On the Physical Layer Security of Millimeter Wave NOMA Networks

Shaocheng Huang, Ming Xiao, Senior Member, IEEE, and H. Vincent Poor, Fellow, IEEE

Abstract—For the capability of providing multi-giga BPS (bits per second) rates, millimeter wave (mmWave) communication is one of the key enabling technologies for the new and future generations of mobile communications, i.e., the fifth generation (5G) and beyond. Meanwhile, non-orthogonal multiple access (NOMA) can significantly increase the spectral efficiency by simultaneously serving multiple users in the same channel. Thus, mmWave NOMA networks have recently attracted considerable research attention. Meanwhile, a large number of confidential messages exchanged within highly interconnected systems has posed tremendous challenges on secure wireless communications, and thus in this article, we investigate the physical layer security of mmWave NOMA networks. Considering the limited scattering characteristics of mmWave channels and imperfect successive interference cancellation at receivers, we develop an analytic framework for the secrecy outage probability (SOP) for mmWave NOMA networks, in which legitimate users and eavesdroppers are randomly distributed. Based on the directional transmission property of mmWave signals, we propose a minimal angle-difference user pairing scheme to reduce the SOP of users. Considering the spatial correlation between the selected user pair and eavesdroppers, we develop two maximum ratio transmission (MRT) beamforming schemes to further enhance the secrecy performance of mmWave NOMA networks. Closed-form SOPs for the paired users with different eavesdropper detection capacities are derived. Numerical results show the effectiveness of our analysis and that there exists an optimal radius of network coverage ranges and transmit power to minimize the SOP of the user pair.

Index Terms—Millimeter wave, non-orthogonal multiple access, physical layer security, maximum ratio transmission, secrecy outage probability.

I. INTRODUCTION

With the development of various emerging applications (e.g., virtual reality, augmented reality, autonomous driving, and big data analytics), data traffic has explosively increased and caused growing demands for very high communication rates in new and future generations of mobile communications, i.e., the fifth generation (5G) and beyond [1]–[5]. For the capability of providing multi-giga BPS (bits per second) rates, millimeter wave (mmWave) communications has become one of the key enablers in the next generation mobile [1], [2], [6]. Despite the high data rates possible, mmWave communications suffers from severe path-loss and penetration loss. Thanks to the short wavelength of mmWave radio, large antenna arrays can be packed into mmWave transceivers with limited sizes for enhancing directional array gains [3]. With efficient beamforming techniques, highly directional transmission in mmWave can effectively overcome path-loss and mitigate interference, and thus improve system performance [4], [7].

When applying mmWave communications to mobile networks, multiple access strategies are critical for performance and complexity. If transmission resources (e.g., time/frequency/code) are limited, it will be challenging to support a large number of users in mobile networks with high rates and limited complexity [8]. Due to its benefits of low complexity and high performance, non-orthogonal multiple access (NOMA) has been proposed and has become one of the key potential enabling technologies for future mobile networks. NOMA-enabled base stations (BSs) can simultaneously serve multiple users in the same channel, and thus potentially increase the spectral efficiency and fairness of wireless networks [3], [9]. For instance, power domain NOMA employs superposition coding at the transmitter and successive interference cancellation (SIC) at receivers [10]. MmWave NOMA networks have recently attracted considerable research attention [3], [6], [8], [9], [11], [12]. To analyze the system performance of single-cell mmWave NOMA networks, an angle-dependent user pairing scheme was proposed in [9]. Furthermore, a distance-dependent user pairing scheme was proposed in [3] for multi-cell NOMA-based clustered mmWave networks. To reduce the system overhead and ensure two users are served simultaneously within a single BS beam, a random beamforming scheme was considered in [6], [11] and the coverage probability was investigated for extremely narrow beams. To achieve user separation in the power domain, effective channel gains of users are ranked based on the angle offset between the randomly generated BS beam and user locations in [11], while the gains are ranked based on user distance in [6]. From power allocation and beam design perspectives, a joint power and beamforming scheme was proposed in [8] to find the

Manuscript received April 27, 2020; revised July 11, 2020; accepted August 11, 2020. Date of publication August 17, 2020; date of current version October 22, 2020. The work of Ming Xiao was supported in part by the EU Marie Skłodowska-Curie Actions project entitled “High-reliability Low-latency Communications with network coding,” and ERA-NET Smart Energy Systems 5G+2017 Program, “SMART-MLA” with project number 89029 (and SWEA number 42811-2), and Swedish Strategic Research Foundation project “High-reliable and Limited Complexity User Pairing for mmWave Networks.” The work of H. Vincent Poor was supported in part by the U.S. National Science Foundation under Grant CCF-1908308. The review of this article was coordinated by Dr. S. Majji. (Corresponding author: Ming Xiao.) Shaocheng Huang and Ming Xiao are with the Division of Information Science and Engineering, KTH Royal Institute of Technology, Stockholm 10044, Sweden (e-mail: shahua@kth.se; mingx@kth.se). H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu). Digital Object Identifier 10.1109/TVT.2020.3017086
beamforming vector steering towards two users simultaneously subject to an analog beamforming structure.

Meanwhile, having large numbers of confidential messages exchanged within highly interconnected systems has posed tremendous challenges on secure wireless communications [13], [14]. Physical layer security, by exploiting the randomness of wireless channels without necessarily relying on secret keys, is a promising technique to improve the secrecy performance of wireless networks [13]. Particularly, multi-antenna techniques have been proposed as an efficient way to enhance physical layer security in wireless networks [4], [7]. By exploiting the degrees of freedom provided by multiple antennas, the transmitter can use beamforming to adjust its beam direction to maximize the received signal-to-noise ratio (SNR) (e.g., maximum ratio transmission (MRT) beamforming), or send artificial noise (AN) to jam potential eavesdroppers (EVEs) [15]. Compared to sub 6 GHz communications, mmWave has inbuilt advantages of enhancing physical layer security for the following reasons: (1) devices working in mmWave bands can support a larger number of antennas and thus support highly directional transmission; and (2) mmWave channels are of sparse, which can reduce signal leakage to malicious users [16]. For these reasons, physical layer security in mmWave communications has attracted considerable recent attention [4], [7], [14], [16]. Specifically, by using a sectored model to analyze the beam pattern, the average achievable secrecy rate in different mmWave bands was analyzed for AN-assisted mmWave ad hoc networks in [7], where it was shown that mmWave communications can further enhance secrecy performance relative to microwave. Furthermore, secrecy performance was analyzed for mmWave-overlaid mobile networks and a user associated scheme was proposed to determine which network (mmWave or microwave) a user should be associated to [14]. Considering both passive and active eavesdropping, several performance limits (in terms of distance, transmission power and beam-width, etc) of eavesdropping immunity in mmWave networks were studied in [4]. It was shown that mmWave networks with narrow beams exhibit inherent security and the existing physical layer security techniques have limited gains. With a more practical ray cluster channel model, secure multi-path mmWave communications were analyzed with two beamforming schemes, i.e., MRT beamforming and AN beamforming in [16]. With the benefit of high spectral efficiencies, secure NOMA has attracted considerable attention in the design and implementation of 5G mobile networks [17]–[19]. Considering the worst case where the EVE can always cancel inter-user interference, secrecy sum rates of the NOMA system were first investigated in [17]. The power allocation and the secrecy rate for the user with strong SNRs were examined in [18]. Furthermore, the secrecy rates and secrecy outage probability (SOP) for both NOMA assisted multicasting and unicasting were studied in [19]. It was shown that the secrecy rate with NOMA is no less than that with orthogonal multiple access (OMA) in high SNR regimes. In the above results, secrecy performance was analyzed under the assumption that perfect SIC is always achieved at the user with the strong SNR.

Based on the above observations, it is of interest to study the physical layer security of mmWave NOMA networks. Different from the traditional wireless channels with rich scattering, mmWave channels have limited angular coverage, which leads to highly directional transmission. To the best of our knowledge, there are no existing results investigating the secure transmission schemes and secrecy performance of mmWave NOMA networks considering the limited scattering characteristics of mmWave propagation and highly directional transmission. In what follows, we will investigate the physical layer security of NOMA mmWave networks, in which users and EVEs are randomly located. To capture the multi-path characteristics of mmWave signals, a discrete angular domain channel model will be used for theoretical analysis. The main contributions of this paper can be summarized as follows:

1) Based on the directional transmission characteristics of mmWave signals, we propose a minimal angle-difference (MA) user pairing scheme to support secure NOMA transmission, which can significantly reduce signal leakage to EVEs in the angular domain. Relaxing the assumption of perfect SIC at receivers as in [10], [17], [18], we investigate the more practical NOMA scheme with imperfect SIC. To measure the channel correlation between the selected user pair and the EVEs from a stochastic geometric framework, we derive the probability mass function (PMF) of the number of common resolvable paths between the selected user pair and the EVEs for theoretical analysis.

2) Based on the spatial correlation between the selected user pair and the EVEs, we develop two secrecy beamforming schemes with the aid of MRT for further enhancing the secrecy performance of NOMA mmWave networks, namely, NMRT beamforming (near-user based MRT beamforming) and CMRT beamforming (common-path based MRT beamforming). For both beamforming schemes, we first derive exact analytical expressions for the channel statistics (i.e., the distributions of common resolvable paths and signal-to-noise-plus-interference ratio (SINR)) for paired users and EVEs. To analyze the impact of non-colluding EVEs with different detection capacities, we then provide closed-form expressions for the SOP for the paired users.

3) Numerical results from simulations show the effectiveness of our analysis. Results also show that: (a) The proposed MA user pairing scheme can achieve better secrecy performance than that with randomly selected user pairing; (b) There exist an optimal radius of network coverage range, and number of resolvable paths and transmit power to minimize the system SOP of the user pair; (c) NMRT beamforming can significantly improve the security of the near user, while CMRT beamforming can achieve a smaller system SOP of the user pair; and (d) Compared with conventional OMA, NOMA with CMRT beamforming can achieve better secrecy performance in low to medium transmit power regimes.

The rest of the paper is organized as follows. The system model is given in Section II. The beamforming schemes for mmWave NOMA networks are proposed in Section III. The secrecy performance analysis of mmWave NOMA networks with NMRT and CMRT beamforming is given in Section IV and V, respectively. Numerical results are given and discussed in Section VI and we state our conclusions in Section VII.
Note: Bold uppercase (lowercase) letters denote matrices (vectors). $E_{p}[\cdot]$ represents the expectation over $x$. $||\cdot||$, $(\cdot)^T$ and $(\cdot)^H$ denote absolute value, Euclidean norm, conjugate, transpose and conjugate transpose, respectively. $\lfloor x \rfloor = \text{floor}(x)$ and $\lceil x \rceil = \text{ceil}(x)$ and $1(\cdot)$ is the indicator function.

II. SYSTEM MODEL

A. Network Model

We consider a secure downlink in an mmWave NOMA network, which consists of one BS and multiple users and EVEs. It is assumed that the BS is located at the center of a disc, denoted by $\mathcal{D}$, which has a radius of $R$. The users are randomly located in $\mathcal{D}$ following a homogeneous Poisson point process (PPP). We further assume that EVEs are randomly located according to a homogeneous PPP $\Psi_e$ with density $\lambda$, on an infinite two-dimensional plane. For tractable analysis, we assume that the BS is equipped with $N_t$ antennas, user and each EVE is equipped with a single antenna.

With limited scattering, mmWave channels can be described by a geometric channel model, which is assumed to be the sum of the channel gains of $N_p$ paths [20], [21]

$$h = \sqrt{\frac{N_t}{P_L(r) \sum_{l=1}^{N_p}}} g_l a(\Theta_l)^H,$$  

(1)

where $r$ is the distance between the BS and the receiver, $P_L(r)$ is average path-loss, $g_l$ is the complex gain of the $l$-th path, $a(\Theta_l)$ is the normalized array steering vector at the azimuth angle of departure (AOD) $\theta_l$, and $\Theta_l = \sin(\theta_l)$. When an uniform linear array (ULA) is adopted at the BS, the normalized array steering vector can be expressed as

$$a(\Theta) = \frac{1}{\sqrt{N_t}} [e^{-j\frac{2\pi}{\lambda} d \sin(\Theta)}, e^{-j\frac{2\pi}{\lambda} 2d \sin(\Theta)}, \ldots, e^{-j(N_t-1)\frac{2\pi}{\lambda} d \sin(\Theta)}]^T,$$  

(2)

where $\lambda$ is wavelength and $d = \frac{\lambda}{2}$ is antenna spacing.

In following analysis, we consider the discrete angular domain representation of the mmWave channel in (1) as [16], [22]. Let $E = \frac{dN_t}{\lambda}$ denote the normalized length of the transmitting antenna. As shown in [23], the transmitting signals with direction difference less than $\frac{\pi}{2}$ are not resolvable. Hence, the angular domain can be sampled at a fixed space of $\frac{\pi}{2}$, and represented by the spatially orthogonal basis $\mathbf{U}$ defined as $\mathbf{U} = \{a(\Psi_1), a(\Psi_2), \ldots, a(\Psi_{N_t})\}$, where $\Psi_i = \frac{\lambda}{\lambda} (i - 1 - N_t) \arcsin(\sin(\theta_l))$ for $i = 1, 2, \ldots, N_t$. Basis $\mathbf{U}$ provides the representation of transmitting signals in the angular domain. It was shown that the signal along any physical direction (i.e., $\Psi_i$) has almost all its energy by particular vector $a(\Psi_i)$ and very little in other directions [23]. Thus, all paths with the transmitting direction (i.e., $\Theta_l$) within a window of width $\frac{\pi}{2}$ around $\Psi_l$ can be approximatively aggregated into one resolvable path. Then, the mmWave channel (1) in the discrete angular domain can be described as [16]

$$h = \sqrt{\frac{N_t}{P_L(r)}} \sum_{l=1}^{N_p} g_l a(\Psi_l)^H,$$  

(3)

where $g = [g_1, g_2, \ldots, g_{N_t}]$ is the complex gain vector of the resolvable paths, $L$ is the number of spatially resolvable paths. We assume that the AOD of all paths is distributed in an angular range $[\theta_{min}, \theta_{max}] \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Then, we have $L = \frac{E\sin(\theta_{max}) + N_{\text{t}} + 1}{E\sin(\theta_{min}) + N_{\text{t}} + 1} + 1$. Due to the sparse scattering feature of mmWave channels, we have $L < N_t$ [24]. Since each resolvable path contains an aggregation of individual physical paths, letting $g_l \sim \text{CN}(0, 1)$ for all $l$ with $\Psi_l \in [\sin(\theta_{min}), \sin(\theta_{max})]$ [16], [22], [24]; otherwise, $g_l = 0$. We further assume that the complex gain vectors for different users are independent [16].

With $\Psi_i$, we can obtain the angle of the $i$-th resolvable path denoted by $\theta_l = \arcsin(\Psi_l)$. Letting $\bar{\Psi}_l = [-\frac{\pi}{2}, \theta_1, \theta_2, \ldots, \theta_{N_t}, \frac{\pi}{2}]$, we then can calculate user position boundaries in the angular domain as $\varphi_l = \frac{\theta_l + \bar{\varphi}_l}{2}$ for $l = \frac{N_t - L}{2} + 1, \frac{N_t - L}{2} + 2, \ldots, N_t - L + 2$ and $\varphi_l = -\varphi_{N_t - L + 3} - i$ for $i = 1, 2, \ldots, N_t - L + 2$. For example, as shown in Fig. 1(a), if the user with $L = 3$ is located in the angular range $[\varphi_{11}, \varphi_{12}]$, the user has three resolvable paths corresponding to directions $\{\Psi_{11}, \Psi_{12}, \Psi_{13}\}$. In order to ensure that the number of resolvable paths equals to constants, we only consider the users located in the angular range $[\varphi_{11}, \varphi_{12}, \varphi_{N_t - L + 2}]$ for downlink transmission. Letting $\mathcal{D}$ denote the area with the angular range $[\varphi_{11}, \varphi_{12}, \varphi_{N_t - L + 2}]$ in $\mathcal{D}$, it is clear that the users located in $\mathcal{D}$ still follow a homogeneous PPP $\Psi_e$ [25]. We consider the downlink transmission with dense user deployment and the number of users located in $\mathcal{D}$ is $K \geq 2$. The number of resolvable paths for every user is the same and denoted as $L$, and the $k$-th user ($k \in \{0, 1, \ldots, K - 1\}$) is located at the center of its angular range $[\theta_{k, min}, \theta_{k, max}]$. Meanwhile, for $K_e$ EVEs in $\mathcal{D}$, we assume that EVEs and users have similar computing and receiving capability. Hence the number of resolvable paths for the $e$-th user is $L_e = L_e \in \{0, 1, \ldots, K_e - 1\}$. Since mmWave signals are vulnerable to blockage, line-of-sight (LOS) and none-line-of-sight (NLOS) pathloss characteristics should be taken into account [1]. Based on the experiment results in [26], the pathloss is defined as $P_L(r) = \beta r^{-\alpha}$, where $\beta$ is a frequency-dependent constant, $\alpha$ is the pathloss exponent. For mmWave channels with LOS paths, the contribution of NLOS paths is marginal since the pathloss of NLOS components is much larger than that of the LOS component [6], [11]. Hence, we assume that the channel in (2) only contains LOS paths, and the contribution of NLOS paths is ignored for tractable analysis.

B. Secure mmWave NOMA Communications

We consider multiple pairs of users for downlink communication, in which each paired users are served by the BS with NOMA techniques in each time-frequency block [10], [27], [28]. Beamforming is used to provide directional transmission. In each resource block, one beam serves two paired users if there are common resolvable paths between them. In what follows, we shall propose an angle-based user pairing scheme to reduce the overhearing of EVEs. Let the angle of the $k$-th user $U_k$ with respect to the BS be $\theta(U_k)$ for $k = 0, 1, \ldots, K - 1$, depicted in Fig. 1(a). To ensure fairness for all users in $\mathcal{D}$, a typical user, denoted by $U_0$, is randomly selected by the BS. We assume that $U_0$ is located in angular range $[\varphi_1, \varphi_{12}]$.
for $i = 1, 2, \ldots, N_t - L + 1$ with the center angle denoted by $\theta^i_0 = \frac{\bar{\phi}^i_0 + \bar{\phi}^{i+1}_0}{2}$. The paired NOMA user of $U_0$, denoted by $U_p$, can be selected according to the following minimal angle-difference (MA) scheme

$$U_p = \arg \min_{U_k \in \Phi_u \setminus \{U_0\}} |\theta^i_0 - \theta(U_k)|.$$  \hspace{1cm} (4)

The proposed MA user pairing scheme in (4) selects the paired NOMA user of $U_0$, which has the minimal angle difference to the center angle of $U_0$. With the proposed MA user pairing scheme, we can increase the probability that paired users share the same spatially resolvable paths. Particularly, when users are densely deployed in networks, the probability that paired users are located in the same beam is very high. Compared to the distance-based user pairing scheme [6], [29], the proposed angle-based user pairing scheme can ensure that almost all transmission energy in a particular direction for the paired users, and hence reduce the overhearing of EVEs.

If the NOMA pair users are located in the same beam direction, a common decoding procedure is that the user with a better condition first decodes the signals of other users [10]. As shown in [30], small-scale fading shows little change in received power when highly directional antennas are used. Thus, we assume that the decoding order of mmWave NOMA schemes mainly depends on large-scale fading, i.e., the signal intended to the one far from the BS is decoded first [3]. Thus, the near user first decodes the signal intended for the far user and then applies SIC to remove interference and decodes its own information.

### C. Performance Metrics

In what follows, we consider a practical scenario, in which randomly distributed EVEs are non-colluding [10], [16], [28]. In this scenario, each EVE individually decodes confidential messages and the SINR of detecting the message intended for user $u$, $u \in \{n, f\}$, at the most detrimental EVE can be expressed as $\zeta_{E,u} = \max_{c \in \Phi_e} \zeta_{c,u}$, where $n$ and $f$ denote the near user and far user, respectively, and $\zeta_{c,u}$ is the SINR of detecting the message intended for user $u$ at the $c$-th EVE. With imperfect SIC at the near user, the secrecy rate for the near user $R_{n,u}$ is defined as [28]

$$R_{n,u} = \mathbb{E}(\zeta_{f \rightarrow n} \geq \zeta^*_{f \rightarrow n}) \log(1 + \zeta_{n}) - \log(1 + \zeta_{E,n})^+,$$  \hspace{1cm} (5)

where $[x]^+ = \max\{0, x\}$. $\zeta_{f \rightarrow n}$ is the SINR of the message intended for the far user observed at the near user, $\zeta_{n}$ is the SINR of the near user, $\zeta^*_{f \rightarrow n} = e^{\mathcal{R}_f} - 1$ and $\mathcal{R}_f$ is the target code rate for the message intended for the far user. Additionally, the secrecy rate of the far user is defined as

$$R_{f,u} = \mathbb{E}(1 + \zeta_{f}) - \log(1 + \zeta_{E,f})^+,$$  \hspace{1cm} (6)

where $\zeta_{f}$ is the SINR of the far user detecting its own message.

Secrecy outage probability: a secrecy outage event occurs at user $u$, $\forall u$, if the secrecy rate falls below a given target secrecy rate $\mathcal{R}^*_{u}$, $\forall u$. Thus, the SOP for user $u$ is defined as

$$\mathcal{P}_u = \text{Pr}\{R_{u,s} < \mathcal{R}^*_{u} \}. \hspace{1cm} (7)$$

For simplifying exposition, we define set $\Omega_{c} = \{I_{c,i} \mid I_{c,i} \in \mathbb{Z}_+^3, I_{c,i} \in [1, N_t], I_{c,i} = I_{c,1} < \cdots < I_{c,L_c} \}$, $c \in \{n, f\}$, corresponding to the indexes of the spatially resolvable paths of receiver $c$. We also define $\Omega = \{1, 2, \ldots, N_t\}$. As shown in Fig. 1(b), the spatially resolvable paths of each receiver $c$ consist of two types of paths: private paths and common paths. Then we define $\Omega_{p_c}$ as an index set of the private resolvable paths of receiver $c$. Similarly, $\Omega_{c_{n,f}}, \Omega_{c_{e,f}}$, and $\Omega_{c_{e,f}}$ denote the index sets of common resolvable paths between the paired receivers $\{n, f\}$, $\{n, e\}$, and $\{e, f\}$, respectively. We define a function $\mathcal{W}(M, \Omega_u)$ to generate a matrix with columns selected from $M$ based on the selected column index set $\Omega_u$. Let $g_{c,u} = \mathcal{W}(g_c, \Omega_u)$, $c \in \{n, f\}$ and $\forall u \in \{p_n, p_f, p_e, c_{n,f}, c_{e,f}, c_{e,f}\}$.

### III. Beamforming Schemes for Secure MMwave NOMA Networks

MRT beamforming is an effective approach to enhance the legitimate user channels [16]. Based on the spatial correlation of the selected user pair and EVEs, we develop two MRT beamforming schemes to enhance the secrecy performance of mmWave NOMA networks, i.e., NMRT beamforming.
(near-user based MRT beamforming) and CMRT beamforming (common-path based MRT beamforming).

A. NMRT Beamforming

We consider the scenarios of one beam serving the paired users. Since the performance of NOMA networks is severely impacted by inter-user interference and unsuccessful SIC [28], [31], the NMRT beamforming scheme is designed according to the CSI of the near user to improve the probability of canceling interference at the near user. Specifically, we design the beam for the information-bearing signal as $w_{N} = h_{u}^{H} \|h_{u}^{N}\| \in \mathbb{C}^{N_{c} \times 1}$, where $h_{u}$ is the channel between the BS and the near user. With this scheme, the BS tries to align the direction of the beam with the AOD of the near user. Then, the transmitted superposed signal vector at the BS is $x_{t}^{N} = w_{N}(\sqrt{a_{u}P} s_{u} + \sqrt{a_{f}P} s_{f})$, where $P_{t}$ is the sum transmitting power, $s_{u}$ and $a_{u}$ for $u \in \{n, f\}$ are the information-bearing signal and the power allocation coefficient intended for user $u$, respectively, with $\mathbb{E} \|s_{u}\|^{2} = 1$ and $a_{n} + a_{f} = 1$. The received signal at user $u$ can be expressed as $y_{u}^{N} = h_{u}w_{N}(\sqrt{a_{u}P} s_{n} + \sqrt{a_{f}P} s_{f}) + \omega_{u}$, where $\omega_{u}$ denotes additive Gaussian noise with a distribution $\omega_{u} \sim \mathcal{CN}(0, \sigma^{2})$. According to the NOMA decoding approach, the near user first tries to decode the information-bearing signal $s_{f}$ with SINR

$$\zeta_{s_{f} \rightarrow n}^{N} = \frac{a_{f}P_{t}}{a_{u}P_{t} + 1} \|h_{u}w_{N}\|^{2} \|h_{u}w_{N}\|^{2}$$

(8)

where $P_{t} = \frac{P}{2}$ is the transmitting SNR. If the near user can successfully decode the signal $s_{f}$, the near user applies SIC to subtract $s_{f}$ and then decodes its own signal with SINR

$$\zeta_{s_{u} \rightarrow n}^{N} = a_{n}P_{t} \|h_{u}w_{N}\|^{2}.$$  

(9)

Otherwise, the near user cannot use SIC and decode its own signal [9]. On the other hand, by treating $s_{n}$ as interference, the far user decodes its own signal $s_{f}$ with SINR

$$\zeta_{s_{f} \rightarrow u}^{N} = \frac{a_{f}P_{t}}{a_{u}P_{t} + 1} \|h_{u}w_{N}\|^{2} \|h_{u}w_{N}\|^{2}.$$  

(10)

The signal observed at the $e$-th EVE is given by $y_{e}^{N} = h_{e}w_{N}(\sqrt{a_{u}P} s_{u} + \sqrt{a_{f}P} s_{f}) + \omega_{e}$, where $\omega_{e}$ denotes additive Gaussian noise with a distribution $\omega_{e} \sim \mathcal{CN}(0, \sigma^{2})$. According to the detection capacity of EVEs, we consider the following two cases:

Case I: Assuming the detection capacity of EVEs is not strong enough to distinguish the individual signal from users and subtract inter-user interference generated by the superposed information-bearing signals from each other. Thus, the SINR of the most detrimental EVE to decode $s_{u}, \forall u$, is

$$\zeta_{E_{1}, u}^{N} = \max_{e \in \Phi_{e}} \frac{a_{u}P_{t} \|h_{u}w_{N}\|^{2}}{(1 - a_{u})P_{t} \|h_{u}w_{N}\|^{2} + 1} + 1.$$  

(11)

Case II: Assuming EVEs have strong enough detection capacity. Hence, they can unambiguously distinguish the individual signal and subtract inter-user interference from each other [28]. Thus, the SINR of the most detrimental EVE to decode $s_{u}, \forall u$, is

$$\zeta_{E_{1}, u}^{N} = \max_{e \in \Phi_{e}} \frac{a_{u}P_{t} \|h_{u}w_{C}\|^{2}}{(1 - a_{u})P_{t} \|h_{u}w_{C}\|^{2} + 1} + 1.$$  

(12)

B. CMRT Beamforming

Since NMRT beamforming can align transmitting beams in all resolvable paths of the near user, it can enhance the signal strengths of both $s_{n}$ and $s_{f}$ at the near user. However, NMRT beamforming may cause more interference and thus lead to degraded reception quality to the far user. To address this issue, we consider the number of common resolvable paths between the paired users, the confidentiality of the far user cannot be guaranteed if $L_{c} = 0$. We then propose CMRT beamforming, by which the beamforming vector for the information-bearing signal is designed according to $L_{c}$. Specifically, if $L_{c} \neq 0$, we design the beamforming vector for the information-bearing signal as $w_{C} = (g_{n,c_{n}}U_{c}^{H}) / \|g_{n,c_{n}}U_{c}^{H}\| \in \mathbb{C}^{N_{c} \times 1}$ where $g_{n,c_{n}} = \mathcal{W}(g_{n}, \Omega_{c_{n}}), U_{c} = \mathcal{W}(U, \Omega_{c_{n}})$. If $L_{c} = 0$, OMA is used to serve different users in different time-frequency blocks. Compared to the NMRT scheme, the CMRT scheme can guarantee the fairness of users and the transmitting beam is narrower, which can potentially protect against information leakage. Then similar to NMRT beamforming, the near user first tries to decode signal $s_{f}$ with SINR

$$\zeta_{s_{f} \rightarrow n}^{C} = \max_{e \in \Phi_{e}} \frac{a_{f}P_{t} \|h_{u}w_{C}\|^{2}}{a_{u}P_{t} \|h_{u}w_{C}\|^{2} + 1}.$$  

(13)

If the near user can successfully decode signal $s_{f}$, it decodes its own signal at following SNR

$$\zeta_{s_{u} \rightarrow n}^{C} = \frac{a_{n}P_{t} \|h_{u}w_{C}\|^{2}}{a_{f}P_{t} \|h_{u}w_{C}\|^{2} + 1}.$$  

(14)

where $w_{n} = w_{N}$. The far user decodes its own signal $s_{f}$ at following SINR

$$\zeta_{s_{f} \rightarrow u}^{C} = \frac{a_{f}P_{t} \|h_{f}w_{C}\|^{2}}{a_{u}P_{t} \|h_{f}w_{C}\|^{2} + 1} + 1.$$  

(15)

where $h_{f}^{H} / \|h_{f}^{H}\|$. Considering the EVEs in Case I, the SINR of the most detrimental EVE to decode $s_{u}, \forall u$, is

$$\zeta_{E_{1}, u}^{C} = \frac{a_{u}P_{t} \|h_{u}w_{C}\|^{2}}{(1 - a_{u})P_{t} \|h_{u}w_{C}\|^{2} + 1}.$$  

(16)

Similarly, considering the EVEs in Case II, the SINR of the most detrimental EVE to decode $s_{u}, \forall u$, is

$$\zeta_{E_{1}, u}^{C} = \frac{a_{u}P_{t} \|h_{u}w_{C}\|^{2}}{(1 - a_{u})P_{t} \|h_{u}w_{C}\|^{2} + 1} + 1.$$  

(17)
IV. Secrecy Performance Analysis With NMRT Beamforming

In this section, we will analyze the secrecy performance of mmWave NOMA networks with NMRT beamforming. The analysis of CMRT will be given in the next section. We will first derive the channel statistics, i.e., the distribution of common resolvable paths and the SINR distributions of the paired users and EVEs. Then, we will give the analytical expressions of the SOP for both paired users.

A. Channel Statistics

In order to measure the channel correlation between paired users, we need to obtain the number of common resolvable paths between paired users, i.e., \( L_c \). With stochastic geometry, it is hard to find the exact value of \( L_c \) due to the randomness of the selected paired users. Instead, we give the PMF of \( L_c \) in the following lemma.

Lemma 1: Based on the MA user pairing scheme in (4), the PMF of \( L_c \) is

\[
P_u(L_c) = \begin{cases} 
\sum_{i=1}^{N_r-L+1} \Pr(\epsilon_i) F^{\Delta_{u,p}}(\varphi_{i+1} - \theta^0_0), & \text{if } L_c = L, \\
\sum_{i=1}^{N_r-L+1} \Pr(\epsilon_i) (F_U(i) + F_D(i)) + \Pr(\tilde{N}) F_U(\tilde{N}), & \text{if } L_c = 1, \ldots, L-1, \\
1 - \sum_{i=1}^L P_u(l), & \text{if } L_c = 0, 
\end{cases}
\]

(18)

where \( \Pr(\epsilon_i) = \frac{\varphi_{i+1} - \varphi_i}{2}, \Delta \varphi = \varphi_{N_r-L-2} - \varphi_1, \theta^0_0 = \frac{\varphi_{i+1} - \varphi_i}{2}, \tilde{N} = \frac{N_r-L+2}{2}, F^{\Delta_{u,p}}(\Delta) = 1 - (1 - \frac{\Delta}{\Delta_\varphi})^{-1}, F_U(i) \) and \( F_D(i) \) are given in (19), shown at the bottom of this page.

Proof: See Appendix A. ■

Remark 1: As \( L \rightarrow \infty \), \( F^{\Delta_{u,p}}(\Delta) = 1 \) and thus \( P_u(L_c = L) = 1 \). This implies that when the number of users in \( D \) is sufficiently large, based on the MA user pairing scheme, the paired user is always selected with the same resolvable paths as the typical user.

The common resolvable paths of the paired users only describe the channel statistics in the angular domain. For our NOMA scheme in II-B, we need to determine which of the paired users \( (U_0 \) and \( U_p ) \) is the near user form the BS in the distance domain. Denote \( r_n \) and \( r_f \) the distance of the near user and the far user from the BS, respectively. The following lemma gives the probability density function (PDF) of the distance of the near user and the far user from the BS.

Lemma 2: For two users \( U_0 \) and \( U_p \) in \( D \), the PDFs of the distance of the near and the far user from the BS are respectively given by

\[
f_{r_n}(r) = \frac{4r(R^2 - r^2)}{R^4} I(0 \leq r \leq R),
\]

(20)

\[
f_{r_f}(r) = \frac{4r^3}{R^4} I(0 \leq r \leq R).
\]

(21)

Proof: See Appendix B. ■

Since users and EVEs are located according to different homogeneous PPPs, the spatial locations of the selected user pair and EVEs are independent. Furthermore, from the proposed NMRT beamforming scheme, we know that the SINR of the most detrimental EVE is not related to the far user. Thus, we only need to find channel correlation between the near user and the EVEs, which can be measured by the number of resolvable common paths between the near user and the EVEs. Let \( L_c^e \) denote the number of common resolvable paths between the near user and the \( e \)-th EVE. The following lemma presents the distribution of \( L_c^e \).

Lemma 3: The PMF of \( L_c^e \) is

\[
P_e(L_c^e) = \begin{cases} 
\sum_{i=1}^{N_r-L+1} \Pr(\epsilon_n^e) F^{\Delta_{u,p}}(\varphi_{i+1}, \varphi_i), & \text{if } L_c^e = L, \\
\sum_{i=1}^{N_r-L+1} \Pr(\epsilon_n^e) F_e(L_c^e, i), & \text{if } L_c^e = 1, 2, \ldots, L-1, \\
1 - \sum_{i=1}^L P_e(l), & \text{if } L_c^e = 0, 
\end{cases}
\]

(22)

where \( \Pr(\epsilon_n^e) = \frac{\varphi_{i+1} - \varphi_i}{\Delta_\varphi}, F_e(L_c^e, A, B) = \frac{|B - A|}{\Delta_\varphi} \), \( F_e(L_c^e, i) \) is given in (23), shown at the bottom of this page.

Proof: The proof is similar to Lemma 1, but with the different conditional PDF \( F_e^{\Delta_{u,p}}(A, B) \), \( F_e(L_c^e, i) \) is given in (23).

Based on the distributions of \( L_c, L_c^e, r_n \) and \( r_f \), we can find the distributions of \( \zeta_n^N \) and \( \zeta_{B,c}^N \), presented in following lemmas.

Lemma 4: The CDF of \( \zeta_n^N \) in (9) is

\[
F_{\zeta_n^N}(x) = 1 + \sum_{i=0}^{L-1} \frac{4}{\alpha \Gamma(l+1) R^4} \left( \Xi_n^{-\frac{\zeta}{\alpha}} \gamma(\frac{x}{\Xi_n R^\alpha}) - R^2 \Xi_n^{-\frac{\zeta}{\alpha}} \gamma(\frac{2}{\alpha}, \Xi_n R^\alpha) \right),
\]

(24)

Based on the parameter settings shown in Table 1, we have

\[
F_c(L_c^e, i) = 1(i \leq N_t - 2L + L_c^e + 1)F^{\Delta_{u,p}}_c(\varphi_{i+L-L_c^e, \varphi_{i+L-L_c^e}+1}) + 1(i \geq L - L_c^e + 1)F^{\Delta_{u,p}}_c(\varphi_{i+L-L_c^e, \varphi_{i+L-L_c^e}+1})
\]

(23)
where $\Xi_n = \frac{L \alpha_n r_n}{\alpha \rho_n^2}$, $\Gamma(\cdot)$ is the gamma function, $\gamma(\cdot, \cdot)$ is the lower incomplete gamma function.

Proof: With $h_n = \sqrt{\frac{\beta N_c}{\sigma^2}} g_n U^H$, $\zeta_n^N$ in (9) can be expressed as

$$\zeta_n^N = \frac{a_n \rho_n \beta N_c r_n^{-\alpha}}{L} \left\| g_n U^H \right\|^2 = \frac{a_n \rho_n \beta N_c \nu r_n^{-\alpha}}{L}, \quad (25)$$

where $\nu = \left\| g_n U^H \right\|^2 \sim \text{Gamma}(L, 1)$. Then, the CDF of $\zeta_n^N$ is

$$F_{\zeta_n}^N(x) = \int_0^x f_{\zeta_n}(r_n) \Pr\{r_n < \Xi_n r_n^{\alpha}\} dr_n$$

$$= \int_0^x 4r_n(R^2 - r_n^2) \left( 1 - \sum_{l=0}^{L-1} \left( \Xi_n r_n^{\alpha} \right)^l e^{-\Xi_n r_n^{\alpha}} \Gamma(l+1, \frac{x}{\Xi_n r_n^{\alpha}}) \right) dr_n,$$

where (a) follows from the PDF of $r_n$ in Lemma 2, and the CDF of gamma distribution. By applying (3.381.8) in [32], $F_{\zeta_n}^N(x)$ in (24) can be obtained.

Lemma 5: The CDF of $\zeta_f^N$ in (10) is

$$F_{\zeta_f}^N(x) = 1 \left( x \geq \vartheta_f \right) + 1 \left( x < \vartheta_f \right) (1 - F_f^N(x)), \quad (27)$$

where $F_f^N(x)$ is given in (28), shown at the bottom of this page, $\vartheta_f = \frac{a_f}{\alpha_f}$, $\Xi_f = \frac{a_f \beta N_c \nu}{\alpha_f - \alpha_a}$. $B(\cdot, \cdot)$ is the beta function, $G_{p,q}^m[\frac{\alpha}{b_1} \ldots \frac{\alpha}{b_q}]$ is Meijer’s G-function.

Proof: See Appendix C.

According to the detection capacity of EVEs, we first derive the SINR distribution of the most detrimental EVE in Case I, which is shown in the following lemma.

Lemma 6: The CDF and PDF of $\zeta_{E_1,u}^N$ in (11) are respectively given by

$$F_{\zeta_{E_1,u}^N}(x) = 1 \left( x \geq \vartheta_u \right) + 1 \left( x < \vartheta_u \right) e^{-\Xi u Q_1^f},$$

$$f_{\zeta_{E_1,u}^N}(x) = 1 \left( x < \vartheta_u \right) 2\alpha_u e^{-\Xi u Q_1^f} \Xi u Q_1^f,$$ (29)

where

$$\vartheta_u = \frac{a_u}{(1-a_u)}, \quad \Xi_u = \rho_u \Delta (\frac{a_u \beta N_c u}{L}) \frac{\nu}{\alpha - \alpha_u} (P_u (L) + \sum_{l=1}^{L-1} P_l (L_e)),$$

and $Q_1 = \frac{e^{-\Xi u Q_1^f}}{a_u (1-a_u)}$.

Proof: See Appendix D.

Remark 2: The CDF of $\zeta_{E_1,u}^N, \forall u$, denoted by $F_{\zeta_{E_1,u}^N}(x)$, can be obtained by relaxing the indicator conditions and replacing $Q_1$ in (29) with $Q_{II} = \frac{x}{\alpha_u}$. Similarly, the PDF of $\zeta_{E_1,u}^N$, denoted by $f_{\zeta_{E_1,u}^N}(x)$, can be obtained by relaxing the indicator conditions and replacing $Q_1$ in (30) with $Q_{II}$.

B. SOP Analysis With NMRT Beamforming

Based on the channel statistics in IV-A, we will analyze the SOP of the paired users with NMRT beamforming. The SOPs of the near and far users are presented in the following theorems and corollary.

Theorem 1: For the EVEs in Case I, the SOP of the near user can be evaluated by following two cases: (a) $a_f \leq a_n \gamma^{th}_{f,n}$, $\varphi_{n_1} = 1$; (b) $a_f > a_n \gamma^{th}_{f,n}$.

$$\varphi_{n_1}^N \approx \left( \vartheta_n < \mu_n \right) F_{\zeta_n}^N(\eta_1) + \left( \mu_n < \vartheta_n \right) \sum_{m=0}^{M} \frac{\pi (\vartheta_n - \mu_n)}{2 M} \left( 1 - e^{-\Xi_n r_n^{\alpha}} \right) \vartheta_n \left( 1 - \sqrt{1 - r_m^2 f_{\zeta_{E_1,n}}^N(\eta_2)(\vartheta_m)} - F_{\zeta_{E_1,n}}^N(\vartheta_n) \left( F_{\zeta_{E_1,n}}^N(\vartheta_n) - F_{\zeta_{E_1,n}}^N(\mu_n) - 1 \right) \right), \quad (31)$$

where $\mu_n = (\eta_1 + 1)e^{-\Xi_n r_n^{\alpha}} - 1$, $\eta_2(x) = e^{-\Xi_n r_n^{\alpha}} (1 + x) - 1$, $F_{\zeta_n}^N(x)$ is given in (24), $F_{\zeta_{E_1,n}}^N(x)$ and $f_{\zeta_{E_1,n}}^N(x)$ are given in Lemma 6, $\vartheta_m = \cos\left(\frac{(2m+1)\pi}{2M}\right)$, $\vartheta_m = \frac{(2m+1)\vartheta_m}{2M}$, and $M$ is the parameter to balance the tradeoff between the complexity and accuracy of Gauss-Chebyshev quadrature approximation.

Proof: See Appendix E.

Theorem 1 indicates that the SOP for the near user depends on the target code rate of the far user and the power allocation factors (i.e., $a_n$ and $a_f$). For instance, SOP for the near user always equals to one if $a_f \leq a_n \gamma^{th}_{f,n}$. Furthermore, if $\vartheta_n < \mu_n$, the SOP of the near user is not influenced by EVEs.

Corollary 1: For the EVEs in Case II and $a_f > a_n \gamma^{th}_{f,n}$, the SOP of the near user is

$$\varphi_{n_1}^N \approx \sum_{m=0}^{M} \frac{\pi^2 \sec^2\left( \frac{(2m+1)\pi}{4} \right)}{4 M} \left( 1 - \vartheta_m \right) \varphi_{n_1}^N(\vartheta_m) + \varphi_{n_1}^N(\eta_1) F_{\zeta_{E_1,n}}^N(\mu_n), \quad (32)$$

where $\vartheta_m = \tan\left( \frac{(2m+1)\pi}{4} \right)$ + $\mu_n$, $F_{\zeta_n}^N(x)$ is given in (24), $F_{\zeta_{E_1,n}}^N(x)$ and $f_{\zeta_{E_1,n}}^N(x)$ are given in Remark 2.

Proof: The proof is similar to Theorem 1 and omitted here for space limitation.

Theorem 2: For the EVEs in Case L, $L \in \{I, II\}$, the SOP of the far user is

$$\varphi_{f_1}^N \approx \sum_{m=0}^{M} \frac{\pi^2 L}{M} \left( 1 - \vartheta_m \right) \varphi_{f_1}^N(\vartheta_m) F_f^N(\eta_1(\vartheta_m)), \quad (33)$$

where

$$\eta_1(x) = e^{-\Xi x^{\alpha}} (1 + x) - 1, \quad \mu_f = e^{-\Xi x^{\alpha}} (1 + \vartheta_f) - 1, \quad \vartheta_m = \frac{(2m+1)\vartheta_m}{2M},$$

and $F_f^N(x)$ is given in (28), $F_{\zeta_{E_1,f}^N}(x)$ and $\varphi_{f_1}^N(\eta_1(\vartheta_m))$.

$$F_f^N(x) = \frac{4 \Xi^{\frac{1}{2}}}{\alpha R^2} \left( \frac{4}{\alpha} \Xi f R^2 \right)^2 + \sum_{l=1}^{L-1} P_u (L_e) \frac{\Gamma(1-L_e)2^L}{B(L-L_e,L_e)} \frac{Q_{II}^{1/2}}{R^2} \left[ \frac{\Xi f R^2}{L_e + \frac{\alpha}{2}} \right], \quad (28)$$
\[ f_{\xi_{E_{1,f}}}^N(x) \text{ are given in Lemma 6, } F_{\xi_{E_{1,f}}}^N(x) \text{ and } f_{\xi_{E_{1,f}}}^C(x) \text{ are given in Remark 2.} \]

**Proof:** With the definition of SOP in (7), the SOP of the far user is

\[
P_j^N = \Pr \{ R_{f,s} < R_{f,s} \} = \Pr \{ \xi_f < \eta_2(\xi_{E_{1,f}}) \}
\]

\[
= \int_0^{\mu_f} f_{\xi_{E_{1,f}}}^N(x) F_{\eta_2}^C(\eta_2(x)) \, dx + \int_{\mu_f}^{\infty} f_{\xi_{E_{1,f}}}^N(x) \, dx
\]

\[
= 1 - \int_0^{\mu_f} f_{\xi_{E_{1,f}}}^N(x) \bar{P}_j^N(\eta_2(x)) \, dx,
\]

where (a) follows from the fact that \( F_{\xi_{E_{1,f}}}^N(\eta_2(x)) \) always equals to one if \( \eta_2(x) \geq \vartheta_f \) (i.e., \( \xi_{E_{1,f}} < \mu_f \)); (b) follows from \( \mu_f < \vartheta_f \) and \( F_{\xi_{E_{1,f}}}^N(x) = 1 - \bar{P}_j^N(x) \) when \( x < \vartheta_f \) as in Lemma 5. Finally, by applying Gauss-Chebyshev quadrature, we obtain the SOP of the far user given in (33).

**V. SECRECY PERFORMANCE ANALYSIS WITH CMRT BEAMFORMING**

In this section, we will analyze the secrecy performance of mmWave NOMA networks with CMRT beamforming. We will first derive the channel statistics, i.e., the distribution of common resolvable paths and the SINR distributions of the paired users and EVEs. Then, we will derive the analytical expressions of the SOP for both paired users.

**A. Channel Statistics**

According to the proposed CMRT beamforming scheme, we know that the SINRs at the paired users and EVEs are conditional on \( L_c \). Thus, we need to derive the conditional distributions of \( \xi_u^C \) and \( \xi_{E_{1,u}}^C \) for \( u \in \{ n, f \} \).

**Lemma 7:** The conditional CDF of \( \xi_u^C \), i.e., \( \Pr \{ \xi_u^C < x; L_c \} \), is

\[ F_{\xi_u^C}^C(x; L_c) = \begin{cases} 1 \text{ if } (L_c = 0) F_n(x; L, 0.5) + \sum (L_c \neq 0) F_n(x; L_c, a_n), \end{cases} \]

where

\[ F_n(x; L, a_n) = \left[ 1 + \frac{\beta}{\alpha} \sum_{i=0}^{L-1} \frac{1}{\alpha^2 (i+1)^2} \right] (R^2 x \tilde{\Delta}_n^2) - \frac{\alpha^2}{\alpha^2 (L-a_n)^2}. \]

**Proof:** The proof is similar to Lemma 4 and omitted here for space limitation.

**Lemma 8:** The conditional CDF of \( \xi_f^C \), i.e., \( \Pr \{ \xi_f^C < x; L_c \} \), is

\[ F_{\xi_f^C}^C(x; L_c) = \begin{cases} 1 \text{ if } (L_c = 0) F_f(x; L, 0.5) + \sum (L_c \neq 0, x \geq \vartheta_f) \end{cases} + \frac{1}{1 - F_f(x; L, 0.5)} \]

\[ + \sum (L_c \neq 0, x < \vartheta_f) \]

\[ A_2^U(i) = \begin{cases} 1 \text{ if } (i \leq N_t - 2L + L_a + 1, L_a < L_c) F_{\xi_{E_{1,u}}}^C(\varphi_i + L - L_a, \varphi_i + L_a + 1) + \frac{1}{L - L_a + 1}, L_a < L_c \end{cases} \]

\[ \times F_{\xi_{E_{1,u}}}^C(\varphi_i - L_a, \varphi_i - L_a + 1) \]

where \( F_f(x; L, a_n) = \frac{1}{2} \sum_{i=0}^{L-1} \frac{1}{\alpha^2 (i+1)^2} \frac{1}{2} \gamma(1 + 2L, 2L + 1) \Gamma(2L + 1) \).

**Proof:** The proof is similar to Lemma 5 and omitted here for space limitation.

To obtain the conditional distribution of \( \xi_{E_{1,u}}^C \) in (16), we need to find the number of common resolvable paths between the user pair and the \( e \)th EVE, denoted by \( L_a \). It is clear that \( L_a \) depends on \( L_c \). In the following lemma, we give the joint distribution of \( L_a \) and \( L_c \).

**Lemma 9:** Based on the MA user pairing scheme in (4), the joint distribution of \( L_a \) and \( L_c \), \( 1 \leq L_a \leq L_c \leq L \), is

\[ P_a(L_a, L_c) = \begin{cases} \sum_{i=1}^{N_t-L_c} \frac{\gamma - 1}{2} \frac{\gamma + 1}{2} \gamma(1 + 2L, 2L + 1) \Gamma(2L + 1) \end{cases} \]

\[ + \frac{1}{1 - F_f(x; L, 0.5)} \]

\[ + \sum (L_c \neq 0, x < \vartheta_f) \]

\[ A_2^U(i) = \begin{cases} 1 \text{ if } (i \leq N_t - 2L + L_a + 1, L_a < L_c) F_{\xi_{E_{1,u}}}^C(\varphi_i + L - L_a, \varphi_i + L_a + 1) + \frac{1}{L - L_a + 1}, L_a < L_c \end{cases} \]

\[ \times F_{\xi_{E_{1,u}}}^C(\varphi_i - L_a, \varphi_i - L_a + 1) \]

\[ A_2^D(i) = \begin{cases} 1 \text{ if } (i \leq N_t - L - L_a + 1, L_a < L_c) F_{\xi_{E_{1,u}}}^C(\varphi_i + L_a - L_a, \varphi_i + L_a + 1) + \frac{1}{L - L_a + 1}, L_a < L_c \end{cases} \]

\[ \times F_{\xi_{E_{1,u}}}^C(\varphi_i - L_a, \varphi_i - L_a + 1) \]

\[ = \begin{cases} \sum_{i=1}^{N_t-L_c} \frac{\gamma - 1}{2} \frac{\gamma + 1}{2} \gamma(1 + 2L, 2L + 1) \Gamma(2L + 1) \end{cases} \]

\[ + \frac{1}{1 - F_f(x; L, 0.5)} \]

\[ + \sum (L_c \neq 0, x < \vartheta_f) \]

\[ A_2^D(i) = \begin{cases} 1 \text{ if } (i \leq N_t - L - L_a + 1, L_a < L_c) F_{\xi_{E_{1,u}}}^C(\varphi_i + L_a - L_a, \varphi_i + L_a + 1) + \frac{1}{L - L_a + 1}, L_a < L_c \end{cases} \]

\[ \times F_{\xi_{E_{1,u}}}^C(\varphi_i - L_a, \varphi_i - L_a + 1) \]

shown at the bottom of this page, respectively.
where \( \Xi = \lambda_c \Delta_p \left( \frac{\alpha_2 N_1}{L} \right)^\frac{1}{2} \sum_{L=1}^{L_c} \frac{L_c-1}{L_c} P_c(L_c)^{4(L_c+1)} \alpha_1(L_c+1) \),
\[
\Xi = \lambda_c \Delta_p \left( \frac{\alpha_2 N_1}{L} \right)^\frac{1}{2} \sum_{L=1}^{L_c} \frac{L_c-1}{L_c} P_c(L_c)^{4(L_c+1)} \alpha_1(L_c+1) 
+ \sum_{L=1}^{L_c-1} \frac{L_c-1}{L_c} P_c(L_c) B(L_a + \bar{\zeta}, L_c - L_a) \right). 
\]

**Proof:** The proof is similar to Lemma 6 and omitted here for space limitation.

Based on the result in Lemma 10, we can then obtain the conditional PDF of \( \zeta_{E,u} \) given as
\[
f_{\zeta_{E,u}}(x; L_c) = \frac{2\Xi}{\alpha x_1 + \Xi} e^{-\Xi x_1} F_1 \sum_{n=0}^{L_c-1} \left( \frac{\alpha_2 N_1}{L_c} \right)^n \left( \frac{L_c-1}{L_c} P_c(L_c)^{4(L_c+1)} \alpha_1(L_c+1) \frac{\Xi}{\alpha} \right),
\]
and \( f_{\zeta_{E,u}}(x; L_c) = 0 \) if \( \Xi = 0 \).

**B. SOP Analysis With CMRT Beamforming**

Based on the channel statistics in V-A, we can analyze the SOP of the proposed NOMA scheme with CMRT beamforming. From Theorem 1, we know that the SOP of the near user always equals to one if \( \alpha_f \leq \alpha_n \zeta_{f,n} \), and hence we only need to investigate the SOP with \( \alpha_f > \alpha_n \zeta_{f,n} \). The SOPs of the near and far users are presented in following theorems.

**Theorem 3:** For the EVEs in Case 1 and \( \alpha_f > \alpha_n \zeta_{f,n} \), the SOP of the near user is \( \mathcal{P}_{n,i}^C = \mathcal{P}_{n,i,1}^C + \mathcal{P}_{n,i,2}^C \), where
\[
\mathcal{P}_{n,i,1}^C \approx \sum_{m=0}^{M} \frac{\pi^2 \sec^2 \left( \frac{\pi (z_m + 1)}{4} \right)}{M} \sqrt{1 - z_m^2} \mathcal{P}_u(0) 
\times f_{\zeta_{E,i}}(\hat{\theta}_n; 0) F_{\zeta_{C}}(\hat{\eta}_2(\hat{\theta}_n); 0),
\]
\[
\mathcal{P}_{n,i,2}^C \approx \sum_{L=1}^{L_c} \frac{L_c-1}{L_c} P_c(L_c) \left( 1 - \mu_n \right) F_{\zeta_{C}}(\hat{\eta}_2(\hat{\theta}_n); 0) 
+ \frac{1}{M} \mathcal{P}_u(0) \mathcal{P}_u(0) \left( 1 - \mu_n \right)
\times f_{\zeta_{E,i}}(\hat{\theta}_n; L_c) F_{\zeta_{C}}(\hat{\eta}_2(\hat{\theta}_n); L_c) - F_{\zeta_{C}}(\hat{\theta}_n; L_c),
\]
(46)

**VI. NUMERICAL RESULTS**

In this section, numerical results are provided to evaluate the secrecy performance of mmWave NOMA networks with the proposed user pairing scheme and beamforming schemes. The carrier frequency is \( f_c = 73 \) GHz, and the mmWave bandwidth is \( W = 2 \) GHz. The noise figure is \( NF = 10 \) dB, and the noise power is \( \sigma^2 = -174 + 10 \log_{10}(W) + NF \) dB [7]. Based on the UMI-street LOS pathloss model in 5G Channel Model (5GCM) [26], we have \( \alpha = 2.1 \) and \( \beta = 10^{3.24} f_c^2 \). The optimal power allocation factors for the near user and the far user can be obtained with bisection search. To facilitate illustration, we set \( R_u = 0.5 \) bps/Hz and \( R_{ul} = 0.1 \) bps/Hz [26]. For all numerical results, the number of the simulation term of Gauss-Choebyshev quadrature is set to 50. Monte Carlo simulations are provided to evaluate the effectiveness of analytical results. In simulations, the radius of the disc region of potential EVEs is 2000 meters.

Fig. 2(a) illustrates the impact of \( K, \lambda_c \) and different NOMA user pairing schemes (i.e., the MA user pairing scheme in (4) and the randomly selected pairing scheme) on the system SOP in Case 1 with NMRT beamforming. In the randomly selected pairing scheme, the paired users are randomly selected in the angular domain, which is consistent with the random far-user and random near-user (RNRF) pairing scheme in [6]. Fig. 2(a) shows the close agreement between simulated and analytic results. We can observe that SOP decreases as the EVE density decreases. Additionally, when user density increases, SOP with the MA user pairing scheme decreases. MA user pairing can achieve smaller SOP than randomly selected pairing. The reason is that MA pairing can increase the probability that the paired users located in the same beam and thus potentially protect against information leakage.

**Theorem 4:** Considering the EVEs in Case 1, the SOP of the far user is \( \mathcal{P}_{f,i} = \mathcal{P}_{f,i,1}^C + \mathcal{P}_{f,i,2}^C \), where
\[
\mathcal{P}_{f,i,1}^C \approx \sum_{m=0}^{M} \frac{\pi^2 \sec^2 \left( \frac{\pi (z_m + 1)}{4} \right)}{4 M} \sqrt{1 - z_m^2} \mathcal{P}_u(0) 
\times f_{\zeta_{E,i}}(\hat{\theta}_n; 0) F_{\zeta_{C}}(\hat{\eta}_2(\hat{\theta}_n); 0),
\]
(47)

\[
\mathcal{P}_{f,i,2}^C = \sum_{m=0}^{M} \frac{\pi^2 \sec^2 \left( \frac{\pi (z_m + 1)}{4} \right)}{4 M} \sqrt{1 - z_m^2} P_u(0) 
\times \hat{\eta}_2(1 + x - 1, F_{\zeta_{C}}^f(x; L_c) \text{ and } f_{\zeta_{E,i}}^f(x; L_c) \text{ are given in (36) and (45), respectively.}

**Proof:** The proof is similar to Theorem 2 and is omitted here for space limitation.

For Case 2, the SOP of user \( u, \forall u \), denoted by \( \mathcal{P}_{u,i}^C \), is straightforward to obtain following the similar procedure to Case 1. Thus, the detailed expression of \( \mathcal{P}_{u,i}^C \) is omitted. Considering the EVEs in case \( L, L \in \{1, 2\} \), the system SOP of the selected user pair (i.e., the probability of either user in outage) [10] is
\[
\varphi_{L}^S = 1 - (1 - \varphi_{L}^S)(1 - \varphi_{L}^S),
\]
(50)
of the user pair. However, the probability of the paired users and EVEs in the same beam increases and hence increases the probability of information leakage. Furthermore, it is shown that SOP increases as $N_t$ increases when $L$ is small and decreases as $N_t$ increases when $L$ is large. The reason is that, when $L$ is small, the probability that the selected user pair in the same beam is small and becomes smaller as $N_t$ decreases. When $L$ is large, there might be lots of users in the beam of the near user and we can always select the paired user in the same beam. Additionally, the probability of the user pair and EVE in the same beam decreases as $N_t$ increases. Finally, we observe that the CMRT scheme can achieve a smaller system SOP than the NMRT scheme.

Fig. 3(a) shows the SOPs of the far user ($f$) and the near user ($n$) with different beamforming schemes (i.e., NMRT and CMRT beamforming) versus $P_t$. For both beamforming schemes, the SOP of the near user monotonously decreases as $P_t$ increases and the SOP of the near user is significantly smaller than that of the far user. The reason is that the designed beam mainly depends on the channel of the near user. Additionally, the SOP of the far user first decreases and then increases when $P_t$ increases. The reason is that, when $P_t$ increases, the signal power for the far user increases, and hence SOP decreases. However, the far user also suffers from increasing interference from the near user and thus SOP increases. With NMRT beamforming, the SOP of the near user is smaller than that with CMRT beamforming. In contrast, with CMRT beamforming, the SOP of the far user is smaller than that with NMRT beamforming. The reason is that the NMRT beamforming can align transmitting beam steering in all resolvable paths of the near user, and thus guarantee the security for the near user. However, NMRT leads to stronger interference and poor reception quality to the far user. We also observe that CMRT beamforming can achieve smaller system SOP than NMRT beamforming since the system SOP of the selected user pair is mainly determined by the SOP of the far user, as shown in Fig. 3(a). Thus, for
the paired users, there may be an optimal $P_t$ to minimize the system SOP.

Fig. 3(b) shows the impacts of the radius of networks (i.e., $R$), the target secrecy rate (i.e., $R_u^\mathrm{e}_{1}\ni\forall t$) and different beamforming schemes on the system SOP. We observe that, for both beamforming schemes, SOP first decreases and then increases when $R$ increases. This implies that there exists the optimal radius of networks to minimize the system SOP. The reason is that, when $R$ increases, the number of users located in the network increases and thus the probability that the selected user pair in the same beam increases. However, the selected user pair is more likely to suffer from large path-loss. Additionally, we see that CMRT beamforming can achieve smaller SOP than NMRT beamforming. If $R$ increases, the SOPs with different beamforming schemes tend to be the same. The reason is that, when $R$ is large, the selected user pair is always located in the same beam and the number of common resolvable paths equals to $L$. Thus, the near-user based beamforming scheme (NMRT) and common-path based beamforming scheme (CMRT) are the same, as shown in Fig. 3(b). We observe that, for both beamforming schemes, SOP increases if $R_u^\theta$ increases. Finally, we see that the SOP in Case 1 is always smaller than that in Case 2.

Fig. 4 shows the system SOPs of NOMA-CMRT and OMA schemes versus $P_t$ and $a_u$. It is shown that there exists an optimal power allocation factor $a_u$ to minimize the SOP of the proposed NOMA-CMRT scheme. We can also see that, with appropriate power allocation factor $a_u$, the SOP of NOMA-CMRT scheme is smaller than that of OMA schemes at low to medium transmit power regimes. However, at high transmit power regimes, the OMA scheme can achieve smaller SOP than the proposed NOMA-CMRT scheme. The reason is that, with increasing $P_t$, the far user with the NOMA-CMRT scheme suffers from increasing interference from the near user, and thus SOP increases, while there is no interference between the far user and the near user with OMA schemes. Therefore, NOMA-CMRT requires proper power allocation in order to outperform OMA, which may cause high computational complexity and energy cost.

VII. Conclusion

We have studied the physical layer security of mmWave NOMA networks with a geometric channel model characterizing the limited scattering propagation of mmWave signals. Considering the directional mmWave signals, we have proposed a minimal angle-difference (MA) user pairing scheme to enhance secrecy performance. Based on the spatial correlation of the paired users, we have developed two beamforming schemes (i.e., NMRT and CMRT beamforming) to further improve the secrecy performance. Then stochastic geometry has been used to derive the channel statistics and the SOPs for the paired users. Simulation results reveal that our proposed MA user pairing scheme can achieve better secrecy performance than that with the randomly selected pairing scheme. Furthermore, they reveal that there exists an optimal radius of networks, and number of spatially resolvable paths and transmitting SNR to minimize the system SOP. Finally, we have found that NMRT beamforming can significantly reduce the SOP of the near user, while CMRT beamforming can effectively reduce the system SOP. If the number of users located in the network is large, these two schemes can achieve similar secrecy performance. With proper power allocation, NOMA with CMRT beamforming scheme can achieve better secrecy performance than conventional OMA in low to medium transmit power regimes.

APPENDIX A

PROOF OF LEMMA 1

We first derive the distribution of the angle difference between paired users according to the proposed MA user pairing scheme in (4). Since users are randomly located in $\mathcal{D}$ following a homogeneous PPP, the locations of $K$ users in $\mathcal{D}$ are independent and the angle of the $k$-th user $U_k$ with respect to the BS denoted by $\theta(U_k)$ for $k = 0, 1, \ldots, K - 1$ is uniformly distributed in $[\varphi_1, \varphi_{N_t} - L + 2]$. Let $\phi_k^0$ denote the event $\theta(U_0) \in [\varphi_1, \varphi_{N_t} - L + 2]$. For any $k \neq 0$, the probability of $\Delta_{0,k}^i = |\theta_0^i - \theta(U_k)| < \triangle$ conditioned on $\phi_k^0$, can be expressed as $F_{\Delta_{0,k}^i}(\triangle) = \Pr\{\Delta_{0,k}^i < \triangle; \phi_k^0\} = \frac{2\triangle}{\Delta_p}$. Based on the MA user pairing scheme, we have $\Delta_{0,k}^i = |\theta_0^i - \theta(U_p)| = \min_{k \neq 0} \Delta_{0,k}^i$. Thus, the conditional cumulative distribution function (CDF) of $\Delta_{0,k}^i$ is

$$F_{\Delta_{0,k}^i}(\triangle) = \Pr\{\min_{k \neq 0} \Delta_{0,k}^i < \triangle; \phi_k^0\}.$$ (51)

Conditioned on $\phi_k^0$, $\min_{k \neq 0} \Delta_{0,k}^i < \triangle$ occurs when at least one user $U_k$, $k \neq 0$ satisfies $\Delta_{0,k}^i < \triangle$. The complement of this event is $\Delta_{0,k}^i \geq \triangle$ for all $k \neq 0$, which has the probability $(1 - F_{\Delta_{0,k}^i}(\triangle))^{K-1}$. We then have

$$F_{\Delta_{0,k}^i}(\triangle) = 1 - \left(1 - \frac{2\triangle}{\Delta_p}\right)^{K-1}.$$ (52)

Since all users are uniformly distributed in $[\varphi_1, \varphi_{N_t} - L + 2]$, we have $\Pr\{\phi_k^0\} = \frac{\varphi_{N_t} - \varphi_1}{\Delta_p}$. Conditioned on $\phi_k^0$, we analyze the distribution of $L_c$ in following three cases.
Case (1): $L_c = L$. The paired user $U_p$ share the same resolvable paths as $U_0$. We then have
\[
\Pr(L_c = L; e_0^{(i)}) = \Pr\{\theta(U_p) - \theta_0^i < \phi_{i+1} - \theta_0^i; e_0^{(i)}\} = F_{\Delta \theta_p}(\phi_{i+1} - \theta_0^i).
\]
According to the law of total probability, we then have
\[
P_u(L) = \sum_{i=1}^{N_t - L + 1} \Pr(e_0^{(i)}) \Pr(L_c = L; e_0^{(i)}) = \sum_{i=1}^{N_t - L + 1} \Pr(e_0^{(i)}) F_{\Delta \theta_p}(\phi_{i+1} - \theta_0^i).
\]

Case (2): $L_c = 1, 2, \ldots, L - 1$. Since the angular range $[\varphi_1, \varphi_{N_t-L+2}]$ is symmetry, we just need to calculate the distribution of $L_c$ with the condition $e_0^{(i)}$ for $i \in \{N_t, \ldots, N_t - L + 1\}$. Given $e_0^{(i)}$ and the paired user $U_p$ should be located in the angular range $[\varphi_{i+L-L_c} - \theta_0^i, \varphi_{i+L-L_c+1} - \theta_0^i]$ for $i + L - L_c + 1 \leq N_t - L + 2$ and the angular range $[\theta_0^i - \varphi_{i-L+L_c}, \theta_0^i - \varphi_{i-L+L_c+1}]$ for $i + L - L_c \geq 1$. Thus, we have $\Pr(L_c; e_0^{(i)})$ given in (55), shown at the bottom of this page.

According to the law of total probability, we then have
\[
P_u(L) = \Pr(e_0^{N_t}) \Pr(L_c; e_0^{N_t}) + \sum_{i=N_t+1}^{N_t-L+1} 2 \Pr(e_0^{(i)}) \Pr(L_c; e_0^{(i)}).
\]

Case (3): $L_c = 0$. Based on the results in Case (1) and Case (2), we have $P_u(L_c = 0) = 1 - \sum_{L=1}^{L_c} P_u(L_c = l)$.

APPENDIX B
PROOF OF LEMMA 2
For two users $U_0$ and $U_p$ in $\mathcal{D}$, we have $r_n = \min(r_0, r_p)$, where $r_0$ ($r_p$) is the distance between $U_0$ ($U_p$) and the BS. Since the spatial locations of $U_0$ and $U_p$ follow a homogeneous PPP, the CDFs of $r_0$ and $r_p$ are the same, and given as $F_{r_n}(r) = F_{r_p}(r) = \frac{r^2}{R^2}$. Then, the CDF of $r_n$ is
\[
F_{r_n}(r) = 1 - \Pr(\min(r_0, r_p) > r)
\]
\[
= 1 - \Pr(r_0 > r) \Pr\{\min(r_0, r_p) > r\}
\]
\[
= 1 - (1 - F_{r_0}(r))(1 - F_{r_p}(r))
\]
\[
= \left(1 - \left(1 - \frac{r^2}{R^2}\right)^2\right).
\]

Thus, the PDF of $r_n$ in (20) can be obtained by taking the derivative of $F_{r_n}(r)$. On the other hand, let $r_f = \max(r_0, r_p)$ denote the distance between the far user and the BS. Following a similar procedure in (57), the PDF of $r_f$ in (21) can be obtained.

APPENDIX C
PROOF OF LEMMA 5
With $h_f = \sqrt{\frac{\beta N_t r_f^{\alpha_c}}{L}} \cdot g_f U^H$ and $w_N = \frac{h_f}{\|g_n\|}$, we have
\[
\|h_f w_N\|^2 = \left(\frac{\beta N_t r_f^{\alpha_c} \|g_{f,c_n} H_{f,c_n}\|^2}{L \|g_n\|^2}\right)
\]
\[
= \left(\frac{\beta N_t r_f^{\alpha_c} \|g_{c_n}\|^2 \|H_{c_n}\|^2}{L \|g_n\|^2}\right), \quad \text{if } L_c > 0,
\]
\[
= 0, \quad \text{if } L_c = 0,
\]

where (a) follows from the fact that $g_f H_{c_n} = g_{c_n}^H H_{c_n}$ only if $i \in \Omega_{c_n}$, $g_f^g H_{c_n}$ since $g_{c_n}^g \neq 0$. Let $u_c = \|g_{c_n}\|^2 \sim \Gamma \left(L_c, 1\right)$ and $\tau = \|g_f H_{c_n}\|^2 \sim \Gamma \left(L_c, 1\right)$. According to our channel model, $g_n$ and $g_f$ are uncorrelated, and thus $g_{c_n}$ and $g_f H_{c_n}$ are independent. With the result in [24], we find that $\tau \sim \text{Exp}(1)$. We then have, if $L_c > 0$, $\zeta^{N_t}_{f,c} = \frac{1}{2} \left\{\zeta^{N_t}_{f,c}(i \leq N_t - 2L + L_c + 1) \Pr\{\theta(U_p) - \theta_0^i \in [\varphi_{i+L-L_c} - \theta_0^i, \varphi_{i+L-L_c+1} - \theta_0^i]; e_0^{(i)}\}ight\}
\]
The CDF of $\zeta_j^N$ is

$$F_{\zeta_j^N}(x) = P_a(0) \Pr \{ \zeta_j^N < x; L_c = 0 \} + \sum_{L_c=1}^{L} P_a(L_c) \Pr \{ \zeta_j^N < x; L_c = 0 \},$$

(59)

where $\Pr \{ \zeta_j^N < x; L_c = 0 \} = 1$ and $T_f^j(x)$ is expressed as

$$T_f^j(x) = \begin{cases} 1 - E_{r_f,\nu_c}[e^{-\frac{\nu r_f}{\nu_c}}], & \text{if } x < \vartheta_f, \\ 1, & \text{if } x \geq \vartheta_f. \end{cases}$$

(60)

By denoting $T_f^2(x) = E_{r_f,\nu_c}[e^{-\frac{\nu r_f}{\nu_c}}]$ and with the PDF of $r_f$ in Lemma 2, we have

$$T_f^2(x) = \frac{4}{\alpha R^3} \mathcal{F}_\nu \left( \int_0^R \frac{4 \nu^3}{R^2} e^{-\frac{\nu r_f}{\nu_c}} dr_f \right) \left(\frac{\nu}{\nu_c}\right)^{-\frac{2}{3}} \gamma \left(\frac{4}{\alpha}, -\frac{\nu^2 R^3}{\nu_c} \right).$$

(61)

Since $\nu$ and $\nu_c$ are dependent, we cannot calculate the expectation in (61) over $\nu$ and $\nu_c$ individually, and thus the joint distribution of $\nu$ and $\nu_c$ should be defined. Defining $w = \frac{\nu}{\nu_c}$, we can discuss the distribution of $w$ in following two cases:

a) $L_c = L$: It is clear that $\nu_c = \nu$, and $w = 1$. Thus, we have

$$T_f^2(x) = \frac{4}{\alpha R^3} \mathcal{F}_\nu \left( \int_0^R \frac{4 \nu^3}{R^2} e^{-\frac{\nu r_f}{\nu}} dr_f \right);$$

b) $0 < L_c < L$: Since $\Omega_{c,a} = \Omega_a \setminus \Omega_{pa}$, we have $\|g_n\|^2 = \|g_{n,pa}\|^2 + \|g_{n,ca}\|^2$, and $g_{n,pa}$ and $g_{n,ca}$ are independent. Let $\nu_c = \|g_{n,pa}\|^2$, we have $w = 1 + \frac{\nu_c}{\nu}$. Since $\nu_c \sim \Gamma(1, L_c)$, $\nu_c \sim \Gamma(L_c, L_c)$ are independently distributed, $\frac{\nu}{\nu_c}$ follows a beta prime distribution, denoted by $\beta^\nu(L_c, L_c)$. Thus, we can obtain the PDF of $w$ given as $f_w(w) = \frac{(w-1)^{L-c-1} e^{-w}}{w^{L-L_c}}$ for $w > 1$.

Then, substituting $f_w(w)$ into (61), we have

$$T_f^2(x) = \frac{4 \mathcal{F}_\nu \left( \int_0^\infty \left( w-1 \right)^{L-L_c-1} e^{-w} \frac{4}{\alpha} \mathcal{F}_{\nu_c}(w) dw \right)}{\alpha R^3 \mathcal{B}(L-L_c, L_c)}$$

$$= \frac{4 \mathcal{F}_\nu \left( \int_0^\infty \left( w-1 \right)^{L-L_c-1} e^{-w} \frac{4}{\alpha} \mathcal{F}_{\nu_c}(w) dw \right)}{\alpha R^3 \mathcal{B}(L-L_c, L_c)}$$

(62)

where (a) follows from $\gamma(s, x) = \mathcal{G}_{\nu_c}^{1,1}[x]^{\frac{1}{\nu_c},1}$ and by invoking (7.811.3) in [32]. Finally, after combining the aforementioned results in case (a) and (b), the CDF of $\zeta_j^N$ in (27) can be obtained.

### Appendix D

#### Proof of Lemma 6

Assuming $h_e = \sqrt{\frac{\beta N_t}{L_c}} g_e U_e^H$, the channel of the $e$-th EVE in $\Phi_c$. With a similar procedure in Lemma 5, we have

$$\|h_e w_N\|^2 = \frac{\|h_e h_N^H\|^2}{\|h_n\|^2} = \left( \frac{\beta N_t c_e^2 \nu_c}{L_p} \right) \left( \frac{\beta N_t c_e^2 \nu_c}{L_p} \right) \neq 0,$$

(63)

where $\nu_c^e = \|g_e, c_e\|^2 \sim \Gamma(1, L_c)$, $\tau_e = \|g_e, c_e\|^2 \sim \exp(1)$. Thus, if $L_c > 0$, $\zeta_N^{E_1, u, e} = \frac{\beta N_t c_e^2 \nu_c}{L_p} \frac{\beta N_t c_e^2 \nu_c}{L_p} \neq 0$. Considering non-colluding EVEs, the CDF of $\zeta_N^{E_1, u}$ is

$$F_{\zeta_N^{E_1, u}}(x) = \mathbb{E}_{\Phi_c} \left( \prod_{e \in \Phi_c} \Pr \{ \zeta_N^{E_1, u, e} < x \} \right)$$

(64)

where (a) follows from the probability generating functional lemma (PGFL) of a homogeneous PPP [10] and switches to polar coordinates. (b) follows by taking the expectation over variable $\tau_e$. With a similar procedure in Lemma 5 and by invoking (3.26.1) and (3.19.6) in [32], we can obtain the CDF of $\zeta_N^{E_1, u}$ presented in (29). Finally, by taking the derivative of $F_{\zeta_N^{E_1, u}}(x)$, we obtain the PDF of $\zeta_N^{E_1, u}$ given in (30).

### Appendix E

#### Proof of Theorem 1

With the definition of SOP in (7), we find that the SOP of the near user is conditioned on whether the signal intended for the far user, i.e., $s_f$, can be decoded or not. Thus, we need to find the distribution of $\zeta_j^N$ given, as follows

$$\Pr \{ \zeta_j^N < x \} = \begin{cases} \frac{F_{\zeta_N^a}}{\alpha_f - a_n x}, & \text{if } a_f > a_n x, \\ 1, & \text{if } a_f \leq a_n x. \end{cases}$$

(65)

Then, the SOP of the near user is given in (66), shown at the top of the next page. In (66), if $a_f > a_n c_e^{h_{E_1, n}}$, $P_{n, 0} = 1$, since the near user cannot decode $s_f$, and thus it cannot use SIC and decode its own signal. In (66), $P_{n, 0} = 0$ if $\eta_2(\zeta_N^{E_1, n}) < \eta_1$, and it has no contribution to $P_n$. Hence, we only need to consider the case $\eta_2(\zeta_N^{E_1, n}) \geq \eta_1$, which implies that $\zeta_N^{E_1, n} \geq \mu_n$. According to the distributions of $\zeta_N^N$ and $\zeta_N^{E_1, n}$, we will derive $P_n$ in following three cases:

a) $\vartheta_n \leq \mu_n \leq \zeta_N^{E_1, n}$: $P_n = \int_0^\infty f_{\zeta_N^{E_1, n}}(x) F_{\zeta_N^a}(\eta_2(x)) dx - \int_0^{\vartheta_n} f_{\zeta_N^{E_1, n}}(x) F_{\zeta_N^a}(\eta_2(x)) dx = 0;

b) $\mu_n \leq \vartheta_n \leq \zeta_N^{E_1, n}$: with a similar procedure in case (a), we also have $P_n = 0;
\[
\mathcal{P}_n = \Pr \{ \mathcal{R}_{n,s} < \mathcal{R}_{f,n}^{th}; \xi_{f,n}^{th} \geq \xi_{f,n}^{th} \} + \Pr \{ \xi_{f,n}^{th} \geq \xi_{f,n}^{th} \} + \Pr \{ \xi_{f,n}^{th} < \xi_{f,n}^{th} \}
\]

\[
\begin{cases}
\Pr \{ \eta \leq \xi_{f,n}^{th} < \eta \xi_{f,n}^{th} \} + F_{\xi_{f,n}^{th}}(\eta), & \text{if } \eta > \alpha_n \xi_{f,n}^{th} \\
1, & \text{if } \eta \leq \alpha_n \xi_{f,n}^{th}
\end{cases}
\]

(66)

Following [10], we apply Gauss-Chebyshev quadrature to obtain an approximation expression of \( P_n \), given by

\[
P_n^1 \approx \frac{1}{2M_1} \sum_{m_1=0}^{M_1} \pi(\xi_{f,n}^{th} - \mu_{n}) \sqrt{1 - \alpha_n z_{f,n}^{th}(\mu_{n}) F_{\xi_{f,n}^{th}}(\eta_{m_1})}. 
\]

(68)

Additionally, based on the CDF of \( \xi_{f,n}^{th} \) in Lemma 6, we can directly obtain

\[
P_n^2 = F_{\xi_{f,n}^{th}}(\eta_{m_1}) - F_{\xi_{f,n}^{th}}(\mu_{n}). 
\]

(69)

By substituting (68) and (69) into (67), we obtain \( P_n \) for case (c).

Finally, combining the results in above three cases, we obtain the SOP of the near user given by (31).

REFERENCES

[1] M. Xiao et al., “Millimeter wave communications for future mobile networks,” IEEE J. Sel. Areas Commun., vol. 35, no. 9, pp. 1909–1935, Sep. 2017.
[2] X. Wang et al., “Millimeter wave communication: A comprehensive survey,” IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 1616–1653, Jul.–Sep. 2018.
[3] W. Yi, Y. Liu, A. Nallanathan, and M. Elkashlan, “Clustered millimeter-wave networks with non-orthogonal multiple access,” IEEE Trans. Commun., vol. 67, no. 6, pp. 4350–4364, Jun. 2019.
[4] Q. Xue, P. Zhou, X. Fang, and M. Xiao, “Performance analysis of interference and eavesdropping immunity in narrow beam mmWave networks,” IEEE Access, vol. 6, pp. 67 611–67 624, 2018.
[5] C. Jiang and X. Zhu, “Reinforcement learning based capacity management in multi-layer satellite networks,” IEEE Trans. Wireless Commun., vol. 19, no. 7, pp. 4685–4699, Jul. 2020.
[6] T. Lv, Y. Ma, J. Zeng, and P. T. Mathiopoulos, “Millimeter-wave NOMA transmission in cellular M2M communications for Internet of Things,” IEEE Internet Things J., vol. 5, no. 3, pp. 1989–2000, Jun. 2018.
[7] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, “Secure communications in millimeter wave ad hoc networks,” IEEE Trans. Wireless Commun., vol. 16, no. 5, pp. 3205–3217, May 2017.
[8] Z. Xiao, L. Zha, J. Choi, P. Xia, and X.-G. Xia, “Joint power allocation and beamforming for non-orthogonal multiple access (NOMA) in 5G millimeter wave communications,” IEEE Trans. Wireless Commun., vol. 17, no. 5, pp. 2961–2974, May 2018.
[9] Y. Zhou, V. W. Wong, and R. Schober, “Coverage and rate analysis of millimeter wave NOMA networks with beam misalignment,” IEEE Trans. Wireless Commun., vol. 17, no. 12, pp. 8211–8227, Dec. 2018.
[10] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks,” IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656–1662, Mar. 2017.
[11] Z. Ding, P. Fan, and H. V. Poor, “Random beamforming in millimeter-wave NOMA networks,” IEEE Access, vol. 5, pp. 7667–7681, 2017.
[12] N. Rupasinghe, Y. Yapici, I. G üvenç, and Y. Kakihima, “Non-orthogonal multiple access for mmWave drone networks with limited feedback,” IEEE Trans. Commun., vol. 67, no. 1, pp. 762–777, Jan. 2019.
[13] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, “Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems,” IEEE Trans. Veh. Technol., vol. 66, no. 9, pp. 8139–8151, Sep. 2017.
[14] S. Vuppala, Y. J. Tolosa, G. Kaddoum, and G. Abreu, “On the physical layer security analysis of hybrid millimeter wave networks,” IEEE Trans. Commun., vol. 66, no. 3, pp. 1139–1152, Mar. 2018.
[15] Y. Huang, J. Zhang, and M. Xiao, “Constant envelope hybrid precoding for directional millimeter-wave communications,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 845–859, Apr. 2018.
[16] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, “Safeguarding millimeter wave communications against randomly located eavesdroppers,” IEEE Trans. Wireless Commun., vol. 17, no. 4, pp. 2675–2689, Apr. 2018.
[17] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, “Secrecy sum rate maximization in non-orthogonal multiple access,” IEEE Commun. Lett., vol. 20, no. 5, pp. 930–933, May 2016.
[18] Y. Feng, S. Yan, and Z. Yang, “Secure transmission to the strong user in non-orthogonal multiple access,” IEEE Trans. Commun., vol. 66, no. 12, pp. 6263–6266, Dec. 2018.
[19] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, “On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming,” IEEE Trans. Commun., vol. 65, no. 7, pp. 3151–3163, Jul. 2017.
[20] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, “Channel estimation and hybrid precoding for millimeter wave cellular systems,” IEEE J. Sel. Topics Signal Process., vol. 8, no. 5, pp. 831–846, Oct. 2014.
[21] A. M. Sayeed and V. Raghavan, “Maximizing MIMO capacity in sparse multipath reconfigurable antenna arrays,” IEEE J. Sel. Topics Signal Process., vol. 1, no. 1, pp. 156–166, Jul. 2007.
[22] W. Mei, Z. Chen, and S. Li, “Confidential broadcasting and service integration in millimeter wave systems,” IEEE Syst. J., vol. 13, no. 1, pp. 147–158, Mar. 2018.
[23] D. Tse and P. Viswanath, Fundamentals of Wireless Communication. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[24] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, “Secure transmissions in millimeter wave systems,” IEEE Trans. Commun., vol. 65, no. 5, pp. 2114–2127, May 2017.
[25] A. Baddeley, I. Bárány, and R. Schneider, Stochastic Geometry: Lectures Given at the CIME Summer School Held in Martina Franca, Italy, Sep. 13–18, 2004. Berlin, Germany: Springer, 2006.
[26] T. S. Rappaport, X. Peng, R. MacCartney, A. F. Molisch, E. Melli, and J. Zhang, “Overview of millimeter wave communications for fifth-generation (5G) wireless networks—With a focus on propagation models,” IEEE Trans. Antennas Propag., vol. 65, no. 12, pp. 6213–6230, Dec. 2017.
[27] 3GPP TR 36.859, “Study on Downlink Mutiluser Superposition Transmission (MUST) for LTE,” Sophia Antipolis Cedex, France, 2016.
[28] L. Yu, Z. Ding, Q. Ni, and J. Chen, “Secure MISO-NOMA transmission with artificial noise,” IEEE Trans. Veh. Technol., vol. 67, no. 7, pp. 7600–7605, Jul. 2018.
[29] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, “Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer,” IEEE J. Sel. Areas Commun., vol. 34, no. 4, pp. 938–953, Apr. 2016.
[30] T. S. Rappaport et al., “Millimeter wave mobile communications for 5G cellular: It will work!” IEEE Access, vol. 1, pp. 335–349, 2013.
[31] M. Vaezi, R. Schober, Z. Ding, and H. V. Poor, “Non-orthogonal multiple access: Common myths and critical questions,” IEEE Wireless Commun., vol. 26, no. 5, pp. 174–180, Oct. 2019.

[32] I. Gradshteyn, J. Ryzhik, A. Jeffrey, and D. Zwillinger, Table of Integrals, Series, and Products. 7th ed. New York, NY, USA: Academic, 2007.

[33] S. D. Dubey, “Compound gamma, beta and F distributions,” Metrika, vol. 16, no. 1, pp. 27–31, 1970.

Shaocheng Huang received the bachelor’s degree in electronic and information engineering from the Changsha University of Science & Technology, Changsha, China, in 2013. He is currently working toward the Ph.D. degree with the Division of Information Science and Engineering, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden. His current research interests include massive MIMO, millimeter wave communications, machine learning, and physical layer security.

H. Vincent Poor (Fellow, IEEE) received the Ph.D. degree in EECS from Princeton University, in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as Dean of the Princeton’s School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory, signal processing and machine learning, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book Multiple Access Techniques for 5G Wireless Networks and Beyond. (Springer, 2019). Dr. Poor is a Member of the National Academy of Engineering and the National Academy of Sciences, and is a Foreign Member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, the 2019 ASEE Benjamin Garver Lamme Award, a D.Sc. honoris causa from Syracuse University awarded in 2017, and a D.Eng. honoris causa from the University of Waterloo awarded in 2019. In 2018 and 2019, he served as a Distinguished Lecturer for the IEEE Vehicular Technology Society.

Ming Xiao (Senior Member, IEEE) received the bachelor’s and master’s degrees in engineering from the University of Electronic Science and Technology of China, ChengDu, in 1997 and 2002, respectively and the Ph.D. degree from the Chalmers University of Technology, Sweden, in 2007. From 1997 to 1999, he worked as a Network and Software Engineer with ChinaTelecom. From 2000 to 2002, he also held a position in the SiChuan communications administration. From 2007 to now, he has been with the Department of Information Science and Engineering, School of Electrical Engineering and Computer Science, Royal Institute of Technology, Sweden, where he is currently an Associate Professor. He was an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS (2012–2017), IEEE COMMUNICATIONS LETTERS (Senior Editor Since January 2015) and IEEE WIRELESS COMMUNICATIONS LETTERS (2012–2016), and has been an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2018. He was the Lead Guest Editor for IEEE JSAC Special Issue on “Millimeter Wave Communications for Future Mobile Networks in 2017. He has been an Area Editor for IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY since 2019.