{\gamma_{E_\kappa,\infty}^{AN}}(x) = e^{-\frac{\mu_{\kappa 1}^{AN}\Gamma\left(\delta,\mu_{\kappa 2}^{AN}x\right)e^{-\frac{P_A x}{a_\kappa P_S}}}{x^\delta} - \frac{P_A x}{a_\kappa P_S}} \mu_{\kappa 1}^{AN} x^{-\delta}\left(\left(\mu_{\kappa 2}^{AN}\right)^\delta x^{\delta-1} e^{-\mu_{\kappa 2}^{AN}x} + \Gamma\left(\delta, \mu_{\kappa 2}^{AN}x\right)\left(\frac{P_A}{a_\kappa P_S} + \frac{\delta}{x}\right)\right). \tag{46}$$

Remark 2. *The results derived in* (46) *show that the PDF of* $f_{\gamma_{E_\kappa,\infty}^{AN}}$ *is independent of the number of antennas* N_A *in our large antenna array analysis. This indicates that* N_A *has no effect on the channel of the Es, when the number of antennas is sufficiently high.*

Let us now derive the SOP for our large antenna array scenario. Using the results of **Lemma 8** and **Lemma 9**, based on (14), we can express the SOP for user m in the following theorem.

Theorem 7. Assuming that the LUs and Es distribution obey PPPs, AN is generated at the BS, and $N_A \to \infty$, the SOP for user m is given by

$$\begin{aligned}
P_{m,\infty}^{AN}(R_m) &= 1 - e^{-\frac{\mu_{\kappa 1}^{AN}\Gamma\left(\delta,\mu_{\kappa 2}^{AN}\chi_{m1}\right)}{(\chi_{m1})^\delta} e^{-\frac{P_A \chi_{m1}}{a_\kappa P_S}}} \\
&+ \frac{\mu_{m1}^{AN} b_1 \Lambda_1}{R_{D_2}^2 - R_{D_1}^2}\int_0^{\chi_{m2}} e^{-\frac{\mu_{m1}^{AN}\Gamma\left(\delta,\mu_{m2}^{AN}x\right)e^{-\frac{P_A x}{a_m P_S}}}{x^\delta} - \frac{a_m P_S N_A}{\left(2^{R_m}(1+x)-1\right)a_n P_S} - \frac{P_A x}{a_m P_S}} \Xi_1 dx \\
&+ \frac{\mu_{m1}^{AN}}{R_{D_2}^2 - R_{D_1}^2}\int_{\chi_{m2}}^{\chi_{m1}} e^{-\frac{\mu_{m1}^{AN}\Gamma\left(\delta,\mu_{m2}^{AN}x\right)e^{-\frac{P_A x}{a_m P_S}}}{x^\delta} - \frac{P_A x}{a_m P_S}}\left(R_{D_2}^2 - t_{m*}^2 + b_1 e^{-\frac{a_m P_S N_A}{\left(2^{R_m}(1+x)-1\right)a_n P_S}}\right)\Xi_1 \Lambda_2 dx,
\end{aligned} \tag{47}$$

where we have $\Xi_1 = x^{-\delta}\left(\mu_{m2}^{AN}\left(\mu_{m2}^{AN}x\right)^{\delta-1} e^{-\mu_{m2}^{AN}x} + \Gamma\left(\delta, \mu_{m2}^{AN}x\right)\left(\frac{P_A}{a_m P_S} + \frac{\delta}{x}\right)\right)$, $\Lambda_1 = \int_{R_{D_1}}^{R_{D_2}} r e^{\frac{r^\alpha}{a_n P_S}} dr$, $\Lambda_2 = \int_{R_{D_1}}^{t_{m*}} r e^{\frac{r^\alpha}{a_n P_S}} dr$, $t_{m*} = \sqrt[\alpha]{\frac{a_m P_S N_A}{2^{R_m}(1+x)-1} - a_n P_A - 1}$, and $\chi_{m2} = \frac{\zeta_{m2}+1}{2^{R_m}} - 1$.

Similarly, using the results of **Lemma 7** and **Lemma 9**, as well as (16), we can express the

SOP for user n in the following theorem.

Theorem 8. Assuming that the LUs and Es distribution obey PPPs, AN is generated at the BS and $N_A \to \infty$, the SOP for user n is given by

$$P_{n,\infty}^{AN}\left(R_n\right) = 1 - e^{-\frac{\mu_{n1}^{AN}\Gamma\left(\delta,\mu_{n2}^{AN}\chi_{n2}\right)}{\left(\chi_{n2}\right)^{\delta}} e^{-\frac{P_A\chi_{n2}}{a_nP_S}}} + \mu_{n1}^{AN}\int_{\chi_{n1}}^{\chi_{n2}} e^{-\frac{\mu_{n1}^{AN}\Gamma\left(\delta,\mu_{n2}^{AN}x\right)e^{-\frac{P_Ax}{a_nP_S}}}{x^{\delta}}-\frac{P_Ax}{a_nP_S}}\Xi_2$$
$$\times\left(1-\frac{1}{R_{D_1}^2}\left(\frac{a_nP_SN_A}{2^{R_n}\left(1+x\right)-1}-a_mP_A-1\right)^{\delta}\right)dx, \tag{48}$$

where $\chi_{n1} = \frac{\zeta_n+1}{2^{R_n}}-1$, $\chi_{n2} = \frac{\xi_n+1}{2^{R_n}}-1$, and $\Xi_2 = x^{-\delta}\left(\left(\mu_{n2}^{AN}\right)^{\delta}x^{\delta-1}e^{-\mu_{n2}^{AN}x} + \Gamma\left(\delta,\mu_{n2}^{AN}x\right)\left(\frac{P_A}{a_nP_S}+\frac{\delta}{x}\right)\right)$.

Based on (47) and (48), the SOP for the selected user pair can be expressed as

$$P_{mn,\infty}^{AN} = 1 - \left(1-P_{m,\infty}^{AN}\right)\left(1-P_{n,\infty}^{AN}\right). \tag{49}$$

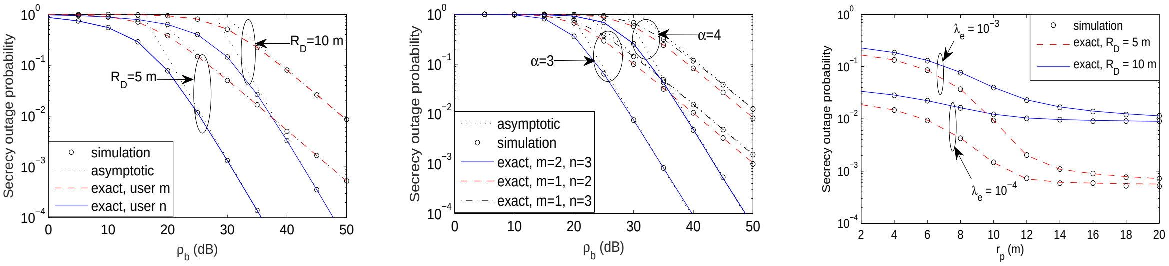
IV. NUMERICAL RESULTS

In this section, our numerical results are presented for characterizing the performance of large-scale networks. It is assumed that the power allocation coefficients of NOMA are $a_m = 0.6$, $a_n = 0.4$. The targeted data rates of the selected NOMA user pair are assumed to be $R_m = R_n = 0.1$ bit per channel use (BPCU). The complexity-vs-accuracy tradeoff parameter is $K = 20$.

A. Secrecy outage probability with channel ordering

In Fig. 3, we investigate the secrecy performance in conjunction with channel ordering, which correspond to the scenario considered in Section II.

Fig. 3(a) plots the SOP of a single user (m-th and n-th) versus ρ_b for different user zone radii. The curves represent the exact analytical SOP of both the m-th user and of n-th user derived in (15) and (17), respectively. The asymptotic analytical SOP of both the m-th and n-th users, are derived in (25) and (24), respectively. Monte Carlo simulations are used for verifying our derivations. Fig. 3(a) confirms the close agreement between the simulation and analytical results. A specific observation is that the reduced SOP can be achieved by reducing the radius of the user zone, since a smaller user zone leads to a lower path-loss. Another observation is that the n-th user has a more steep slope than the m-th user. This is due to the fact that we have $m < n$ and the m-th user as well as n-th user achieve a secrecy diversity order of m and n respectively, as inferred from (25) and (24).



(a) The SOP versus ρ_b, with $\rho_e = 10$ dB, $\alpha = 4$, $\lambda_e = 10^{-3}$, $M = 2$, $m = 1$, $n = 2$, and $r_p = 10$ m.

(b) The SOP of user pair versus ρ_b, with $\rho_e = 10$ dB, $\lambda_e = 10^{-3}$, $R_D = 10$ m, $M = 3$, and $r_p = 10$ m.

(c) The SOP of user pair versus r_p, with $\rho_b = 50$ dB, $\rho_e = 40$ dB, $M = 2$, $m = 1$, $n = 2$, and $\alpha = 4$.

Fig. 3: The SOP with channel ordering, which correspond to the scenario considered in Section II

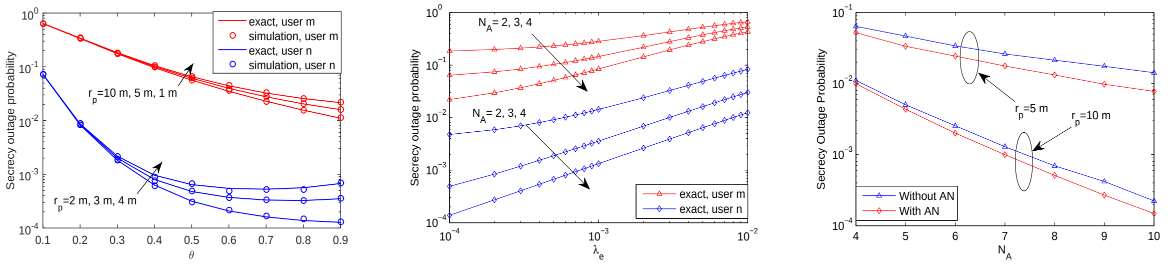
Fig. 3(b) plots the SOP of the selected user pair versus the transmit SNR ρ_b for different path-loss factors. The exact analytical SOP curves are plotted from (18). The asymptotic analytical SOP curves are plotted from (26). It can be observed that the two kinds of dashed curves have the same slopes. By contrast, the solid curves indicate a higher secrecy outage slope, which is due to the fact that the secrecy diversity order of the user pair is determined by that of the poor one. This phenomenon is also confirmed by the insights in **Remark 1**.

Fig. 3(c) plots the SOP of the selected user pair versus r_p for different densities of the Es. We can observe that as expected, the SOP decreases, as the radius of the E-exclusion zone increases. Another option for enhancing the PLS is to reduce the radius of the user zone, since it reduces the total path loss. It is also worth noting that having a lower E density λ_e results in an improved PLS, i.e. reduced SOP. This behavior is due to the plausible fact that a lower λ_e results in having less Es, which degrades the multiuser diversity gain, when the most detrimental E is selected. As a result, the destructive capability of the most detrimental E is reduced and hence the SOP is improved.

B. Secrecy outage probability with artificial noise

In Fig. 4 and Fig. 5, we investigate the secrecy performance in the presence of AN, which correspond to the scenario considered in Section III.

Fig. 4(a) plots the SOP of user m and user n versus θ for different E-exclusion zones. The solid and dashed curves represent the analytical performance of user m and user n, corresponding to the results derived in (38) and (39). Monte Carlo simulations are used for verifying our



(a) The SOP versus θ, with $\alpha = 4$, $R_{D_1} = 5$ m, $R_{D_2} = 10$ m, $\lambda_e = 10^{-4}$, $N_A = 4$, $\rho_t = 30$ dB.

(b) The SOP versus λ_e, with $\theta = 0.8$, $\alpha = 4$, $R_{D_1} = 5$ m, $R_{D_2} = 10$ m, $\rho_t = 30$ dB, $r_p = 4$ m.

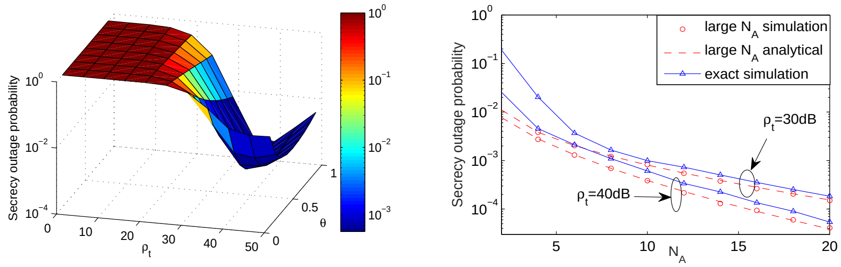
(c) The SOP of the user pair versus N_A, with $R_{D_1} = 5$ m, $R_{D_2} = 10$ m, $\alpha = 3$, $\lambda_e = 10^{-3}$, $\rho_t = 30$ dB.

Fig. 4: The SOP with artificial noise, which correspond to the scenario considered in Section III

derivations. Fig. 4(a) confirms a close agreement between the simulation and analytical results. Again, a reduced SOP can be achieved by increasing the E-exclusion zone, which degrades the channel conditions of the Es. Another observation is that user n achieves a lower SOP than user m, which is explained as follows: 1) user n has better channel conditions than user m, owing to its lower path loss; and 2) user n is capable of cancelling the interference imposed by user m using SIC techniques, while user m suffers from the interference inflicted by user n. It is also worth noting that the SOP is not a monotonic function of θ. This phenomenon indicates that there exists an optimal value for power allocation, which depends on the system parameters.

Fig. 4(b) plots the SOP of user m and user n versus λ_e for different number of antennas. We can observe that the SOP decreases, as the E density is reduced. This behavior is caused by the fact that a lower λ_e leads to having less Es, which reduces the multiuser diversity gain, when the most detrimental E is considered. As a result, the distinctive capability of the most detrimental E is reduced and hence the secrecy performance is improved. It is also worth noting that increasing the number of antennas is capable of increasing the secrecy performance. This is due to the fact that $\|\mathbf{h}_m\|^2$ in (30) and $\|\mathbf{h}_n\|^2$ in (32) both follow $Gamma\left(N_A, 1\right)$ distributions, which is the benefit of the improved multi-antenna diversity gain.

Fig. 4(c) plots the SOP of the selected user pair versus N_A for different path loss exponents. In this figure, the curves representing the case without AN are generated by setting $\theta = 1$, which means that all the power is allocated to the desired signal. In this case, the BS only uses beamforming for transmitting the desired signals and no AN is generated. The curves in the presence of AN are generated by setting $\theta = 0.9$. We show that the PLS can be enhanced by



(a) The SOP versus θ, with $\alpha = 4$, $R_{D_1} = 5$ m, $R_{D_2} = 10$ m, $\lambda_e = 10^{-4}$, $N_A = 4$, $\rho_t = 30$ dB.

(b) Large analysis for the SOP of user pair versus N_A, with $\theta = 0.8$, $R_{D_1} = 5$ m, $R_{D_2} = 10$ m, $\lambda_e = 10^{-4}$, $r_p = 5$ m.

Fig. 5: The SOP with artificial noise, which correspond to the scenario considered in Section III

using AN. This behavior is caused by the fact that at the receiver side, user m and user n are only affected by the AN generated by each other; By contrast, the Es are affected by the AN of both user m and user n. We can observe that the SOP of the selected user pair decreases, as the E-exclusion radius increases.

Fig. 5(a) plots the SOP of the selected user pair versus ρ_t and θ. It is observed that the SOP first decreases then increases as ρ_t increases, which is in contrast to the traditional trend, where the SOP always decreases as the transmit SNR increases. This behavior can be explained as follows. The SOP of the selected user pair is determined by user m. As ρ_t increases, on the one hand, the signal power of user m is increased, which improves the secrecy performance; On the other hand, user m also suffers from the interference imposed by user n (including both the signal and AN), because when ρ_t increases, the signal power of user n is also increased, which in turn degrades the secrecy performance. As a consequence, there is a tradeoff between ρ_t and the SOP. It is also noted that the power sharing factor θ also affect the optimal SOP associated with different values of ρ_t. This phenomenon indicates that it is of salient significance to select beneficial system parameters. Furthermore, optimizing the parameters ρ_t and θ is capable of further improving the SOP.

Fig. 5(b) plots the SOP of large antenna arrays of the selected user pair versus N_A parameterized by different transmit SNRs. The dashed curves represent the analytical SOP of the selected user pair, corresponding to the results derived in (49). We observe a close agreement between the theoretical analysis and the Monte Carlo simulations, which verifies the accuracy of our derivations. We observe that as N_A increases, the approximation used in our analysis approaches the exact SOP. This phenomenon indicates that the asymptotic SOP derived converges to the exact values, when N_A is a sufficiently large number.

V. CONCLUSIONS

In this paper, the secrecy performance of applying the NOMA protocol in large-scale networks was examined. Specifically, stochastic geometry based techniques were used for modeling both the locations of NOMA users and of the Es in the networks considered. Additionally, new analytical SOP expressions were derived for characterizing the system's secrecy performance in both single-antenna and multiple-antenna scenarios. For the single-antenna scenario, the secrecy diversity order of the user pair was also characterized. It was analytically demonstrated that the secrecy diversity order was determined by that one of the user pair who had a poorer channel. For the multiple-antenna scenario, it was shown that the Es' channel quality is independent of the number of antennas at the BS for large antenna array scenarios. Numerical results were also presented for validating the analysis. It was concluded that the secrecy performance can be improved both by extending the E-exclusion zone and by generating AN at the BS.

APPENDIX A: PROOF OF LEMMA 1

To derive the CDF of F_{γ_B}, based on (2), we can formulate

$$F_{\gamma_B}(x) = \Pr\left\{\rho_b a_n |h_n|^2 \le x\right\} = F_{|h_n|^2}\left(\frac{x}{\rho_b a_n}\right), \tag{A.1}$$

where $F_{|h_n|^2}$ is the CDF of the ordered channel gain for the n-th user. Assuming $y = \frac{x}{\rho_b a_n}$, and using order statistics [26] as well as applying binary series expansion, the CDF of the ordered channels has a relationship with the unordered channels captured as follows:

$$F_{|h_n|^2}(y) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \left(F_{|\tilde{h}_n|^2}(y)\right)^{n+p}, \tag{A.2}$$

where $F_{|\tilde{h}_n|^2}$ is the CDF of unordered channel gain for the n-th user.

Based on the assumption of homogeneous PPP, and by relying on polar coordinates, $F_{|\tilde{h}_n|^2}$ is expressed as

$$F_{|\tilde{h}_n|^2}(y) = \frac{2}{R_D^2} \int_0^{R_D} \left(1 - e^{-(1+r^{\alpha})y}\right) r dr. \tag{A.3}$$

However, it is challenging to arrive at an easily implemented insightful expression for $F_{\left|\tilde{h}_n\right|^2}\left(y\right)$. Therefore, the Gaussian-Chebyshev quadrature relationship [27] is invoked for finding an approximation of (A.3) in the following form:

$$F_{\left|\tilde{h}_n\right|^2}\left(y\right) \approx \sum_{k=0}^{K} b_k e^{-c_k y}. \tag{A.4}$$

Substituting (A.4) into (A.2) and applying the multinomial theorem, the CDF $F_{|h_n|^2}$ of ordered channel gain is given by

$$F_{|h_n|^2}\left(y\right) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \sum_{\tilde{S}_n^p} \binom{n+p}{q_0+\cdots+q_K} \left(\prod_{k=0}^{K} b_k^{q_k}\right) e^{-\sum\limits_{k=0}^{K} q_k c_k y}. \tag{A.5}$$

Substituting $y = \frac{x}{\rho_b a_n}$ into (A.5), we can obtain (4). The proof is completed.

APPENDIX B: PROOF OF LEMMA 4

Based on (30), we express the CDF of $F_{B_m}^{AN}$ as

$$F_{B_m}^{AN}\left(x\right) = \Pr\left\{\gamma_{B_m}^{AN} \le x\right\} = \Pr\left\{\frac{a_m \sigma_s^2 \|\mathbf{h}_m\|^2}{a_n \sigma_s^2 \left|\mathbf{h}_m \frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\right|^2 + a_n \sigma_a^2 \|\mathbf{h}_m \mathbf{V}_n\|^2 + 1 + d_m^\alpha} \le x\right\}. \tag{B.1}$$

It may be readily seen that $\|\mathbf{h}_m\|^2$ obeys a Gamma distribution having the parameters of $(N_A, 1)$. Hence the CDF of $\|\mathbf{h}_m\|^2$ is given by

$$F_{B_m}^{AN}\left(x\right) = 1 - e^{-x} \sum_{p=0}^{N_A-1} \frac{x^p}{p!}. \tag{B.2}$$

Denoting $X_m = \left|\mathbf{h}_m \frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\right|^2, Y_m = \|\mathbf{h}_m \mathbf{V}_n\|^2$, based on (B.2), we can re-write (B.1) as

$$\begin{aligned} F_{B_m}^{AN}\left(x\right) &= \Pr\left\{\|\mathbf{h}_m\|^2 \le x\nu\left(I_m^{AN} + \frac{1+d_m^\alpha}{a_n}\right)\right\} \\ &= 1 - \int\limits_{D_2} \int_0^\infty \sum_{p=0}^{N_A-1} \frac{\left(\nu x\left(z_m + \frac{1+d_m^\alpha}{a_n}\right)\right)^p}{p!} \left(e^{-\nu x z_m - \nu x \frac{1+d_m^\alpha}{a_n}}\right) f_{I_m^{AN}}\left(z_m\right) f_{D_2}\left(\omega_m\right) dz_m d\omega_m, \end{aligned} \tag{B.3}$$

where $\nu = \frac{a_n}{a_m P_S}$, $f_{I_m^{AN}}$ and f_{D_2} are the PDF of I_m^{AN} and D_2, respectively. Here we have $I_m^{AN} = \sigma_s^2 X_m + \sigma_a^2 Y_m$ and $f_{D_2}\left(\omega_m\right) = \frac{1}{\pi\left(R_{D_2}^2 - R_{D_1}^2\right)}$. Applying a binary series expansion to (B.3), we arrive at:

$$F_{B_m}^{AN}\left(x\right) = 1 - \sum_{p=0}^{N_A-1} \frac{\nu^p x^p}{p!} \sum_{q=0}^{p} \binom{p}{q} Q_1 \int\limits_{D_2} e^{-\nu x \frac{1+d_m^\alpha}{a_n}} \left(\frac{1+d_m^\alpha}{a_n}\right)^{p-q} f_{D_2}\left(\omega_m\right) d\omega_m, \tag{B.4}$$

where $Q_1 = \int_0^\infty e^{-\nu x z_m} z_m^q f_{I_m^{AN}}\left(z_m\right) dz_m$. Note that the distance d_m is determined by the location of ω_m. Then we change to polar coordinates and applying a binary series expansion again, we obtain

$$F_{B_m}^{AN}\left(x\right) = 1 - \frac{2e^{-\frac{\nu x}{a_n}}}{R_{D_2}^2 - R_{D_1}^2} \sum_{p=0}^{N_A-1} \frac{\nu^p x^p}{p!} \sum_{q=0}^{p} \binom{p}{q} Q_1 \frac{1}{a_n^{p-q}} \sum_{u=0}^{p-q} \binom{p-q}{u} \int_{R_{D_1}}^{R_{D_2}} r^{u\alpha+1} e^{-\nu x P_S r^\alpha} dr. \tag{B.5}$$

By invoking [21, Eq. (3.381.8)], we obtain

$$\begin{aligned} F_{B_m}^{AN}\left(x\right) = 1 - \frac{2e^{-\frac{\nu x}{a_n}}}{R_{D_2}^2 - R_{D_1}^2} \sum_{p=0}^{N_A-1} \frac{\nu^p x^p}{p!} \sum_{q=0}^{p} \binom{p}{q} Q_1 \frac{1}{a_n^{p-q}} \\ \times \sum_{u=0}^{p-q} \binom{p-q}{u} \frac{\gamma\left(u+\delta, \frac{\nu x}{a_n} R_{D_2}^\alpha\right) - \gamma\left(u+\delta, \frac{\nu x}{a_n} R_{D_1}^\alpha\right)}{\alpha \left(\frac{\nu x}{a_n}\right)^{u+\delta}}. \end{aligned} \tag{B.6}$$

Let us now turn our attention to the derivation of the integral Q_1 in (B.4) – (B.6). Note that X_m follows the exponential distribution with unit mean, while Y_m follows the distribution $Y_m \sim Gamma\left(N_A - 1, 1\right)$. As such, the PDF of $f_{I_m^{AN}}$ is given by [17]

$$f_{I_m^{AN}}\left(z_m\right) = \begin{cases} \frac{t_1}{e^{\frac{z_m}{P_S}}} \left(1 - \sum\limits_{l=0}^{N_A-2} \frac{\left(\frac{N_A-1}{P_A} - \frac{1}{P_S}\right)^l z_m^l}{l! e^{\left(\frac{N_A-1}{P_A} - \frac{1}{P_S}\right) z_m}}\right), \theta \neq \frac{1}{N_A} \\ \frac{z_m^{N_A-1} e^{-\frac{z_m}{P_S}}}{{P_S}^{N_A} (N_A-1)!}, \theta = \frac{1}{N_A} \end{cases}, \tag{B.7}$$

where we have $t_1 = \frac{\left(1 - \frac{P_A}{(N_A-1)P_S}\right)^{1-N_A}}{P_S}$. Based on (B.7), and applying [21, Eq. (3.326.2)], we can express Q_1 as follows:

$$Q_1 = \begin{cases} \frac{t_1 \Gamma(q+1)}{\left(x\nu + \frac{1}{P_S}\right)^{q+1}} - \sum\limits_{l=0}^{N_A-2} \frac{\frac{t_1}{l!}\left(\frac{N_A-1}{P_A} - \frac{1}{P_S}\right)^l \Gamma(q+l+1)}{\left(\nu x + \frac{N_A-1}{P_A}\right)^{q+l+1}}, \theta \neq \frac{1}{N_A} \\ \frac{\Gamma(q+N_A)}{{P_S}^{N_A}(N_A-1)!\left(\nu x + \frac{1}{P_S}\right)^{q+N_A}}, \theta = \frac{1}{N_A} \end{cases}. \tag{B.8}$$

Upon substituting (B.8) into (B.6), the CDF of $F_{B_m}^{AN}$ is given by (35).

APPENDIX C: PROOF OF LEMMA 5

Based on (32), we express the CDF of $F_{B_n}^{AN}$ as follows:

$$\begin{aligned} F_{B_n}^{AN}(x) &= \Pr\left\{ \|\mathbf{h}_n\|^2 \le x\vartheta\left(\frac{P_A}{N_A-1}Y_n + \frac{1+d_n^{\alpha}}{a_m}\right)\right\} \\ &= 1 - \sum_{p=0}^{N_A-1}\frac{\vartheta^p x^p}{p!}\sum_{q=0}^{p}\binom{p}{q}Q_3\int\limits_{D_1} e^{-\frac{\vartheta x}{a_m}(1+d_n^{\alpha})}\left(\frac{1}{a_m}(1+d_n^{\alpha})\right)^{p-q} f_{D_1}(\omega_n)\,d\omega_n, \end{aligned} \tag{C.1}$$

where $\vartheta = \frac{a_m}{a_n P_S}$, $Q_3 = \int_0^{\infty} e^{-\vartheta x z_n} z_n^q f_{I_n^{AN}}(z_n)\,dz_n$, $f_{I_n^{AN}}$ and $f_{D_1}(\omega_n)$ are the PDF of I_n^{AN} and D_1. Here $I_n^{AN} = \frac{P_A}{N_A-1}Y_n, Y_n = \|\mathbf{h}_n\mathbf{V}_m\|^2$, and $f_{D_1}(\omega_n) = \frac{1}{\pi R_{D_1}^2}$. Upon changing to polar coordinates and applying [21, Eq. (3.381.8)], we arrive at

$$F_{B_n}^{AN}(x) = 1 - \frac{\delta e^{-\frac{\vartheta x}{a_m}}}{R_{D_1}^2}\sum_{p=0}^{N_A-1}\frac{\vartheta^p x^p}{p!}\sum_{q=0}^{p}\binom{p}{q}Q_3 a_m^{q-p}\sum_{u=0}^{p-q}\binom{p-q}{u}\frac{\gamma\left(u+\delta, \frac{\vartheta x}{a_m}R_{D_1}^{\alpha}\right)}{\left(\frac{\vartheta x}{a_m}\right)^{u+\delta}}. \tag{C.2}$$

Finally we turn our attention on Q_3. It is readily seen that I_n^{AN} obeys the Gamma distribution in conjunction with the parameter $\left(N_A-1, \frac{P_A}{N_A-1}\right)$. Then we can obtain the PDF of $f_{I_n^{AN}}(z_n) = \frac{z_n^{N_A-2} e^{-\frac{z_n(N_A-1)}{P_A}}}{\left(\frac{P_A}{N_A-1}\right)^{N_A-1}\Gamma(N_A-1)}$. Applying [21, Eq. (3.326.2)], we can express Q_3 as $Q_3 = \frac{\Gamma(N_A-1+q)}{\Gamma(N_A-1)\left(\frac{P_A}{N_A-1}\right)^{N_A-1}\left(\vartheta x+\frac{N_A-1}{P_A}\right)^{N_A-1+q}}$. Upon substituting Q_3 into (C.2), we obtain the CDF of $F_{B_n}^{AN}(x)$ as (36).

APPENDIX D: PROOF OF LEMMA 6

Based on (34), the CDF of $F_{\gamma_{E_\kappa}^{AN}}$ can be expressed as

$$\begin{aligned} F_{\gamma_{E_\kappa}^{AN}}(x) &= \Pr\left\{ \max_{e\in\Phi_e, d_e\ge r_p}\left\{\frac{a_\kappa P_S X_{e,\kappa}}{I_e^{AN}+d_e^{\alpha}}\right\} \le x\right\} \\ &= E_{\Phi_e}\left\{ \prod_{e\in\Phi_e, d_e\ge r_p}\int_0^{\infty} F_{X_{e,\kappa}}\left(\frac{(z+d_e^{\alpha})\,x}{a_\kappa P_S}\right) f_{I_e^{AN}}(z)\,dz \right\}. \end{aligned} \tag{D.1}$$

Following a procedure similar to that used for obtaining (10), we apply the generating function and switch to polar coordinates. Then (D.1) can be expressed as

$$F_{\gamma_{E_\kappa}^{AN}}(x) = \exp\left[-2\pi\lambda_e \int_{r_p}^{\infty} r e^{-\frac{x}{a_\kappa P_S}r^{\alpha}}\,dr Q_2\right], \tag{D.2}$$

where $Q_2 = \int_0^\infty e^{-z\frac{x}{a_\kappa P_S}} f_{I_e^{AN}}\left(z\right) dz$. Applying [21, Eq. (3.381.9)], we arrive at

$$F_{\gamma_{E_\kappa}^{AN}}\left(x\right) = \exp\left[-\frac{\mu_{\kappa1}^{AN}\Gamma\left(\delta, \mu_{\kappa2}^{AN}x\right)}{x^\delta}Q_2\right]. \tag{D.3}$$

Let us now turn our attention to solving the integral Q_2. Note that all the elements of $\mathbf{h}_e\mathbf{V}_m$ and $\mathbf{h}_e\mathbf{V}_n$ are independent complex Gaussian distributed with a zero mean and unit variance. We introduce the notation $Y_{e,m} = \left\|\mathbf{h}_e\mathbf{V}_m\right\|^2$ and $Y_{e,n} = \left\|\mathbf{h}_e\mathbf{V}_n\right\|^2$. As a consequence, both $Y_{e,m}$ and $Y_{e,n}$ obey the $Gamma\left(N_A-1,1\right)$ distribution. Based on the properties of the Gamma distribution, we have $a_m\sigma_a^2Y_{e,m} \sim Gamma\left(N_A-1, a_m\sigma_a^2\right), a_n\sigma_a^2Y_{e,n} \sim Gamma\left(N_A-1, a_n\sigma_a^2\right)$. Then the sum of these two items I_e^{AN} obeys the generalized integer Gamma (GIG) distribution. According to [28], the PDF of I_e^{AN} is given by

$$f_{I_e^{AN}}\left(z\right) = \left(-1\right)^{N_A-1}\prod_{i=1}^{2}\tau_i^{N_A-1}\sum_{i=1}^{2}\sum_{j=1}^{N_A-1}\frac{a_{N_A-j,N_A-1}}{\left(j-1\right)!}\left(2\tau_i-L\right)^{j-\left(2N_A-2\right)}z^{j-1}e^{-\tau_i z}. \tag{D.4}$$

Upon substituting (D.4) into (D.3), as well as applying [21, Eq. (3.381.4)], after some further manipulations, we obtain the CDF of $F_{\gamma_{E_\kappa}^{AN}}$ as

$$F_{\gamma_{E_\kappa}^{AN}}\left(x\right) = \exp\left[\Omega\frac{\Gamma\left(\delta, x\mu_{\kappa2}^{AN}\right)}{\sum\limits_{p=0}^{j}\binom{j}{p}\left(x\right)^{p+\delta}\left(a_\kappa P_S\right)^{-p}\tau_i^{j-p}}\right]. \tag{D.5}$$

Upon setting the derivative of the CDF in (D.5), we can obtain (37).

REFERENCES

[1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. Vehicular Technology Conference (VTC Spring)*, June Dresden, Germany, Jun. 2013, pp. 1–5.

[2] 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.*, submitted. [Online]. Available: http://arxiv.org/abs/1511.08610

[3] 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, 2014.

[4] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct 2015.

[5] 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, April 2016.

[6] J. Choi, "Minimum power multicast beamforming with superposition coding for multiresolution broadcast and application to NOMA systems," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 791–800, March 2015.

[7] Q. Sun, S. Han, C.-L. I, and Z. Pan, “On the ergodic capacity of MIMO NOMA systems,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 405–408, Aug. 2015.

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

[9] A. Mukherjee and A. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[10] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communications,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[11] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Duong, “Relay selection for security enhancement in cognitive relay networks,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[12] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[13] Y. Liu, L. Wang, S. Zaidi, M. Elkashlan, and T. Duong, “Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model,” *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan 2016.

[14] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[15] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[16] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[17] X. Zhang, X. Zhou, and M. R. McKay, “Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[18] P. C. Pinto, J. Barros, and M. Z. Win, “Secure communication in stochastic wireless networksłpart I: Connectivity,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[19] 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, May 2013.

[20] W. K. D. Stoyan and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. John Wiley and Sons, 1996.

[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.

[22] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[23] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical layer security of tas/mrc with antenna correlation,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[24] 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. of International Commun. Conf. (ICC)*, to appear in 2016.

[25] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[26] H. A. David and N. Nagaraja, *Order Statistics*, 3rd ed. John Wiley, 2003.

[27] E. Hildebrand, “Introduction to numerical analysis,” *NewYork, NY, USA: Dover,*, 1987.

[28] C. A. Coelho, “The generalized integer Gamma distribution a basis for distributions in multivariate statistics,” *Journal of Multivariate Analysis*, vol. 64, no. 1, pp. 86–102, 1998.