Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks

Zhijin Qin*, Yuanwei Liu*, Zhiguo Ding†, Yue Gao*, and Maged Elkashlan*
* Queen Mary University of London, London, UK
† Lancaster University, Lancaster, UK

***Abstract*—In this paper, the physical layer security of applying non-orthogonal multiple access (NOMA) in large-scale networks is investigated. In the considered scenario, both the NOMA users and eavesdroppers are spatially randomly deployed. A protected zone around the source node is adopted to enhance the security of a random network. In order to characterize the secrecy performance of the considered scenario, new exact and asymptotic expressions for the security outage probability are derived. These analytical results demonstrate that the secrecy diversity order is m, which is determined by the user with poor channel condition. Monte Carlo simulations are provided to verify the derived analytical results. Furthermore, it is also confirmed that the secure performance of the NOMA networks can be improved by either enlarging the scope of the protected zone or reducing the scope of the user zone.**

I. Introduction

Non-orthogonal multiple access (NOMA) has been conceived as a breakthrough technology in the fifth generation (5G) networks because of its superior spectral efficiency [1, 2]. It is pointed that NOMA has the potential to integrate well with existing multiple access (MA) paradigms [3] as it exploits a new dimension, the power domain, which means that multiple users can be served at the same resource block (e.g., time/frequrecy/code). So far, NOMA has received remarkable attention. In [4], the performance of a downlink NOMA scheme with randomly deployed users was investigated. By considering the user fairness of NOMA system, a power allocation optimization problem for different users was addressed in [5]. To further improve the performance of NOMA system, the multiple antennas technologies were introduced to NOMA in [6, 7], by providing the additional degrees of freedom. Particularly, the application of multiple-input single-output (MISO) to NOMA was investigated in [6]. With considering signal alignment, a more general multiple-input multiple-output (MIMO) framework both for downlink and uplink transmission was proposed in [7].

It is noted that wireless communication networks are confronted with security issues due to the broadcast nature of the wireless medium. The concept of physical (PHY) layer security, which was initially proposed by Wyner [8] from the information-theoretical perspective, has been sparked widespread interest. Lately, research works of PHY layer security are mainly from a practical perspective [9–12]. Specifically, a robust beamforming with applying artificial noise to mitigate the impact of imperfect channel state information (CSI) in MIMO wiretap channels was proposed in [9]. In [10], the authors introduced the cooperative diversity into secure communications. Particularly, the impact of eavesdroppers on the diversity and multiplexing gains were investigated in both a single-antenna scenario and a multiple-antennas scenario. In addition, by considering the security enhancement in cognitive radio relay networks, the authors of [11] proposed several policies by opportunistically performing relay selection. Furthermore, by studying more realistic scenarios, such as the randomly deployed users in large-scale networks, the authors of [12] investigated the physical layer security where both legitimate and eavesdropping nodes are modeled using stochastic geometry.

As aforementioned, PHY layer security has been well studied in many scenarios. However, the design of secrecy transmission for NOMA protocol is still not clear. The aim of this paper is to examine the secure performance of applying NOMA protocol in large-scale networks by considering a downlink communication scenario. Particularly, one base station (BS) is supposed to communicate with M NOMA users which are randomly deployed in an finite user zone. The m-th NOMA user has m-th order of channel connection to the BS. In order to reduce the system complexity, user pairing technique is adopted among the M NOMA users [3], i.e., the m-th user is paired with the n-th user to perform NOMA. A random number of eavesdroppers are randomly deployed in an infinite two dimension via a homogeneous Poisson point process (PPP). In order to improve the secrecy performance of the large-scale networks, a protected zone around the BS is introduced, in which no eavesdroppers are allowed to locate inside. Based on the aforementioned scenario, we derive the exact analytical expressions for the secrecy outage probability of the selected pair of NOMA users. To obtain more insights, we further proceed the asymptotic analyses and confirm that: 1) for a single user, the m-th user can experience a secrecy diversify of m; 2) for the selected pair, the secrecy diversity order is determined by the poor one of the paired users. It is also noted that the secure performance can be improved by either enlarging the scope of the protected zone or reducing the scope the user zone.

II. Network Model

As shown in Fig. 1, we focus on a downlink secure communication scenario. In the considered scenario, one BS (Alice) communicates with M users (Bobs) by applying the NOMA transmission protocol under the malicious attempt of

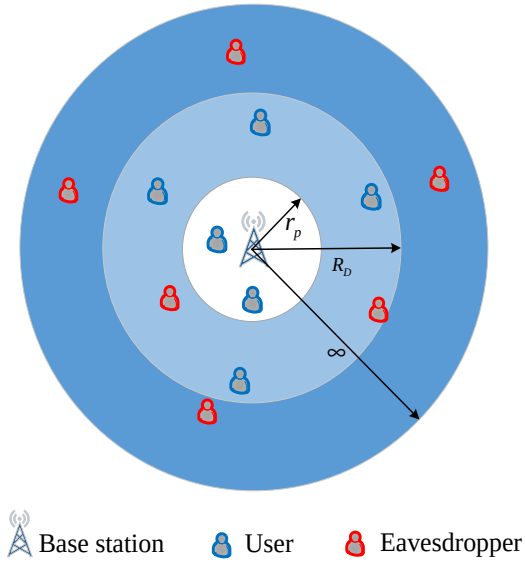

Fig. 1: Network model for the NOMA transmission protocol under malicious attempt of eavesdroppers in large-scale networks.

eavesdroppers (Eves). The Eves would interpret the signal but without trying to modify it. It is assumed that Alice is located at the origin of a disc, denoted by $\mathcal{D}$ with radius R_D as its coverage (which is known as the user zone for NOMA). The M randomly deployed Bobs are uniformly distributed within the disc. A random number of Eves are distributed in an infinite two dimensional plane. The spatial topology of all Eves are modeled using homogeneous poisson point processes (PPPs), denoted by Φ_e with density λ_e. In addition, all channels are assumed to be quasi-static Rayleigh fading, in which 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 Alice and Bobs follow the order of $|h_1|^2 \leq \cdots |h_m|^2 \leq \cdots |h_n|^2 \leq \cdots |h_M|^2$, where $|h_m|^2$ and $|h_n|^2$ are denoted as the ordered channel gain of the m-th user and the n-th user, respectively. Both the the small-scale fading and the path loss are contained in the ordered channel gain. It is considered that the m-th user (poor user) and the n-th user (good user) are paired to perform NOMA. The power allocation coefficients satisfy the conditions that $a_m \geq a_n$ and $a_m + a_n = 1$ by following the NOMA protocol. Successive interference cancelation (SIC) [13] is supposed to be carried out at the good one of the paired users. Based on the aforementioned assumptions, the instantaneous signal-to-interference-plus-noise ratio (SINR) for the m-th user and signal-to-plus-noise ratio (SNR) for the n-th user can be given by

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

and

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

respectively. We denote $\rho_b = \frac{P_A}{\sigma_b^2}$ as the transmit SNR, where P_A is the transmit power at Alice and σ_b^2 is the variance of additive white Gaussian noise (AWGN) at Bobs. In order to ensure that the m-th user can decode the message of the n-th user successfully, it is assumed that the condition of $a_m \geq \left(2^{R_m} - 1\right) a_n$ should be satisfied. In addition, a bounded path loss model is used to guarantee that the path loss keeps larger than one even for small distances.

For Eves, we consider the worst-case scenario of large-scale networks in which Eves are assumed to have strong detection abilities. Specifically, by applying multiuser detection technique, the multiuser data stream from Alice can be distinguished by Eves. In the considered case, the CSI is assumed to be available at Alice. Under this assumption, the most detrimental Eve is not the nearest one, but the one with the largest combined effect of small-scale fading and path-loss. Therefore, the instantaneous SNR for detecting the information of the m-th user and the n-th user at the most detrimental Eve can be expressed as follows:

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

It is assumed that $\kappa \in \{m, n\}$, $\rho_e = \frac{P_A}{\sigma_e^2}$ is the transmit SNR with σ_e^2 is the variance of AWGN at Eves. In addition, g_e is defined as the small-scale fading coefficient 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 Eves to Alice. In this paper, we assume that Eves can be detected if they are close enough to Alice. Therefore, a protect zone with radius r_p is introduced to keep Eves away from Alice.

III. New Channel Statistics

In this section, we derive several new channel statistics for Bobs and Eves, which will be used to derive the secrecy outage probability in the next section.

Theorem 1. Conditioned on the M randomly deployed NOMA users in the disc, the cumulative distribution function (CDF) of the n-th Bob $F_{\gamma_{B_n}}$ is given by

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

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

Proof: See Appendix A . ∎

Theorem 2. Conditioned on the M randomly deployed NOMA users in the disc, the CDF of the m-th Bob $F_{\gamma_{B_m}}$ is given in (5) on the top of next page, where $U\left(x\right)$ is the

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

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

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

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

To derive the CDF of $F_{\gamma_{B_m}}(x)$*,* Φ_m *can be expressed as*

$$\Phi_m=F_{|h_m|^2}\left(\frac{x}{(a_m-a_nx)\rho_b}\right). \tag{7}$$

Based on (A.5)*, interchanging the parameter* $m\to n$ *and applying* $y=\frac{x}{(a_m-a_nx)\rho_b}$*, we can obtain*

$$\Phi_m=\varphi_m\sum_{p=0}^{M-m}\binom{M-m}{p}\frac{(-1)^p}{m+p}\times \sum_{\tilde{S}_m^p}\binom{m+p}{q_0+\cdots+q_K}\left(\prod_{k=0}^{K}b_k^{q_k}\right)e^{-\sum\limits_{k=0}^{K}q_kc_k\frac{x}{(a_m-a_nx)\rho_b}}. \tag{8}$$

By substituting (8) *into* (6)*, with the help of the unit step function, the CDF of* $F_{\gamma_{B_m}}(x)$ *can be obtained. The proof is completed.* ■

Theorem 3. Conditioned on PPP and the protected zone with radius r_p, the probability density function (PDF) of the most detrimental Eve $f_{\gamma_{E_\kappa}}$ is given by

$$f_{\gamma_{E_\kappa}}(x)=\mu_{\kappa 1}e^{-\frac{\mu_{\kappa 1}\Gamma(\delta,\mu_{\kappa 2}x)}{x^\delta}}\left(\frac{\mu_{\kappa 2}^\delta e^{-\mu_{\kappa 2}x}}{x}+\frac{\delta\Gamma(\delta,\mu_{\kappa 2}x)}{x^{\delta+1}}\right), \tag{9}$$

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 need to compute the CDF of* $F_{\gamma_{E_\kappa}}$ *firstly as*

$$\begin{aligned}F_{\gamma_{E_\kappa}}(x)&=\{\gamma_{E_\kappa}\le x\}\\&=E_{\Phi_e}\left\{\prod_{e\in\Phi_e,d_e\ge r_p}\Pr\left\{|g_e|^2\le\frac{xd_e^\alpha}{\rho_e a_\kappa}\right\}\right\}\\&=E_{\Phi_e}\left\{\prod_{e\in\Phi_e,d_e\ge r_p}F_{|g_e|^2}\left(\frac{xd_e^\alpha}{\rho_e a_\kappa}\right)\right\}.\end{aligned} \tag{10}$$

By applying the generating functional given by [14], (10) *can be rewritten as*

$$\begin{aligned}F_{\gamma_{E_\kappa}}(x)&=\exp\left[-\lambda_e\int_{R^2}\left(1-F_{|g_e|^2}\left(\frac{xr_p^\alpha}{\rho_e a_\kappa}\right)\right)rdr\right]\\&=\exp\left[-2\pi\lambda_e\int_{r_p}^{\infty}re^{-\frac{x}{\rho_e a_\kappa}r^\alpha}dr\right].\end{aligned} \tag{11}$$

By applying [15, Eq. (3.381.9)], we can obtain

$$F_{\gamma_{E_\kappa}}(x)=e^{-\frac{\delta\pi\lambda_e(\rho_e a_\kappa)^\delta\Gamma\left(\delta,\frac{xr_p^\alpha}{\rho_e a_\kappa}\right)}{x^\delta}}. \tag{12}$$

By taking the derivative of $F_{\gamma_{E_\kappa}}(x)$ *in* (12)*, we can obtain the PDF of* γ_{E_κ} *in* (9)*. The proof is completed.* ■

IV. Secrecy Outage Probability

In this paper, the secrecy outage probability is used as a secrecy performance metric. Additionally, the secrecy rate of the m-th user and the n-th user can be expressed as

$$I_m=[\log_2(1+\gamma_{B_m})-\log_2(1+\gamma_{E_m})]^+, \tag{13}$$

and

$$I_n=[\log_2(1+\gamma_{B_n})-\log_2(1+\gamma_{E_n})]^+, \tag{14}$$

respectively, where $[x]^+=\max\{x,0\}$.

A. Exact Secrecy Outage Probability

Given the expected secrecy rate R_m and R_n for the m-th and n-th users, a secrecy outage is declared when the instantaneous secrecy rate drops below R_m and R_n, respectively. Based on (13), the secrecy outage probability for the m-th user is given by

$$\begin{aligned}P_m(R_m)&=\Pr\{I_m<R_m\}\\&=\int_0^\infty f_{\gamma_{E_m}}(x)F_{\gamma_{B_m}}\left(2^{R_m}(1+x)-1\right)dx.\end{aligned} \tag{15}$$

Based on the assumption of $a_m\ge\left(2^{R_m}-1\right)a_n$, we consider the secrecy outage probability under the condition that the connection between Alice and Bobs can be established. Substituting (5) and (9) into (15), after some mathematical manipulations, we can obtain the expression of secrecy outage probability of the m-th user as (16) on top of the next page, where $\tau_m=\frac{1}{2^{R_m}(1-a_m)}-1$.

Similarly, for the n-th user, based on (14), the secrecy outage probability is given by

$$\begin{aligned}P_n(R_n)&=\Pr\{I_n<R_n\}\\&=\int_0^\infty f_{\gamma_{E_n}}(x)F_{\gamma_{B_n}}\left(2^{R_n}(1+x)-1\right)dx.\end{aligned} \tag{17}$$

$$P_m = 1 - e^{-\frac{\mu_{m1}\Gamma(\delta,\tau_m\mu_{m2})}{\tau_m{}^{\delta}}} + \varphi_m \sum_{p=0}^{M-m} \binom{M-m}{p} \frac{(-1)^p}{m+p} \sum_{\tilde{S}_m^p} \binom{m+p}{q_0+\cdots+q_K} \left(\prod_{k=0}^{K} b_k^{q_k}\right) \times \int_0^{\tau_m} \mu_{m1} \left(\frac{\mu_{m2}^{\delta} e^{-\mu_{m2}x}}{x} + \frac{\delta\Gamma(\delta,\mu_{m2}x)}{x^{\delta+1}}\right) e^{-\frac{\mu_{m1}\Gamma(\delta,\mu_{m2}x)}{x^{\delta}} - \sum_{k=0}^{K} q_k c_k \frac{2^{R_m(1+x)-1}}{(a_m - a_n(2^{R_m}(1+x)-1))\rho_b}} dx. \quad (16)$$

$$P_n = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \sum_{\tilde{S}_n^p} \binom{n+p}{q_0+\cdots+q_K} \left(\prod_{K=0}^{K} b_k^{q_k}\right) \times \int_0^{\infty} \mu_{n1} \left(\frac{\mu_{n2}^{\delta} e^{-\mu_{n2}x}}{x} + \frac{\delta\Gamma(\delta,\mu_{n2}x)}{x^{\delta+1}}\right) e^{-\frac{\mu_{n1}\Gamma(\delta,\mu_{n2}x)}{x^{\delta}} - \sum_{k=0}^{K} q_k c_k \frac{2^{R_n(1+x)-1}}{\rho_b a_n}} dx. \quad (18)$$

Substituting (4) and (9) into (17), we can obtain the expression of secrecy outage probability of the n-th user as (18) on the second top of this page.

Based on (16) and (18), the secrecy outage probability for the selected user pair can be expressed as

$$P_{mn} = 1 - (1 - P_m)(1 - P_n). \quad (19)$$

B. Secrecy Diversity Order Analyses

In order to derive the secrecy diversity order to obtain more insights in the high SNR regime, a new analytical framework is introduced in the following from (20) to (29). As the worst-case scenario that Eves have strong abilities is considered, the asymptotic behavior is analyzed when the SNR of the channels between Alice and Bobs are sufficiently high, i.e., $\rho_b \to \infty$ and the SNR of the channels between Alice and Eves maintain arbitrary values[1]. Given $\rho_e \to \infty$, the probability of successful eavesdropping approaches one. The secrecy diversity order can be expressed as follows:

$$d_s = -\lim_{\rho_b \to \infty} \frac{\log P_{mn}^{\infty}}{\log \rho_b}. \quad (20)$$

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

$$F_{\left|\tilde{h}_n\right|^2}^{\infty}(y) \approx \frac{2y}{R_D^2} \int_0^{R_D} (1 + r^{\alpha}) r dr = y\ell, \quad (21)$$

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

Substituting (21) into (A.2), the asymptotic unordered CDF of $\left|\tilde{h}_n\right|^2$ is given by

$$F_{|h_n|^2}^{\infty}(y) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} (y\ell)^{n+p} \approx \frac{\varphi_n}{n} (y\ell)^n. \quad (22)$$

[1]In practical scenarios, Alice can generate jamming signals to Eves while the jamming signals can be canceled at Bobs. As such, the high SNR between Alice and Bobs can be guaranteed.

Based on (A.1), we can obtain

$$F_{\gamma_{B_n}}^{\infty}(x) = \varphi_n \sum_{p=0}^{M-n} \binom{M-n}{p} \frac{(-1)^p}{n+p} \left(\frac{x\ell}{\rho_b a_n}\right)^{n+p} \approx \frac{\varphi_n}{n} \left(\frac{x\ell}{\rho_b a_n}\right)^n. \quad (23)$$

Based on (7) and (22), we can obtain

$$\Phi_m^{\infty} = F_{|h_m|^2}^{\infty} \left(\frac{x}{(a_m - a_n x)\rho_b}\right) = \varphi_m \sum_{p=0}^{M-m} \binom{M-m}{p} \frac{(-1)^p}{m+p} \left(\frac{x\ell}{(a_m - a_n x)\rho_b}\right)^{m+p} \approx \frac{\varphi_m}{m} \left(\frac{x\ell}{(a_m - a_n x)\rho_b}\right)^m. \quad (24)$$

Substituting (24) into (6), the asymptotic CDF of γ_{B_m} can be expressed as

$$F_{\gamma_{B_m}}^{\infty}(x) = U\left(x - \frac{a_m}{a_n}\right) + U\left(\frac{a_m}{a_n} - x\right) \Phi_m^{\infty}, \quad (25)$$

where Φ_m^{∞} is given in (24).

Based on (17), we can replace the CDF of $F_{\gamma_{B_n}}$ with the asymptotic $F_{\gamma_{B_n}}^{\infty}$ in (23). After some manipulations, we can obtain the asymptotic secrecy outage probability of the n-th user as

$$P_n^{\infty}(R_n) = G_n(\rho_b)^{-D_n} + o\left(\rho_b^{-D_n}\right), \quad (26)$$

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

Similarly, based on (15), we can replace the CDF of $F_{\gamma_{B_m}}$ with the asymptotic $F_{\gamma_{B_m}}^{\infty}$ in (25). Additionally, we can obtain the asymptotic secrecy outage probability of the m-th user as

$$P_m^{\infty}(R_n) = G_m(\rho_b)^{-D_m} + o\left(\rho_b^{-D_m}\right), \quad (27)$$

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

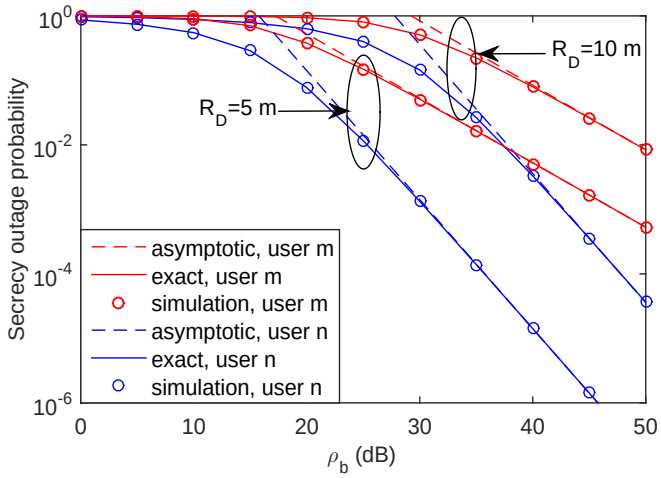

Fig. 2: The secrecy outage probability versus ρ_b, with $\rho_e = 10$ dB, $\alpha = 4$, $\lambda_e = 10^{-3}$, $M = 2$, $m = 1$, $n = 2$, and $r_p = 10$ m.

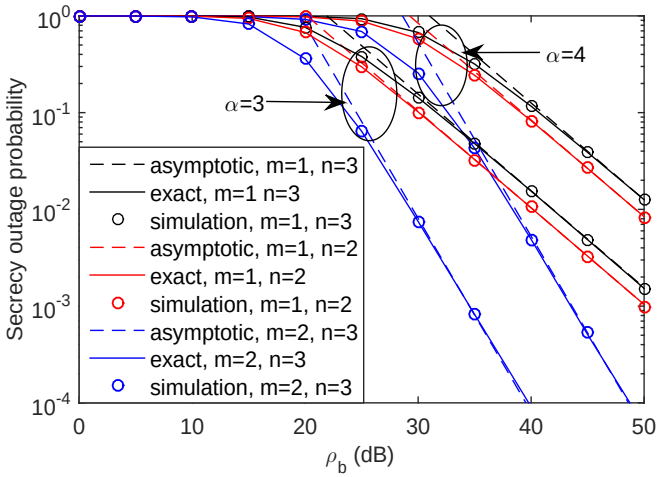

Fig. 3: The secrecy outage probability of user pair versus ρ_b, with $\rho_e = 10$ dB, $\lambda_e = 10^{-3}$, $R_D = 10$ m, $M = 3$, and $r_p = 10$ m.

Substituting (26) and (27) into (20), as $m < n$, the secrecy diversity order can be given by

$$d_s = -\lim_{\rho_b \to \infty} \frac{\log\left(P_m^\infty + P_n^\infty - P_m^\infty P_n^\infty\right)}{\log \rho_b} = m, \tag{28}$$

Substituting (26) and (27) into (19), the asymptotic secrecy outage probability for the user pair can be expressed as

$$\begin{aligned} P_{mn}^\infty =& P_m^\infty + P_n^\infty - P_m^\infty P_n^\infty \\ \approx& P_m^\infty G_m(\rho_b)^{-D_m}. \end{aligned} \tag{29}$$

Remark 1. *The derived results in* (28) *and* (29) *indicate that the secrecy diversity order and the asymptotic secrecy outage probability for the user pair are determined by the m-th user.*

The obtained remark provides insightful guideline to improve the secrecy performance of the considered networks with applying user pairing among M users. Since the secrecy outage probability of the user pair is determined by the poor one, it is efficient to pair the user with the best channel condition and the second best channel condition to achieve a larger secrecy diversity order.

V. Numerical Results

In this section, the numerical results are presented to facilitate the performance evaluations of considered large-scale networks. In this simulation, it is assumed that the power allocation coefficients of NOMA are $a_m = 0.6$, $a_n = 0.4$. The targeted data rates for the selected NOMA user pair are assumed to be the same $R_m = R_n = 0.1$ bit per channel use (BPCU).

Fig. 2 plots the secrecy outage probability of the single user (m-th and n-th) versus ρ_b with different ranges of user zone. In this case, the number of NOMA users is set as $M = 2$. The solid red and blue curves are for the exact analytical of the m-th user and n-th user, corresponding to the results derived in (16) and (18). The dash red and blue curves are for the asymptotic analytical of the m-th user and n-th user, corresponding to the results derived in (27) and (26). Monte Carlo simulations are used to verify our derivations. Fig. 2 shows the precise agreement between the simulation and analytical results. One observation is that the lower secrecy outage probability can be achieved by reducing the scope of the user zone, since smaller user zone leads to smaller path-loss. Another observation is that the n-th user has a larger slope than the m-the user. This is due to the fact that $m < n$ and the m-th user and n-th user achieves a secrecy diversity order of m and n respectively, which are demonstrated by the insights in (27) and (26).

Fig. 3 plots the secrecy outage probability of the selected user pair versus ρ_b with different path-loss factors. The number of NOMA users is set to be $M = 3$. The solid curves are the exact analytical results derived in (19). The dash curves are the asymptotic analytical results derived in (29). It can be observed that the red curves and the black curves have the same slopes. While the blue curves can achieve a larger secrecy outage slope, which is due to the fact that the secrecy diversity order of the user pair is determined by the poor one m. This phenomenon also consists with the obtained insights in **Remark 1**.

Fig. 4 plots the secrecy outage probability of the selected user pair versus r_p with different densities of the Eves. We can observe that the secrecy outage probability decreases as the radius of the protected zone increases, which demonstrates the benefits of the protected zone. It is also noted that another approach to enhance physical layer security is to reduce the scope of the user zone since it achieves the smaller path loss. It is also worth noting that smaller density λ_e of Eves can achieve better secrecy performance. This behavior is caused by the fact that smaller λ_e leads to less number of Eves, which lower the multiuser diversity gain when the most detrimental Eve is selected. As a result, the ability of the most detrimental Eve is lowered and the secrecy performance is improved.

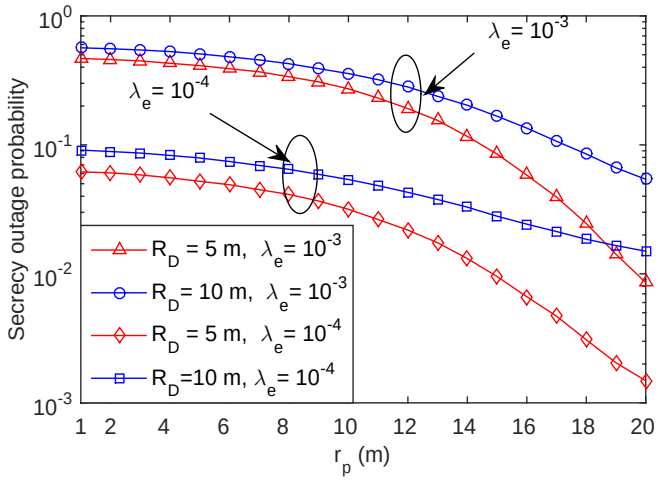

Fig. 4: The secrecy outage probability of user pair versus r_p, with $\rho_b = \rho_e = 50$ dB, $M = 2$, $m = 1$, $n = 2$, and $\alpha = 4$.

VI. Conclusions

In this paper, the secrecy performance of applying NOMA protocol in large-scale networks was examined. Specifically, stochastic geometry approaches were used to model the locations of NOMA users and eavesdroppers in the considered networks. In addition, new analytical expressions were derived in terms of the secrecy outage probability to determine the system secrecy performance. In addition, the secrecy diversity order of the user pair was also characterized. It was analytically demonstrated that the secrecy diversity order was determined by the poor one of the user pair. Meanwhile, the numerical results were presented to validate the analyses. Based on the analyses and simulations, it was concluded that enhancing the secrecy performance can be achieved by enlarging the scope of the protected zone or reducing the scope of the user zone.

Appendix A: Proof of Theorem 1

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

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

where $F_{|h_n|^2}$ is the CDF of ordered channel gain for the n-th user.

Assuming $y = \frac{x}{\rho_b a_n}$, using order statistics [16] and applying binary series expansion, the CDF of the ordered channels has a relationship with the unordered channels as follows:

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

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, by utilizing the polar coordinate, $F_{|\tilde{h}_n|^2}$ is expressed as

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

We notice that it is challenging to obtain an insightful expression for $F_{|\tilde{h}_n|^2}(y)$. Therefore, Gaussian-Chebyshev quadrature [17] is applied to find an approximation for (A.3) in the following:

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

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

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

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

References

[1] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *Proc. IEEE Annual Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, London, UK, Sept. 2013.

[2] 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.

[3] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, to be appear in 2014.

[4] 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.

[5] 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.

[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] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," 2015. [Online]. Available: http://arxiv.org/abs/1508.07433

[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] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[13] T. M. Cover and J. A. Thomas, "Elements of information theory 2nd edition," 2006.

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

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

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

[17] E. Hildebrand, "Introduction to numerical analysis," *NewYork, NY, USA: Dover,*, 1987.