Enhancing the Physical Layer Security of Non-orthogonal Multiple Access in Large-Scale Networks
Liu, Y; Qin, Z; Elkashlan, M; Gao, Y; Hanzo, L

© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

For additional information about this publication click this link.
http://qmro.qmul.ac.uk/xmlui/handle/123456789/19088

Information about this research object was correct at the time of download; we occasionally make corrections to records, please therefore check the published record when citing. For more information contact scholarlycommunications@qmul.ac.uk
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. 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.

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

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. The existing MA techniques can be primarily classified into two main categories, namely orthogonal multiple access and non-orthogonal multiple access (NOMA), by distinguishing whether a specific resource block can be occupied by more than one user [2]. More specifically, upon investigating the multiplexing gain gleaned from the different domains, the NOMA technique can be further classified as code-domain NOMA and power-domain NOMA [3]. Power-domain NOMA1, which has been recently proposed for the 3GPP Long Term Evolution (LTE) initiative [4], is deemed to have a superior spectral efficiency [5, 6]. 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/frequency), by applying successive interference cancellation (SIC). The concept of SIC, which was first proposed by Cover in 1972 [7], constitutes a promising technique, since it imposes lower complexity than the joint decoding approach [8]. Hence NOMA techniques have received remarkable attention both in the world of academia and industry [9–13]. Ding et al. [9] 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) counterpart. By considering the user fairness of a NOMA system, a user-power allocation optimization problem was addressed by Timotheou and Krikidis [10]. A cooperative simultaneous wireless power transfer (SWIPT) aided NOMA protocol was proposed by Liu et al. [11], 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. With the goal of maximizing the energy efficiency of transmission in multi-user downlink NOMA scenarios, Zhang et al. [14] proposed an efficient power allocation technique capable of supporting the data rate required by each user. To further improve the performance of NOMA systems, multiple antennas were introduced in [12, 13]. More particularly, the application of multiple-input single-output (MISO) solution to NOMA was investigated by Choi et al. [12], where a two-stage beamforming strategy was proposed. Power optimization was invoked by Sun et al. [13] for maximizing the ergodic capacity of MIMO aided NOMA systems. As a further advance, a massive multiple-input multiple-output (MIMO) aided hybrid heterogeneous NOMA framework was proposed for downlink scenarios.

1Hence in this paper, we focus our attention on the family of power-domain NOMA schemes. We simply use “NOMA” to refer to “power-domain NOMA” in the following.
transmission by Liu et al. [15]. The impact of the locations of users and interferers was investigated by using stochastic geometry approaches.

Given the broadcast nature of wireless transmissions, the concept of physical (PHY) layer security (PLS) was proposed by Wyner as early as 1975 from an information-theoretical perspective [16]. This research topic has sparked of widespread recent interests. To elaborate, PLS has been considered from a practical perspective in [17–21]. 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 [17]. Ding et al. [18] 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. [20]. Furthermore, the physical layer security of D2D communication in large-scale cognitive radio networks was investigated by Liu et al. [21] 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 [22] and AN [23] 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 [23]. 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 [24] 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. [25], with the aid of both beamforming and sectoring techniques. By simultaneously considering matched filter precoding and AN generation techniques, the secure transmission strategies for a multi-user massive MIMO systems was investigated by Wu et al. [26]. Very recently, the PLS of a single-input single-output (SISO) NOMA system was studied by Zhang et al. [27], with the objective of maximizing the secrecy sum rate of multiple users.

A. Motivation and Contribution

As mentioned above, PLS has been studied in various scenarios, but there is still a paucity of research contributions on investigating the security issues of NOMA, which motivates this contribution. Note that the employment of SIC in NOMA results in a unique interference status at the receivers, which makes the analysis of the PLS of NOMA different from that of OMA. 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 [25,28,29]. 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 infinite 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 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 probability; 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 (Eves). We assume that the \( M \) users are divided into \( M/2 \) orthogonal pairs. Each pair is randomly allocated to a single resource block, such as a time slot or an orthogonal frequency band. For simplicity, we only focus our attention on investigating a typical pair of users in this treatise. Random user-pairing is adopted in this work\(^2\). For each pair, the NOMA transmission protocol is invoked. It is assumed that BS is located at the center of a disc, denoted by \( D \), which has a coverage radius of \( R_D \) (which is defined as the user zone for NOMA \(^9\)). The \( M \) randomly roaming LUs are uniformly distributed within the disc. A random number of Eves is distributed across an infinite two-dimensional plane, which are assumed to have powerful detection capabilities and can overhear the messages of all orthogonal RBs, i.e. time slots or frequency slots. The spatial distribution of all Eves is modeled using a homogeneous PPP, which is denoted by \( \Phi_e \) and is associated with the density \( \lambda_e \). It is assumed that the Eves can be detected, provided that they are close enough to BS. Therefore, an Eve-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 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. Without loss of generality, we 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 \(^5, 6\). Therefore, the power allocation coefficients satisfy the conditions that \( a_m > a_n \) and \( a_m + a_n = 1 \). By stipulating this assumption, SIC can be invoked by the \( n \)-th user for first detecting the specific user having a higher transmit power (TX-power), who hence has a less interference-infested signal. Accordingly, the \( m \)-th user’s signal is then remodulated and deducted from the original composite signal. This procedure then directly delivers the decontaminated lower-TX-power signal of the \( n \)-th user itself\(^3\). We assume having fixed power allocation sharing between two users, but optimal power sharing strategies are capable of further enhancing the performance of the networks considered, which is beyond the scope of this paper. Based on the aforementioned assumptions, the instantaneous SNIR of the \( m \)-th user and the signal-to-noise ratio (SNR) of the \( n \)-th user can be written as:

\[
\gamma_m = \frac{a_m|h_m|^2}{a_n|h_n|^2 + \frac{1}{\rho_b}}, \quad (1)
\]

\[
\gamma_n = \rho_b a_n|h_n|^2, \quad (2)
\]

respectively. We introduce the convenient concept of transmit SNR \( \rho_b = \frac{P_T}{\sigma_b^2} \), where \( P_T \) is the TX-power of composite signal at the BS and \( \sigma_b^2 \) 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. Perfectly flawless detection is assumed in this treatise, which is realistic at today’s state-of-the-art with the aid of iterative turbo-detection techniques \(^30, 31\). 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.

\(^3\)It is assumed that perfect SIC is achieved at the \( n \)-th user, although achieving perfect SIC may be a non-trivial task. As a consequence, our analytical results may over-estimate the attainable secrecy performance of networks. Our future work will relax this idealized simplifying assumption, perhaps by analyzing both the connection outage probability and the secrecy outage probability of the networks considered, with the aid the results derived in this treatise.
We consider the worst-case scenario of large-scale networks, in which the Eves are assumed to have powerful detection capabilities [25, 32]. Specifically, by applying multiuser detection techniques, the multiuser data stream received from BS can be distinguished by the Eves, upon subtracting interference generated by the superposed signals from each other. In fact, this assumption overestimates the Eves’ multi-user decodability. In the scenario considered, all the CSIs of the LUs are assumed to be known at BS. However, the CSIs of Eves are assumed to be unknown at BS. The most detrimental Eve is not necessarily the nearest one, but the one having the best channel to BS. Non-colluding eavesdroppers are considered in this work. Therefore, the instantaneous SNR of detecting the information of the $m$-th user and the $n$-th user at the most detrimental Eve can be expressed as follows:

$$
\gamma_{E_n} = \rho_n a_n \max_{e \in \Phi_e, d_e \geq r_p} \left\{ |g_e|^2 L(d_e) \right\} .
$$

(3)

It is assumed that $\kappa \in \{m, n\}$, $\rho_n = \frac{\rho}{E_k}$ is the transmit SNR with $\sigma_n^2$ being the variance of the AWGN at Eves. Additionally, $g_e$ is defined as the small-scale fading coefficient associated with $g_e \sim CN(0, 1)$, $L(d_e) = \frac{1}{d_e^\alpha}$ is the path loss, and $d_e$ is the distance from Eves to BS. Note that due to the existence of the Eve-exclusion area (we assume $r_p > 1$), it is not required to bound the path loss for Eves 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 Eves, 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

$$
F_{\gamma_{B_n}}(x) \approx \varphi_m \sum_{p=0}^{M-n} \left( \begin{array}{c} M-n \\ p \end{array} \right) \frac{(-1)^p}{n+p} \times \sum_{S_m^n} \left( \begin{array}{c} n+p \\ q_0 + \cdots + q_K \end{array} \right) \left( \prod_{k=0}^{K} b_{k}^{\tilde{r}_k} \right) e^{-\frac{\sum_{k=0}^{K} q_k c_k}{\tilde{r}_m}},
$$

(4)

where $K$ is a complexity-vs-accuracy tradeoff parameter,

$$
b_k = -\omega_K \sqrt{1-\phi_k^2 (\phi_k + 1)}, \quad b_0 = -\sum_{k=1}^{K} b_k, \quad c_k = 1 + \frac{R_d}{2} (\phi_k + 1)^2, \quad \tilde{r}_m = \frac{\pi}{\tilde{r}_m}, \quad \phi_k = \cos \left( \frac{2k-1}{2K} \pi \right), \quad S_m^n = \left\{ (q_0, q_1, \cdots, q_K) \mid \sum q_i = n + p, \frac{(n+p)!}{q_0! \cdots q_K!} = \frac{(n+p)!}{q_0! \cdots q_K!} \right\}, \quad \varphi_m = \frac{1}{(M-n)! (n+1)!}.
$$

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) at the top of next page, where

$$
U(x) = \left\{ \begin{array}{ll} 1, & x > 0 \\ 0, & x \leq 0 \end{array} \right\} \text{ is the unit step function, and } \tilde{S}_m^n = \left\{ (q_0, q_1, \cdots, q_K) \mid \sum q_i = m + p \right\}.
$$

Following the similar approach as [33], by applying the generating function [34], (9) can be rewritten as

$$
F_{\gamma_{B_m}}(x) = \exp \left[ -\lambda_e \int_{r_p}^{\infty} \left( 1 - F_{|x|^2} (\frac{x d_{k}^2}{\rho e a_k}) \right) r dr \right] = \exp \left[ -2\pi \lambda_e \int_{r_p}^{\infty} r e^{-\frac{x d_{k}^2}{\rho e a_k}} dr \right].
$$

(10)

By applying [35, Eq. (3.381.9)], we arrive at:

$$
F_{\gamma_{B_m}}(x) = e^{-\frac{\delta^2 \pi \lambda_e (\rho e a_k)^{\delta}}{2} (\frac{x d_{k}^2}{\rho e a_k})}.
$$

(11)

By taking the derivative of the CDF $F_{\gamma_{E_n}}(x)$ in (11), we obtain the PDF $\gamma_{E_n}$ in (8). The proof is completed.
Upon using the results of Lemma 1 and Lemma 3, substituting (4) and (8) into (15), after some further mathematical manipulations, we can express the SOP of the $n$-th user. The proof is completed.

**Theorem 2.** 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 (16) at the top of next page, where we have $\tau_m = 2^{\frac{n}{1-a_m}} - 1$.

**Proof:** Based on (13) and according to [37], the SOP for the $m$-th user is given by

$$P_m(R_m) = \int_0^{\infty} f_{\gamma_{B_m}}(x) F_{\gamma_{B_m}}(2^{R_m}(1+x) - 1) \, dx.$$  

Upon using the results of Lemma 2 and Lemma 3, as well as substituting (5) and (8) into (17), after some further mathematical manipulations, we can express the SOP of the $m$-th user. The proof is completed.

In this paper, based on the assumptions of perfect SIC of LUs and strong detection capabilities of Eves aforementioned, the secrecy outage occurs in the $m$-th user and the $n$-th user are independent. Note that relaxing these two assumptions requires to consider dependence between two users by discussing more sophisticated connect/secrecy outage events, which should be included in our future work with the aid of the results derived in this paper. In other words, the SOP of the $m$-th user has no 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.

**Proposition 1.** The SOP of the selected user pair is given by

$$P_{mn} = 1 - (1 - P_m)(1 - P_n),$$

where $P_n$ and $P_m$ are given by (14) and (16), respectively.

### 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 Eves 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 $\rho_b \rightarrow \infty$, while and the SNR of the channels between BS and Eves is set to arbitrary values. It is noted that for the Eve’s transmit SNR of $\rho_e \rightarrow \infty$, the probability of successful eavesdropping will tend to unity. The secrecy diversity order can be defined as follows:

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

where $P^\infty$ is the asymptotic SOP.
\[ P_n(R_n) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \left( \frac{-1}{n+p} \right) \sum_{\delta=0}^{\infty} \binom{n+p}{\delta} \left( \prod_{K=0}^{K} b_k \right) \times \int_0^\infty \mu_m (\delta x) \delta x^p \phi_m \left( \frac{2^{R_m(1+x)^2}}{p_m \gamma_m} \right) e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}} dx. \]

\[ P_m(R_m) = 1 - e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}} + \varphi_m \sum_{p=0}^{M-m} \binom{M-m}{p} \left( \frac{-1}{n+p} \right) \sum_{\delta=0}^{\infty} \binom{n+p}{\delta} \left( \prod_{K=0}^{K} b_k \right) \times \int_0^\infty \mu_m (\delta x) \delta x^p \phi_m \left( \frac{2^{R_m(1+x)^2}}{p_m \gamma_m} \right) e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}} dx. \]

**Corollary 1.** 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

\[ P^n = G_n(\rho^n) - D_n + \varphi_n \left( \rho^n D_n \right), \]

where we have \( Q_2 = \int_0^{\tau_m} \mu_m e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}} \times \left( \frac{\mu_m 1 e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}}}{x^p \phi_m} \right) n \times dx, \)

\[ G_n = \frac{\varphi_n Q_n}{m}, \text{ and } D_n = n. \]

**Proof:** We commence our diversity order analysis by characterizing the CDF of the LUs \( F_{\gamma_m} \) and \( F_{\gamma_n} \) 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 \( \tilde{h}_n \) as follows:

\[ F_{|h_n|^2}(y) \approx \frac{2y}{\ell} R_D \int_0^y (1 + r^a) r dr = y \ell, \]

where \( \ell = 1 + \frac{2R_D \alpha + \alpha}{\alpha + 2} \). Substituting (21) into (A.2), the asymptotic unordered CDF of \( |\tilde{h}_n|^2 \) is given by

\[ F_{|\tilde{h}_n|^2}(y) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \left( \frac{-1}{n+p} \right) \left( y\ell \right)^{n+p} \approx \varphi_n \left( y\ell \right)^n. \]

Then based on (A.1), we can obtain \( F_{\gamma_m} \) by the asymptotic \( \gamma_m \). After some manipulations, we arrive at the asymptotic SOP of the \(n\)-th user. The proof is completed.

**Remark 1.** Upon substituting (20) into (19), we obtain the secrecy diversity order of the \(n\)-th user is \( n \).

**Corollary 2.** 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

\[ P^m = G_m(\rho_m) - D_m + \varphi_m \left( \rho_m D_m \right), \]

where we have \( Q_2 = \int_0^{\tau_m} \mu_m e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}} \times \left( \frac{\mu_m 1 e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}}}{x^p \phi_m} \right) n \times dx, \)

\[ G_m = \frac{\varphi_m Q_m}{m}, \text{ and } D_m = m. \]

**Proof:** Based on (24) and (22), we can arrive at:

\[ \Phi_m = \frac{\varphi_m Q_m}{m} \left( \frac{\mu_m 1 e^{-\frac{\mu_m 1 \Gamma(x_m^2 \gamma_m)}{x^p \phi_m}}}{x^p \phi_m} \right) n \times dx, \]

Substituting (24) into (6), the asymptotic CDF of \( \gamma_m \) can be expressed as

\[ F_{\gamma_m}(x) = U \left( x - \frac{a_m}{a_n} \right) + U \left( \frac{a_m}{a_m} - x \right) \Phi_m, \]

where \( \Phi_m \) is given in (24). Then, based on (17), we can replace the CDF of \( F_{\gamma_m} \) by the asymptotic CDF of (25). Additionally, we can formulate the asymptotic SOP of the \(m\)-th user. The proof is completed.

**Remark 2.** Upon substituting (23) into (19), we obtain the secrecy diversity order of the \(m\)-th user is \( m \).

**Proposition 2.** For \( m < n \), the secrecy diversity order can be expressed as

\[ d_s = - \lim_{\rho_n \to \infty} \log(P^m + P^n - P^m P^n) = m. \]

**Proof:** Based on **Corollary 2** and **Corollary 1**, and upon substituting (20) and (23) into (18), the asymptotic SOP for the user pair can be expressed as

\[ P^{mn} = P^m + P^n - P^m P^n \approx P^m G_m(\rho_m) - D_m. \]

Upon substituting (27) into (19), we arrive at (26). The proof is completed.

**Remark 3.** The results of (26) indicate that the secrecy diversity order and the asymptotic SOP for the user pair considered are determined by the \(m\)-th user.

**Remark 3** 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.
such, the transmitted superposed information, which is masked by AN at the BS is given by

$$\kappa h_u C \in [39]$$

can be described as follows: an orthogonal basis of can significantly degrade the channel and hence the capacity of channel, it will not impose any effects on LUs. However, it

It is assumed that the perfect CSI of LUs are known at BS. It is assumed that the perfect CSI of LUs are known at the aid of the BS. It is assumed that the perfect 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 AN. More precisely, the key idea of using AN as proposed in [39] can be described as follows: an orthogonal basis of $C^{N_A}$ is generated at BS for user $\kappa$, (where $\kappa \in \{m, n\}$) as a $(N_A \times N_A)$-element precoding matrix $U_\kappa = [u_\kappa, V_\kappa]$, where we have $u_\kappa = h_\kappa / ||h_\kappa||$; and $V_\kappa$ is of size $N_A \times (N_A - 1)$. Here, $h_\kappa$ is denoted as the intended channel between the BS and user $\kappa$. It is noted that each column of $V_\kappa$ is orthogonal to $u_\kappa$. Beamforming is applied at the BS for generating AN. As such, the transmitted superposed information, which is masked by AN at the BS is given by

$$\sum_{\kappa \in \{m, n\}} \sqrt{s_\kappa} x_\kappa = \sum_{\kappa \in \{m, n\}} \sqrt{a_\kappa} (s_\kappa u_\kappa + t_\kappa V_\kappa), \quad (28)$$

where $s_\kappa$ is the information-bearing signal with a variance of $\sigma_s^2$, and $t_\kappa$ is the AN. Here the $(N_A - 1)$ elements of $t_\kappa$ are independent identically distributed (i.i.d.) complex Gaussian random variables with a variance of $\sigma_\kappa^2$. 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 $P_A = (1 - \theta) P_T = (N_A - 1) \sigma_\kappa^2$ is the transmission power of the AN. Here $\theta$ represents the power sharing coefficients between the information-bearing signal and AN.

As shown in Fig. 2, we divide the disc $D$ into two regions, namely, $D_1$ and $D_2$, respectively. The motivation of using this topology hinges on two aspects. The first one is to create more distinct channel quality differences between the paired users, since existing NOMA studies have demonstrated that it is beneficial to pair two users having rather different channel conditions [5, 11, 40]. The second one is that of reducing the complexity of channel ordering in this MISO NOMA system, which provides a compelling flexibility. By doing so, the path loss is the dominant channel impairment in this scenario, because compared to the instantaneous small-scale fading effects, the path loss is more stable and more dominant. A quantitative example of comparing the small-scale fading and path loss was provided in Chapter 2 of [41]. Note that the proposed design cannot guarantee the optimal ordering for MISO NOMA channels. More sophisticated precoding/detection design strategies (e.g., cluster based design, signal alignment and etc.) can be developed for further enhancing the attainable performance of the networks considered [42, 43], but this is beyond the scope of this treatise. 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. 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$^5$. 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

$$y_m = h_m u_m \sqrt{s_m} + h_m u_n \sqrt{a_n s_n} + h_m V_n \sqrt{a_n \alpha} + n_m, \quad \text{Signal part}$$

$$+ h_m \sqrt{a_n \alpha} + n_m, \quad \text{Interference and noise part}$$

where $n_m$ 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

$$\gamma_B m = \frac{a_m \sigma_m^2 ||h_m||^2}{a_m \sigma_m^2 ||h_m||^2 + a_n \sigma_n^2 ||h_n V_n||^2 + 1 + d_m^2}$$

where the variance of $n_m$ 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

$^5$Note that upon invoking the signal alignment technique [43], the BS is capable of simultaneously supporting multiple pairs of NOMA users, by designing more sophisticated precoding/detection strategies for interference cancelation. However, these considerations are beyond the scope of this paper.
signal at user \(n\) is given by
\[
y_n = \frac{h_n u_n \sqrt{\alpha_m n_n}}{\sqrt{1 + d_n^2}} + \frac{h_m \sqrt{\alpha_m m_m}}{\sqrt{1 + d_m^2}} + n_n, \tag{31}
\]
where \(n_n\) 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
\[
\gamma_{B_n}^{AN} = \frac{a_n \sigma_n^2 \| h_n \|^2}{a_n \sigma_n^2 \| h_m \|^2 + 1 + d_n^2}, \tag{32}
\]
where the variance of \(n_n\) is normalized to unity. The signal observed by Eves is given by
\[
y_e = \sum_{\kappa \in \{m, n\}} \frac{h_e \sqrt{\alpha_e x_e}}{\sqrt{d_e^2}} + n_e, \tag{33}
\]
where \(n_e\) is the Gaussian noise at Eves, while \(h_e \in \mathbb{C}^{1 \times N_A}\) is the channel vector between the BS and Eves. Similar to the single-antenna scenario, again, we assume that the Eves 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 Eve associated with detecting user \(\kappa\) is given by
\[
\gamma_{E_{\kappa}}^{AN} = \frac{a_e \sigma_e^2}{e \in F_{\kappa}, d_{\kappa} \geq r_p} \max \left\{ \frac{X_{e, \kappa}}{\Gamma_e^{AN} + d_e^2} \right\}, \tag{34}
\]
where the variance of \(n_e\) is normalized to unity, and we have \(X_{e, \kappa} = \| h_e \|^2 \| h_e \|^2 + a_n \sigma_n^2 \| h_e \|^2 \| h_m \|^2\).

### A. New Channel Statistics

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

**Lemma 4.** 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
\[
F_{B_n}^{AN}(x) = 1 - b_2 e^{-\frac{a_m}{a_m}} \sum_{p=0}^{N_A-1} \sum_{q=0}^{p} \binom{p}{q} x^{N_A-1+p} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{\frac{1}{N_A-1}+q} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{u} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{u+\delta} \frac{a_m}{a_m} \frac{1}{a_m P_s}, \tag{35}
\]
where we have \(b_2 = \frac{2^\delta}{R_p^{r_p} \Gamma(N_A-1)(\frac{2^\delta}{a_m} P_s^{r_p})^{N_A-1}}\) and \(\theta = \frac{\alpha_m}{a_m P_s^{r_p}}\).

**Proof:** See Appendix B.

**Lemma 5.** 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
\[
F_{B_m}^{AN}(x) = 1 - e^{-\frac{a_m}{a_m}} \sum_{p=0}^{N_A-1} \sum_{q=0}^{p} \binom{p}{q} x^{N_A-1+p} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{\frac{1}{N_A-1}+q} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{u} \left( \frac{2^\delta}{a_m} P_s^{r_p} \right)^{u+\delta} \frac{a_m}{a_m P_s}, \tag{36}
\]
where \(\gamma(1, \cdot)\) is the lower incomplete Gamma function, \(\Gamma(\cdot, \cdot)\) is the Gamma function, \(a_1 = \delta \left(1 - \frac{P_A}{(N_A-1)P_s}\right)\left(R_{D_2}^2 - R_{D_1}^2\right) P_s\), and \(\nu = \frac{a_2}{a_2 P_s}\).

**Proof:** See Appendix C.

**Lemma 6.** Assuming that the distribution of Eves obeys a PPP and that the Eve-exclusion zone has a radius of \(r_p\), the PDF of \(f_{\gamma_{E_{\kappa}}}^{AN}\) (where \(\kappa \in \{m, n\}\)) is given by
\[
f_{\gamma_{E_{\kappa}}}^{AN}(x) = -e^{-\theta_{\kappa} P_s^{r_\kappa}} \Gamma(x, \mu_{\kappa}^{AN}) \frac{\mu_{\kappa}^{AN}}{x} \frac{\delta_{\kappa} \Psi_{\kappa, 1}}{x} \frac{\Theta_{\kappa} \Psi_{\kappa, 2}}{x} \Gamma(x, \mu_{\kappa}^{AN} + \delta_{\kappa} \Psi_{\kappa, 1} + \Theta_{\kappa} \Psi_{\kappa, 2}), \tag{37}
\]
where \(\Theta_{\kappa} = \frac{1}{\Gamma(1, \cdot)} \left( \frac{1}{2^\delta P_s^{r_p}} \right) \Gamma(1, \cdot)\), \(\Gamma(\cdot, \cdot)\) is the upper incomplete Gamma function, \(\Psi_{\kappa, 1} = \frac{1}{\Gamma(1, \cdot)} \left( \frac{1}{2^\delta P_s^{r_p}} \right) \Gamma(1, \cdot)\), \(\Psi_{\kappa, 2} = \frac{1}{\Gamma(1, \cdot)} \left( \frac{1}{2^\delta P_s^{r_p}} \right) \Gamma(1, \cdot)\).

**Proof:** See Appendix D.

### B. Secrecy Outage Probability

In this subsection, we investigate the SOP of a multiple-antenna aided scenario relying on AN.

**Theorem 3.** Assuming that the LUs and Eves distribution obey PPPs and that AN is generated at the BS, the SOP of user \(n\) is given by (38) at the top of next page, where \(\tau_n = \delta \left(2^{N_n(1+\tau_p)} - 1\right)^{-1}\).

**Proof:** Using the results of Lemma 4 and Lemma 6, upon substituting (35) and (37) into (15), we can obtain the SOP of user \(n\). The proof is completed.

**Theorem 4.** Assuming that the LUs and Eves distribution obey PPPs and that AN is generated at the BS, for the case
\( P_{n}^{AN}(R_n) = \int_{0}^{\infty} -e^{\Theta_n\Psi_{n1}} \left( \frac{\mu_{n2}^{AN}}{x} e^{-x\mu_{n2}^{AN}} \Psi_{n1} + \frac{\delta\Theta_n\Psi_{n1} + \Theta_n\Psi_{n2}}{x} \right) \times \left( 1 - b_2 e^{-\gamma_{n}} \sum_{p=0}^{N_A-1} \frac{t_{m}^p}{p!} \sum_{q=0}^{p} \frac{p}{q} \Gamma(N_A-1+q) a_{m_1}^{n}\sum_{u=0}^{p-q} \frac{(p-q) u}{a_{m_1} + \frac{N_A-1+q}{p_A}} \right) dx, \) (38)

\[ P_{m}^{AN}(R_m) = \int_{0}^{\infty} -e^{\Theta_m\Psi_{m1}} \left( \frac{\mu_{m2}^{AN}}{x} e^{-x\mu_{m2}^{AN}} \Psi_{m1} + \frac{\delta\Theta_m\Psi_{m1} + \Theta_m\Psi_{m2}}{x} \right) \times \left( 1 - a_2^* \sum_{p=0}^{N_A-1} \frac{t_{m}^p}{p!} \sum_{q=0}^{p} \frac{p}{q} a_{m}^{n}\sum_{u=0}^{p-q} \frac{(p-q) u}{a_{m_1} + \frac{N_A-1+q}{p_A}} \right), \] (39)

\( \theta \neq \frac{1}{N_A}, \) the SOP of user \( m \) is given by (39) at the top of the next page, where we have 
\[ a_1^* = \frac{\delta e^{-\gamma_{n}} (1 - \frac{p_A}{(N_A-1)p_S})^{1+N_A}}{R_{m2} - R_{m1}} \]

\[ T_1 = \sum_{u=0}^{\infty} \frac{\sum_{p=0}^{p-q} \frac{p}{q} \Gamma(q+1)}{a_{m_1} + \frac{N_A-1+q}{p_A}}, \]

\[ t_{m}^* = \frac{1}{\nu(2^{p/m} (1+x) - 1)}. \]

For the case of \( \theta = \frac{1}{N_A} \), the SOP for user \( m \) is given by (39) upon substituting \( K(\theta) \) with \( K^*(\theta) \), where \( K^*(\theta) = 1 - a_2^* \sum_{p=0}^{N_A-1} \frac{t_{m}^p}{p!} \sum_{q=0}^{p} \frac{p}{q} a_{m}^{n}\sum_{u=0}^{p-q} \frac{(p-q) u}{a_{m_1} + \frac{N_A-1+q}{p_A}} \), and \( T_1 \) is given by 
\[ (R_{m2} - R_{m1}) \sum_{n=0}^{\infty} \left( \frac{a_{m}^{n}}{a_{m_1}} \right)^n. \]

Proof: Using the results of Lemma 5 and Lemma 6, upon substituting (36) and (37) into (17), we obtain the SOP of user \( m \). The proof is completed.

Proposition 3. The SOP of multiple-antenna aided scenario relaying on \( AN \) for the selected user pair can be expressed as
\[ P_{m}^{AN} = 1 - (1 - P_{m}^{AN}) (1 - P_{n}^{AN}). \] (40)

where \( P_n \) and \( P_m \) are given by (38) and (39), respectively.

C. Large Antenna Array Analysis

In this subsection, we investigate the system’s asymptotic behavior when the BS is equipped with large antenna arrays. Large antenna arrays using narrow beamforming are potentially capable of distinguishing multiple users in the angular domain [44, 45]. Nonetheless, the users covered by the same narrow beam in dense deployments still remain non-orthogonal [46]. It is noted that for the exact SOP derived in (39) and (38), 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 [24],
\[ \lim_{N_A \to \infty} \| h_n \| \to N_A, \quad \lim_{N_A \to \infty} \| h_n^2 \| \to N_A - 1, \quad \text{and} \quad \lim_{N_A \to \infty} \| h_n v_m \| \to N_A - 1, \quad \text{and} \]

\[ \lim_{N_A \to \infty} \| h_m \| \to N_A \].

\[ \text{lim} \quad \| h_m v_n \| \to N_A - 1. \]

We first derive the asymptotic \( N_A \to \infty \) of user \( n \) for \( N_A \to \infty \).

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
\[ F_{B_{n}\infty}^{AN}(x) = \begin{cases} 0, x < \zeta_n, \\ 1 - \frac{(a_0 P_A^{n} a_{N_A-1})^{\delta}}{R_{D_1}^{2}}, & \xi_n \leq x \leq \zeta_n, \\ 1, x \geq \xi_n \end{cases} \] (41)

where we have \( \zeta_n = \frac{a_0 P_A^{n} a_{N_A-1}}{R_{D_1}^{2} + a_{0} P_A^{n} a_{+1}} \) and \( \xi_n = \frac{a_0 P_A^{n} a_{N_A-1}}{R_{D_1}^{2} + a_{0} P_A^{n} a_{+1}} \).

Proof: Based on (32), we can express the asymptotic CDF of \( F_{B_{n}\infty}^{AN} \) as \( F_{B_{n}\infty}^{AN}(x) = \text{Pr} \left\{ a_0 P_A^{n} a_{N_A-1} \leq x \right\} \). After some further mathematical manipulations, we can obtain the CDF of \( F_{B_{n}\infty}^{AN} \) for large antenna arrays. The proof is completed.

We then derive the asymptotic CDF of user \( m \) for \( N_A \to \infty \).

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
\[ F_{B_{m}\infty}^{AN}(x) = \begin{cases} 1, x \geq \zeta_m, \\ \frac{b_1}{R_{D_2}^{2} - R_{m}^{2}} \int_{r_{m}^{2}}^{R_{D_2}^{2}} \frac{r e^{-r^{2}/2}}{R_{m}^{2}} dr, \xi_m < x \leq \zeta_m, \\ \frac{b_1}{R_{D_2}^{2} - R_{m}^{2}} \int_{r_{m}^{2}}^{R_{D_2}^{2}} \frac{r e^{-r^{2}/2}}{R_{m}^{2}} dr, x < \xi_m \end{cases} \] (42)

where we have \( b_1 = \frac{a_0 P_A^{n} a_{N_A-1}}{R_{D_2}^{2} + a_{0} P_A^{n} a_{+1}} \), \( t_m = \| h_m v_n \| \), \( \zeta_m = \frac{a_0 P_A^{n} a_{N_A-1}}{R_{D_2}^{2} + a_{0} P_A^{n} a_{+1}} \), \( \xi_m = \frac{a_0 P_A^{n} a_{N_A-1}}{R_{D_2}^{2} + a_{0} P_A^{n} a_{+1}} \).
Proof: Similarly, based on (30), the CDF of the asymptotic $F_{Bm,\infty}^A$ is given by

$$F_{Bm,\infty}^A(x) = \Pr \left\{ \frac{a_mP_SN_A}{a_nP_S\left|h_m\right|^2 + a_nP_A + d_m^2} \leq x \right\}$$

$$= \frac{a_m}{a_n}P_SN_A$$

After some further mathematical manipulations, we obtain the CDF of $F_{Bm,\infty}^A$ for large antenna arrays. The proof is completed. ■

Let us now turn our attention to the derivation of the Eves’ PDF in a large-scale antenna scenario.

**Lemma 9.** Assuming that the Eves distribution obeys a PPP and that AN is generated at the BS, the Eve-exclusion zone has a radius of $r_m$, and $N_A \to \infty$, the PDF of $f_{\gamma_{Bm}\infty}^A$ (where $\kappa \in \{m, n\}$) is given by

$$f_{\gamma_{Bm}\infty}^A(x) = e^{-\frac{a_m\gamma_{Bm}\infty}{2}\left|h_B\right|^2} \frac{P_{AN}}{P_{BS}} \mu_{\kappa_1} x^{-\delta}$$

$$\times \left( \left(\mu_{\kappa_2}\right)^{x-1} - e^{-\frac{a_m\gamma_{Bm}\infty}{2}\left|h_B\right|^2} x + \frac{P_{AN}}{a_nP_S} + \frac{\delta}{x} \right).$$

Proof: Using the theorem of large values, we have

$$\lim_{N_A \to \infty} I_{\gamma_{Bm}\infty}^A = a_m\sigma_B^2\left|h_B\right|^2 + a_n\sigma_B^2\left|h_B\right|^2 = P_A.$$ The asymptotic CDF of $F_{\gamma_{Bm}\infty}^A$ associated with $N_A \to \infty$ is given by

$$F_{\gamma_{Bm}\infty}^A(x) = \Pr \left\{ \max_{\kappa \in \{m, n\}} \left\{ \frac{a_mP_SX_{\kappa,n}}{\mu_{\kappa_1} x^2 + d_m^2} \right\} \leq x \right\}$$

$$= E_{\Phi} \left\{ \prod_{\kappa \in \{m, n\}} F_{X_{\kappa,n}} \left( \frac{P_A + d_m^2}{a_nP_S} \right) \right\}.$$ 

(45)

Following the procedure used for deriving (10), we apply the generating function and switch to polar coordinates. Then with the help of [35, Eq. (3.381.9)], (45) can be expressed as

$$F_{\gamma_{Bm}\infty}^A(x) = \exp \left[ -\frac{\mu_{\kappa_1}}{x^\delta} \Gamma \left( \delta, \frac{a_m\gamma_{Bm}\infty}{2}\left|h_B\right|^2 \right)e^{-\frac{P_{AN}}{a_nP_S}} \right].$$

(46)

Taking derivative of (46), we obtain the PDF of $f_{\gamma_{Bm}\infty}^A$. The proof is completed. ■

Remark 4. The results derived in (44) show that the PDF of $f_{\gamma_{Bm}\infty}^A$ is independent of the number of antennas $N_A$ in our large antenna array analysis.

Let us now derive the SOP for our large antenna array scenario in the following two Theorems.

**Corollary 3.** Assuming that the LUs and Eves distribution obey PPPs, AN is generated at the BS and $N_A \to \infty$, the SOP for user $n$ is given by

$$P_{AN}^n(R_n) = 1 - e^{-\frac{a_n\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2} P_{AN}$$

$$+ \mu_{\kappa_1} \int_{\chi_{\kappa_1}}^{\infty} e^{-\frac{a_m\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2} \frac{P_{AN}}{a_nP_S} + \frac{\delta}{x} \right) \ dx.$$ 

(47)

where $\chi_{\kappa_1} = \frac{\chi_{\kappa_2} + 1}{2\gamma_{AN}(\mu_{\kappa_2})} - 1$, $\chi_{\kappa_2} = \frac{\chi_{\kappa_2} + 1}{2\gamma_{AN}(\mu_{\kappa_2})} - 1$, and $\Xi_k = x^{-\delta} \left( \frac{P_{AN}}{a_nP_S} \delta - 1 - e^{-\frac{a_m\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2} x + \Gamma \left( \delta, \frac{a_m\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2 \right) \right).$

Proof: Using the results of Lemma 7 and Lemma 9, upon substituting (41) and (44) into (15), we can express the SOP for user $n$.

**Corollary 4.** Assuming that the LUs and Eves distribution obey PPPs, AN is generated at the BS, and $N_A \to \infty$, the SOP for user $m$ is given by (48) at the top of the next page, where we have $\Xi_k = x^{-\delta} \left( \frac{P_{AN}}{a_nP_S} \delta - 1 - e^{-\frac{a_m\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2} x + \Gamma \left( \delta, \frac{a_m\gamma_{AN}(\mu_{\kappa_2})}{2}\left|h_B\right|^2 \right) \right).$

Proof: Using the results of Lemma 8 and Lemma 9, upon substituting (42) and (44) into (17), we can express the SOP for user $m$. The proof is completed. ■

**Proposition 4.** Under the assumption of $N_A \to \infty$, the SOP of multiple-antenna aided scenario relaying on AN for the selected user pair can be expressed as

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

(49)

where $P_{AN}^m,\infty$ and $P_{AN}^m,\infty$ are given by (47) and (48), respectively.

IV. Numerical Results

In this section, our numerical results are presented for characterizing the performance of large-scale networks. The complexity-vs-accuracy tradeoff parameter is $K = 20$. Table I summarizes the different Monte Carlo simulation parameters used in this section. BPCU is short for bit per channel use.

A. Secrecy outage probability with channel ordering

From Fig. 3 to Fig. 5, we investigate the secrecy performance in conjunction with channel ordering, which correspond to the scenario considered in Section II.

Fig. 3 plots the SOP of a single user ($m$-th and $n$-th) versus $\rho_l$ for different user zone radii. The curves represent the exact

<table>
<thead>
<tr>
<th>TABLE I: Table of Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Monte Carlo simulations repeated</td>
</tr>
<tr>
<td>The radius of a disc region for Eves</td>
</tr>
<tr>
<td>Power sharing coefficients of NOMA</td>
</tr>
<tr>
<td>Targeted secrecy rates</td>
</tr>
<tr>
<td>Pass loss exponent</td>
</tr>
<tr>
<td>The radius of the user zone of Section II</td>
</tr>
<tr>
<td>The radius of the user zone of Section III</td>
</tr>
</tbody>
</table>
analytical SOP of both the m-th user and of n-th user derived in (16) and (14), respectively. The asymptotic analytical SOP of both the m-th and n-th users, are derived in (23) and (20), respectively. Fig. 3 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 (23) and (20).

Fig. 4 plots the SOP of the selected user pair versus the transmit SNR $\rho_b$, with $\rho_e = 10$ dB, $\alpha = 4$, $\lambda_e = 10^{-3}$, $M = 2$, $m = 1$, $n = 2$, and $r_p = 10$ m. The exact analytical results are calculated from (16) and (14). The asymptotic analytical results are calculated from (20) and (23).

By contrast, the solid curves indicate a higher secrecy outage probability, which is due to the fact that the secrecy diversity order of the user pair is determined by that of the poor one. This behavior is due to the plausible fact that a lower $\lambda_e$ results in an improved PLS, i.e. reduced SOP. This behavior is due to the plausible fact that a lower $\lambda_e$ results in having less Eves, 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. It is worth pointing out that dynamic power sharing between two users is
and secrecy performance. This is due to the fact that most detrimental E is considered. As a result, the distinctive Eves, which reduces the multiuser diversity gain, when the increasing the number of antennas is capable of increasing the secrecy performance is improved. It is also worth noting that the capability of the most detrimental E is reduced and hence the techniques, while user of cancelling the interference imposed by user exists an optimal value for power allocation, which depends on the system parameters.

Fig. 6 plots the SOP of user m and user n versus \( \theta \) 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 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 \( \theta \). This phenomenon indicates that there exists an optimal value for power allocation, which depends on the system parameters.

B. Secrecy outage probability with artificial noise

From Fig. 6 to Fig. 10, we investigate the secrecy performance in the presence of AN, which correspond to the scenario considered in Section III.

Fig. 6 plots the SOP of user m and user n versus \( \theta \) for different Eve-exclusion zones. The solid and dashed curves represent the analytical performance of user m and user n, corresponding to the results derived in (39) and (38). Monte Carlo simulations are used for verifying our derivations. Fig. 6 confirms a close agreement between the simulation and analytical results. Again, a reduced SOP can be achieved by increasing the Eve-exclusion zone, which degrades the channel conditions of the Eves. 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 \( \theta \). This phenomenon indicates that there exists an optimal value for power allocation, which depends on the system parameters.

Fig. 7 plots the SOP of user m and user n versus \( \lambda_e \) 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 \( \lambda_e \) leads to having less Eves, 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 \( (N_A,1) \) distributions, which is the benefit of the improved multi-antenna diversity gain.

Fig. 8 plots the SOP of the selected user pair versus \( N_A \), with \( R_{D_1} = 5 \text{ m, } R_{D_2} = 10 \text{ m, } \theta = 1 \text{, } \lambda_e = 10^{-3}, \rho_t = 30 \text{ dB.} \)

It is observed that the SOP first decreases then increases as
The exact analytical results are calculated from (40).

This behavior can be explained as follows. The SOP of the selected user pair is determined by user $m$. As $\rho_t$ 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 $\rho_t$ 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 $\rho_t$ and the SOP. It is also noted that the power sharing factor $\theta$ also affect the optimal SOP associated with different values of $\rho_t$. This phenomenon indicates that it is of salient significance to select beneficial system parameters. Furthermore, optimizing the parameters $\rho_t$ and $\theta$ is capable of further improving the SOP.

Fig. 10 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 Eves 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 Eves’ 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 Eve-exclusion zone and by generating AN at the BS. Assuming perfect SIC operations may lead to overestimating the performance of the networks considered, hence our future research may consider investigating imperfect SIC. Optimizing the power sharing between two NOMA users is capable of further improving the secrecy performance of the networks considered, which is another promising future research direction.

APPENDIX A: PROOF OF LEMMA 1

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

$$F_{YB}(x) = \Pr \left\{ h_B | h_n |^2 \leq x \right\} = F_{|h_n|^2} \left( \frac{x}{\rho t a_m} \right) , \quad (A.1)$$

where $F_{|h_n|^2}$ is the CDF of the ordered channel gain for the $n$-th user. Assuming $y = \frac{x}{\rho t a_m}$, and using order statistics [47] as well as applying binary series expansion, the CDF of the ordered channels has a relationship with the unordered channels captured as follows:

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

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, \( F_{\bar{h}_n} \) is expressed as

\[
F_{\bar{h}_n}(y) = \frac{2}{R_D^2} \int_0^{R_D} \left( 1 - e^{-(1+y^2)r} \right) r \, dr.
\]  
(A.3)

However, it is challenging to arrive at an easily implemented insightful expression for \( F_{\bar{h}_n}(y) \). Therefore, the Gaussian-Chebyshev quadrature relationship [48] is invoked for finding an approximation of (A.3) in the following form:

\[
F_{\bar{h}_n}(y) \approx \sum_{k=0}^{K} b_k e^{-c_k y}. \tag{A.4}
\]

Substituting (A.4) into (A.2) and applying the multinomial theorem, the CDF \( F_{\bar{h}_n} \) of ordered channel gain is given by

\[
F_{\bar{h}_n}(y) \approx \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \left( \frac{y}{n+p} \right)^p \left( \frac{1-p}{n+p} \right)^{M-n-p} \times \sum_{n=\sum_{k=0}^{K} q_k} \binom{K}{q_k} b_k e^{-c_k y}. \tag{A.5}
\]

Substituting \( y = \frac{x}{\rho_0 h_n} \) into (A.5), we can obtain (4). The proof is completed.

APPENDIX B: PROOF OF LEMMA 4

Based on (32), we express the CDF of \( F_{\bar{h}_n} \) as follows:

\[
F_{\bar{h}_n}(x) = \Pr \left\{ \left\| h_n \right\|^2 \leq x \varphi \left( \frac{N_A}{N_A - 1} Y_n + \frac{1 + d_m}{a_m} \right) \right\} = 1 - \sum_{p=0}^{N_A-1} \varphi_p \sum_{q=0}^{p} \binom{p}{q} Q_3 \times e^{-\frac{\varphi_p}{a_m} \left( 1 + d_m \right)^{p-q}} f_{D_1}(\omega_n) \, d\omega_n, \tag{B.1}
\]

where \( \varphi = \frac{a_m}{\rho_0 h_n} \), \( Q_3 = \int_0^\infty e^{-\psi^{\varphi_q} m} f_{I_{\bar{h}_n}}(z_m) \, dz_m \), \( f_{I_{\bar{h}_n}} \) and \( f_{D_1}(\omega_n) \) are the PDF of \( I_{\bar{h}_n} \) and \( D_1 \). Here \( I_{\bar{h}_n} = \frac{1}{\rho_0 h_n} Y_n = \left\| h_n \right\|^2 \), and \( f_{D_1}(\omega_n) = \frac{\pi}{R_D^2} \).

Upon changing to polar coordinates and applying [35, Eq. (3.381.8)], we arrive at

\[
F_{\bar{h}_n}(x) = 1 - \frac{\varphi q_m}{R_D^2} \sum_{p=0}^{N_A-1} \varphi_p \sum_{q=0}^{p} \binom{p}{q} Q_3 \times e^{-\frac{\varphi_p}{a_m} \left( 1 + d_m \right)^{p-q}} f_{D_1}(\omega_n) \, d\omega_n. \tag{B.2}
\]

Finally we turn our attention on \( Q_3 \). It is readily seen that \( I_{\bar{h}_n} \) obeys the Gamma distribution in conjunction with the parameter \( (N_A - 1, \frac{d_m}{\varphi_q}) \). Then we can obtain

the PDF of \( f_{I_{\bar{h}_n}}(z_m) = \frac{z_m^{N_A-2} e^{-\frac{z_m}{d_m} \varphi_q}}{\Gamma(N_A-1)} \). Applying [35, Eq. (3.326.2)], we can express \( Q_3 \) as

\[
Q_3 = \frac{\varphi q_m}{\Gamma(N_A-1)} \left( \frac{d_m}{\varphi_q} \right)^{N_A-1} \left( \frac{z_m}{d_m} \right)^{N_A-1-\varphi_q} \times \frac{\left( \frac{d_m}{\varphi_q} \right)^{N_A-1}}{\Gamma(N_A-1)} \left( \frac{z_m}{d_m} \right)^{N_A-1-\varphi_q} \tag{B.3}
\]

Upon substituting \( Q_3 \) into (B.2), we obtain the CDF of \( F_{\bar{h}_n}(x) \) as (35).

APPENDIX C: PROOF OF LEMMA 5

Based on (30), we express the CDF of \( F_{\bar{h}_m} \) as

\[
F_{\bar{h}_m}(x) = \Pr \left\{ \left\| h_m \right\|^2 \leq x \frac{a_m \sigma_n^2}{\left\| h_m \right\|^2} \right\} \leq x \tag{C.1}
\]

It may be readily seen that \( \left\| h_m \right\|^2 \) obeys a Gamma distribution having the parameters of \((N_A, 1)\). Hence the CDF of \( \left\| h_m \right\|^2 \) is given by

\[
F_{\bar{h}_m}(x) = 1 - e^{-x} \sum_{p=0}^{N_A-1} \frac{x^p}{p!}. \tag{C.2}
\]

Denoting \( X_m = \left\| h_m \right\|^2, Y_m = \left\| h_m \right\|^2 \), based on (C.2), we can re-write (C.1) as

\[
F_{\bar{h}_m}(x) = \Pr \left\{ \left\| h_m \right\|^2 \leq x \varphi \left( \frac{1 + d_m}{a_m} \right) \right\} = 1 - \int_0^\infty \sum_{p=0}^{N_A-1} \frac{x^p (1 + d_m)}{a_m} \varrho(x) \, dx. \tag{C.4}
\]

By invoking [35, Eq. (3.381.8)], we obtain

\[
F_{\bar{h}_m}(x) = 1 - \frac{2e^{-\frac{x}{a_m}}}{R_D^2 - R_D^2} \sum_{p=0}^{N_A-1} \varphi_p \sum_{q=0}^{p} \binom{p}{q} Q_1 \times e^{-\frac{\varphi_p}{a_m} \left( 1 + d_m \right)^{p-q}} f_{D_1}(\omega_m) \, d\omega_m. \tag{C.5}
\]

By invoking [35, Eq. (3.381.8)], we obtain

\[
F_{\bar{h}_m}(x) = 1 - \frac{2e^{-\frac{x}{a_m}}}{R_D^2 - R_D^2} \sum_{p=0}^{N_A-1} \varphi_p \sum_{q=0}^{p} \binom{p}{q} Q_1 \times e^{-\frac{\varphi_p}{a_m} \left( 1 + d_m \right)^{p-q}} f_{D_1}(\omega_m) \, d\omega_m. \tag{C.6}
\]
Let us now turn our attention to the derivation of the integral $Q_1$ in (C.4) – (C.6). Note that $X_m$ follows the exponential distribution with unit mean, while $Y_m$ follows the distribution $Y_m \sim \text{Gamma}(N_A - 1, 1)$. As such, the PDF of $f_{IA_N}$ is given by [25]

$$f_{IA_N}(z_m) = \left\{ \begin{array}{ll}
\frac{t_1}{\Gamma(q) s_p} \left( 1 - \frac{N_A - 2}{N_A - 1} \right)^{\frac{1}{N_A}} z_m, & \theta \neq \frac{1}{N_A} \\
\frac{N_A - 1}{\Gamma(q) s_p} \left( \frac{N_A - 2}{N_A - 1} \right)^{\frac{1}{N_A}} e^{-z_m}, & \theta = \frac{1}{N_A}
\end{array} \right. , \quad (C.7)$$

where we have $t_1 = \left( 1 - \frac{N_A - 1}{N_A - 1} \right)^{\frac{1}{N_A}}$. Based on (C.7), and applying [35, Eq. (3.326.2)], we can express $Q_1$ as follows:

$$Q_1 = \left\{ \begin{array}{ll}
\frac{t_1 \Gamma(q+1)}{(x+p+1)} \left( 1 - \frac{N_A - 2}{N_A - 1} \right)^{\frac{1}{N_A}} \frac{N_A - 1}{\Gamma(q+1) s_p} \left( \frac{N_A - 2}{N_A - 1} \right)^{\frac{1}{N_A}} e^{-z_m}, & \theta \neq \frac{1}{N_A} \\
\frac{N_A - 1}{\Gamma(q+1) s_p} \left( \frac{N_A - 2}{N_A - 1} \right)^{\frac{1}{N_A}} e^{-z_m}, & \theta = \frac{1}{N_A}
\end{array} \right. , \quad (C.8)$$

Upon substituting (C.8) into (C.6), the CDF of $F_{IA_N}$ is given by (36).

**APPENDIX D: PROOF OF LEMMA 6**

Based on (34), the CDF of $F_{IA_N}$ can be expressed as

$$F_{IA_N}(x) = \Pr \left\{ e \in \Phi_x, d_{e} \geq r_p \left\{ \frac{a_p P_s X_{e,n}}{A_{IN} + d_{e}^2} \right\} \leq x \right\}$$

$$= E_{\Phi_x} \left\{ \prod_{e \in \Phi_x, d_{e} \geq r_p} \int_0^\infty F_{X_{e,n}} \left( \frac{z + d_{e}^2}{a_p P_s} \right) f_{IA_N}(z) \, dz \right\} . \quad (D.1)$$

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

$$F_{IA_N}(x) = \exp \left\{ -2\pi \lambda \int_0^\infty e^{-\frac{t^2}{2\lambda}} \, dt Q_2 \right\} , \quad (D.2)$$

where $Q_2 = \int_0^\infty e^{-\frac{z^2}{2\lambda}} f_{IA_N}(z) \, dz$. Applying [35, Eq. (3.381.9)], we arrive at

$$F_{IA_N}(x) = \exp \left\{ -\frac{\mu_e \Gamma(\delta, \mu_e^2 x)}{x^\delta} \right\} Q_2 . \quad (D.3)$$

Let us now turn our attention to solving the integral $Q_2$. Note that all the elements of $h_i, V_m$ and $h_i, V_n$ are independent complex Gaussian distributed with a zero mean and unit variance. We introduce the notation $Y_{e,m} = \|h_i V_{m}\|^2$ and $Y_{e,n} = \|h_i V_{n}\|^2$. As a consequence, both $Y_{e,m}$ and $Y_{e,n}$ obey the Gamma $(N_A - 1, 1)$ distribution. Based on the properties of the Gamma distribution, we have $a_m \sigma_2^2 Y_{e,m} \sim \text{Gamma} (N_A - 1, a_m \sigma_2^2)$, $a_n \sigma_2^2 Y_{e,n} \sim \text{Gamma} (N_A - 1, a_n \sigma_2^2)$. Then the sum of these two items $I_{AN}$ obeys the generalized integer Gamma (GIG) distribution. According to [49], the PDF of $I_e$ is given by

$$f_{IA_N}(z) = \left( \frac{a_{N_A - 1}}{(j - 1)!} \right)^{N_A - 1} z^{j-1} e^{-z} . \quad (D.4)$$

Upon substituting (D.4) into (D.3), as well as applying [35, Eq. (3.381.4)], after some further manipulations, we obtain the CDF of $F_{IA_N}$ as

$$F_{IA_N}(x) = \exp \left\{ \frac{\Gamma(\delta, \mu_x^2 x)}{\sum_{p=0}^{\infty} \binom{N_A}{p} (a_p P_s)^{-p} \gamma^p} \right\} . \quad (D.5)$$

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

**REFERENCES**


