IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received April 28, 2019, accepted May 27, 2019, date of publication June 5, 2019, date of current version June 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920963

Secure Transmission in mmWave NOMA Networks With Cognitive Power Allocation

YI SONG[1,2], WEIWEI YANG[1], (Member, IEEE), ZHONGWU XIANG[1], BIAO WANG[3], AND YUEMING CAI[1], (Senior Member, IEEE)

[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huaian 223001, China
[3]School of Electronic and Information, Jiangsu University of Science and Technology, Zhenjiang 212003, China

Corresponding author: Weiwei Yang (wwyang1981@163.com)

This work was supported by the National Natural Science Foundation of China under grant 61471393 and grant 61771487.

ABSTRACT Millimeter wave (mmWave) and non-orthogonal multiple access (NOMA) are two key technologies for future wireless networks. In this paper, secure communication in mmWave NOMA networks based on cognitive power allocation scheme is studied by preferentially satisfying the quality of service (QoS) of primary user. Considering directional beamforming, a corresponding sector guard zone is invoked to against the random distributed eavesdroppers. We give a comprehensive investigation of secrecy performance through stochastic geometry in terms of connection outage probability (COP), secrecy outage probability (SOP), and secrecy throughput (ST). The simulation results validate our derivations and show that the secondary user in NOMA schemes can obtain better connection performance than that in orthogonal multiple access (OMA) schemes, while the primary user achieves the same connection performance in NOMA and OMA schemes. In addition, when the system parameters are reasonable set, the secondary user in NOMA schemes can achieve a higher ST than that in OMA. Moreover, blockages can be also utilized to improve secrecy performance on some occasions.

INDEX TERMS Non-orthogonal multiple access (NOMA), millimeter wave, cognitive power allocation, sector guard zone.

I. INTRODUCTION

In recent years, with the rapid popularization of various mobile intelligent devices and the fast development of wireless communication business, wireless data traffic has increased significantly. Due to abundant available bandwidth [1], [2], millimeter wave (mmWave) communication is a particularly promising method to meet the rapidly growing demand for data traffic in the future. According to the actual measurement results in [3], mmWave communication has the following characteristics compared with traditional microwave networks because of its small wavelength: sensitivity to blockages, variable propagation law, and large number of antennas, etc [4]. Blockages can lead to significant differences in path-loss characteristics between the line-of-sight (LOS) and non-line-of-sight (NLOS) links. Different path loss laws are applied to LOS and NLOS links [3]. Because of the large number of antennas, antenna arrays can be deployed at the transmitter and receiver to achieve beamforming and array gains can be used to ensure high enough received signal power. Recently, there have a large amount of works in terms of coverage and achievable rate for the different mmWave systems [5]–[7], which showed that mmWave networks have great potential to provide a tremendous increase in data traffic. Additionally, for mathematical traceability [8], it is meaningful to approximate the actual array model with sector model when assuming simple maximum signal-to-noise ratio beam steering, where the directional gains of main lobe and side lobe are constant. By using a sector antenna model, the authors investigated the secrecy performance of the noise-limited and the AN-assisted mmWave networks in [9]. Similarly, the secrecy performance of mmWave-overlaid wave networks and ad hoc networks were analyzed in [10], [11].

Non-orthogonal multiple access (NOMA) technique is also considered to be one of the key technologies for the fifth generation (5G) information communication in addition to mmWave [12], [13]. Simply stated, NOMA is essentially

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

a kind of multiplexing [14], which can further increase the number of connections of users by introducing power domain. It can provide larger channel capacity than orthogonal multiple access (OMA) [15]. Power domain NOMA is a hotspot research topic at present. Its main purpose is to separate signals belonging to different users by transmission different power values to the users [16]. Users with higher channel gain are paired with users with lower channel gain, and the difference of channel properties is compensated by allocating more power to users with lower channel gain. Receiver uses successive interference cancellation (SIC) to remove interference from different users. Following this rationale, under the fixed power allocation strategy, the performance of NOMA in a cellular downlink scenario and large-scale underlay cognitive radio networks were investigated by [17] and [18], respectively. The main problem of this strategy is that a user's pre-defined quality of service (QoS) may not be strictly satisfied. Under the dynamic power allocation strategy, the authors proposes a cognitive-radio-inspired NOMA, after assuming that the QoS of users with poor channel conditions was guaranteed, the performance of secondary users was studied in [19]. However, secrecy performance analysis is not considered.

Furthermore, in view of the broadcast characteristics of wireless transmissions, physical layer security (PLS) has been considered in some NOMA systems. The PLS in cognitive radio inspired NOMA networks with multiple primary and secondary users was investigated [20]. The secure transmission of untrusted amplify-and-forward relay in NOMA networks was studied [21]. In [22], the effects of user pairing on the secrecy outage probability (SOP) of NOMA systems are studied, where both single-antenna and multiple-antenna scenarios based power allocation scheme are considered.

NOMA schemes for mmWave communications have been studied in recent years [23]–[27]. The application of random beamforming technique in mmWave-NOMA communication systems was considered, which avoided the requirement of base station for channel state information (CSI) of all users [23], [24]. The outage performance of NOMA in multi-cell mmWave networks was studied, which showed that the performance of NOMA in multi-cell mmWave networks was better than that of OMA [25]. Moreover, by using a sector model to approximate the beamforming pattern, the capacity performance of NOMA-mmWave-massive-multiple-input multiple-output systems with both noise-limited and interference-limited scenarios was studied [26]. In [27], the authors studied how to maximize the sum rate of a two users mmWave-NOMA systems under the analog beamforming structure, where needed to find the beamforming vector to steer toward two users and allocate appropriate power for two users.

However, in the above-mentioned mmWave NOMA networks, most of the works focus on the rate/reliability performance, but so far, its secrecy performance has not been fully investigated. In practical implementations, for mmWave NOMA networks in which eavesdroppers are randomly distributed, confidential messages can still be intercepted because eavesdroppers may exist in the signal beam. Therefore, providing a secure service is one of the most important tasks in the design and implementation of mmWave NOMA networks. In addition, compared with the fixed power allocation NOMA, the cognitive power allocation NOMA strategy for two users with different priorities can not only strictly satisfy the pre-defined QoS of high priority user, but also opportunistically serve low-priority user [19]. It can effectively utilize the system resources to meet the diversification requirements of users. Although NOMA has the potential to improve the overall performance of the system and has been studied in some communication systems, as far as we know, the application of cognitive power allocation in mmWave NOMA system has not been considered in the literature, where new challenges will arise for the secrecy performance of cognitive power allocation in mmWave NOMA networks.

In this paper, we specifically consider downlink mmWave NOMA networks with cognitive power allocation, where the transmitter provides opportunity service for secondary user while guaranteeing the QoS of the primary user with high priority. Different from the cognitive-radio-inspired NOMA networks introduced in [19], where the security is not considered, we take full account of the secrecy performance of primary and secondary users. Our analysis considers the key characteristics of mmWave channel and the influence of different transmitting power. In the light of the homogeneous Poisson point process (HPPP), a random number of eavesdroppers are randomly placed on the infinite two-dimension plane. For improving the secrecy performance of mmWave NOMA networks, a sector secrecy guard zone is introduced around the transmitter, in which eavesdroppers are not allowed to roam. Our diversified contributions and insights are listed as follows:

- We propose the secure NOMA transmission scheme of cognitive power allocation in mmWave wiretap networks, that is, the transmitter first dynamically allocates power to satisfy the QoS of the primary user m, and then uses the remaining power to serve the user n. A sector secrecy guard zone is invoked to improve PLS. Additionally, for reducing the complexity of channel sorting in mmWave NOMA, we select users from the internal sector and the external sector ring to perform NOMA transmission.
- Using stochastic geometry framework in proposed mmWave wiretap networks to characterize the random spatial locations of eavesdroppers and users. Taking into account the link blockages and directional beamforming, the closed-form expressions of SOP, COP and secrecy throughput (ST) are derived in the proposed scheme, which shows that both primary and secondary users can achieve better performance by introducing sector secrecy guard zone. Notably, the ST examines the reliability and secrecy performance in a unified manner in both NOMA and OMA.

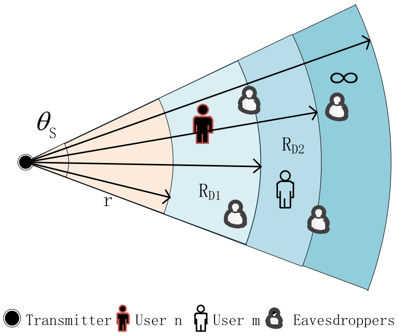

FIGURE 1. Network topology for the considered a mmWave NOMA wiretap network. A sector guard zone is employed to approximate the beamforming pattern, where r and θ_S are radius and central angle of sector guard zone, R_{D_1}, R_{D_2} and ∞ is the NOMA user zone for user n, NOMA user zone for user m, and an infinite two dimensional plane for eavesdroppers, respectively.

- We have investigated the performance of primary user and secondary user, it is shown that: 1) the primary user can get the same connection performance, while the secondary user can get better connection performance than OMA; 2) When the system parameters are reasonable set, the secondary user can achieve higher ST than OMA; 3) For primary and secondary users, there is an optimal power allocation design to maximize the ST. That is to say, an easy choice of transmit power is provided to achieve higher secrecy throughput for primary and secondary users. Moreover, the resulting analysis shows that blockages can be also utilized to improve secrecy performance.

The remainder of this paper is organized as follows. Section II presents the system model including user pairing strategy based on cognitive power allocation. Section III, we derive a set of the exact analytical expressions for the COP, SOP, and ST of primary and secondary users. Numerical and simulation results verified our theoretical analyses are presented in Section IV. Finally, we conclude this paper in Section V.

II. SYSTEM MODEL

A. NETWORK TOPOLOGY

Consider downlink mmWave wiretap networks scenario, which consists of one base station (BS), two different priority legitimate receivers denoted by m and n and spatial random distributed eavesdroppers, as shown in Fig.1. Particularly, the BS is located at the origin of a sector coverage area. We divide the sector coverage area into two regions, which are represented D_1 and D_2, respectively. The idea of using this topology hinges is to create a clearer channel quality differences between the paired users and reduce the complexity of channel sorting, similar topologies are used in [22]. The R_{D_1} represents the radius of the internal sector coverage area D_1, user n is randomly located in this region. D_2 is an external sector ring spanning the radius distance from R_{D_1} to R_{D_2}, user m is randomly located in this region. The eavesdroppers are randomly distributed on a finite two-dimensional plane, denoted by Φ_E, are modeled following an independent HPPP with the density λ_e. The BS is equipped multiple antennas and user n and m and eavesdroppers are equipped with a single antenna.

B. DIRECTIONAL BEAMFORMING

The BS is equipped with multiple antennas, so highly directional beamforming antenna arrays are deployed to perform directional beamforming to compensate for significant path losses at mmWave frequencies. For mathematical tractability, similar to [9]–[11], a sector model is used to analyze the beamforming pattern, particularly

$$G_S(\theta) = \begin{cases} M_S, & if\ |\theta| \le \theta_S, \\ m_S, & Otherwise, \end{cases} \tag{1}$$

where M_S represents the main lobe gain with the beam width θ_S, m_S represents the array gain of side lobe. We assume that the BS can get the perfect CSI of the users m and n, then it can trim its antenna steering orientation array to the users m and n to maximize the directional gain. In practical, estimating the CSI may be a nontrivial task, so our work actually provides an upper bound on achievable secrecy performance. Considering the characteristics of mmWave beam pattern, assuming that the BS can detect eavesdropping within a limited range, we model the finite range around the BS as a sector guard zone with radius r and central angle θ_S. We assume that the eavesdroppers have always been out of sector guard zone.

C. CHANNEL MODEL

According to the characteristics of mmWave in outdoor scenario, channels between BS and receivers can be LOS or NLOS [11]. The probability of a LOS with distance r_d is represented by $P_L(r_d)$, while the NLOS probability is $P_N(r_d)$. The probability $P_L(r_d)$ and $P_N(r_d)$ are given as $P_L(r_d) = e^{-\beta r_d}$ or $P_N(r_d) = 1 - e^{-\beta r_d}$, which can be acquired from stochastic blockage models or field measurements, where β is the blockage density. In light of the pass-loss model and small-scale fading presented in [28], we assume that each link follows independent Nakagami fading, $N_L(N_N)$ is the Nakagami fading parameter of the LOS (NLOS) link, which is assumed to be positive integer for simplicity. The channel gains received by the user m and n can be expressed as $M_S|h_i|^2 L(r_i), i \in \{m, n\}$ and the eavesdroppers can be expressed as $M_S|h_e|^2 L(r_e)$, where both $|h_i|^2$ and $|h_e|^2$ are normalized Gamma random variable with following $\Gamma\left(N_L, 1\big/N_L\right)$ and $\Gamma\left(N_N, 1\big/N_N\right)$, r_i denotes the distance from the BS to the user m or n, r_e denotes the distance from the BS to the eavesdroppers. $L(r_i)$ and $L(r_e)$ denote the path loss function which are modeled as $L\left(r_j\right) = C_L r^{-\alpha_L}$ or $L\left(r_j\right) = C_N r^{-\alpha_N}, j \in \{i, e\}$, r_j is the distance in meters, C_L and α_L are the constant and path loss exponent depending on the LOS, C_N and α_N depend on the NLOS.

D. NOMA SCHEME FOR mmWAVE NETWORKS

We consider a two-user transmission scheme for NOMA under cognitive power allocation. Recently, the 3GPP Long

Term Evolution Advanced (LTE-A) standard [36] includes a two-user NOMA scheme, where it is referred to as multiuser superposition transmission. We select one user n from the internal sector and another user m from the external sector ring, and use NOMA protocol to pair transmission in the same resource slot. Assuming that due to the high priority of the information of user m, the BS first guarantees the QoS of user m, that is, user m is the primary user. Under the condition of satisfying the QoS of user m, user n can be allowed to enter this channel.

According to the NOMA principle, the power allocation coefficients of user m and n are set to a_m and a_n respectively, $a_n + a_m = 1$. Considered that power allocation first ensures the QoS of user m, assuming the target date rate of user m is R_m, which implies that the selection of power allocation coefficients a_m and a_n need to satisfy the following constraint:

$$R_m \leq \log\left(1 + \frac{a_m P M_S |h_m|^2 L\left(r_m\right)}{a_n P M_S |h_m|^2 L\left(r_m\right) + \sigma_m^2}\right), \tag{2}$$

This means that the maximum transmission power coefficient allocated to user n is determined by

$$a_n = \max\left\{0, \frac{P M_s |h_m|^2 L\left(r_m\right) - \varepsilon_1 \sigma_m^2}{\left(\varepsilon_1 + 1\right) P M_s |h_m|^2 L\left(r_m\right)}\right\}. \tag{3}$$

where $\varepsilon_1 = 2^{R_m} - 1$, P denotes the total transmit power of the BS, σ_ϑ^2, $\vartheta \in \{m, n, e\}$ denotes the power of the additive white Gaussian noise. If $|h_m|^2 < \left(\varepsilon_1 \sigma_m^2 / P M_s L\left(r_m\right)\right), a_n = 0$. We can see that a_n in (3) is related to signal-to-interference-plus-noise ratio (SINR), the channel coefficient, target date rate and path loss of user m.

E. RECEIVED SINR

Since QoS of the user m can be guaranteed due to (2). In this case, the SINR at the user m is defined as

$$\gamma_m = \frac{a_m M_S P |h_m|^2 L\left(r_m\right)}{a_n M_S P |h_m|^2 L\left(r_m\right) + \sigma_m^2}, \tag{4}$$

In the light of the NOMA principle, user n implements SIC to first decode the signal intended for user m with SINR

$$\gamma_{n \to m} = \frac{a_m M_S P |h_n|^2 L\left(r_n\right)}{a_n M_S P |h_n|^2 L\left(r_n\right) + \sigma_n^2}, \tag{5}$$

If user n can successfully decode user m's signal intended, user n executes SIC and decodes its own signal with the following SINR

$$\gamma_n = \frac{a_n M_S P |h_n|^2 L\left(r_n\right)}{\sigma_n^2}, \tag{6}$$

We consider the worst case scenario, in which the eavesdroppers are assumed to have strong detection capabilities [25], [32], and can also use SIC to intercept confidential information. In fact, this assumption overestimates the multiuser decoding capability of eavesdroppers. In the scenario considered, the CSIs of the eavesdroppers are assumed to be unknown at the BS. The nearest eavesdropper is not necessarily the most detrimental one, but the one possessing the best channel to the transmitter. In addition, we consider non-colluding eavesdroppers in this treatise. The instantaneous SINR of detecting the information of the user n at the most detrimental eavesdropper is given by

$$\gamma_{e \to n} = \max_{E \in \phi_E}\left(\frac{a_n M_S P |h_e|^2 L\left(r_e\right)}{\sigma_e^2}\right), \tag{7}$$

Similar to user n, the instantaneous SINR of detecting the information of the user m at the most detrimental eavesdropper is given by

$$\gamma_{e \to m} = \max_{E \in \phi_E}\left(\frac{a_m M_S P |h_e|^2 L\left(r_e\right)}{a_n M_S P |h_e|^2 L\left(r_e\right) + \sigma_e^2}\right). \tag{8}$$

III. PERFORMANCE ANALYSIS

In this section, we analyze the COP, SOP, and ST of the paired users for the proposed NOMA scheme. In addition, the COP, SOP, and ST of paired users under OMA transmission based on slot dynamic division are given.

A. COP OF PROPOSED NOMA SCHEME

Based on the analysis in Sections II, the BS should first satisfy the QoS of user m, we present the result on the COP of the proposed NOMA scheme in the following theorem.

Theorem 1: Given that the BS allocates all power to user m, user m still cannot demodulate its signal correctly, and the COP event occurs. The COP of user m can be expressed by (9), as shown at the top of the next page, where $b = \sigma_m^2 / P M_s C_L$, $c = \sigma_m^2 / P M_s C_N$.

Proof: See Appendix A.

It can be deduced from ***Theorem 1*** that the COP of the user m is a decreasing function of the BS (P), which implies that the reliability performance of the user m is strengthened as P increases. Besides, decreasing the target date rate of user m (R_m) and the radius of the external sector ring D_2 (R_{D2}, R_{D1}) can reduce the COP of user m. It means that reducing R_m and the distance between user m and BS are conducive to improving the reliability without changing the transmission power.

Theorem 2: Considering the COP of user n, it can be divided into two parts, namely, the COP of user n when the connection of user m is interrupted, and the COP of user n when the connection of user m is succeeded. The COP of user n can be expressed by (11), $F_\kappa(x)$ as shown at the top of the next page, where R_n is the target date rate of user n, $a = \varepsilon_1 + \varepsilon_2\left(1 + \varepsilon_1\right)$, $\varepsilon_2 = 2^{R_n} - 1$.

Proof: See Appendix B.

According to ***Theorem 2***, the COP of user n decreases with the increase of power allocation factor. It means that when the system satisfies user m's QoS, more power is allocated to user n by increasing transmission power, which is beneficial to the improvement of user n's reliability. In addition,

$$\begin{aligned}
P_{co}^{m} &= \Pr\left(\frac{PM_S|h_m|^2L\left(r_m\right)}{\sigma_m^2} < 2^{R_m}-1\right) = \frac{2}{\left(R_{D2}^2-R_{D1}^2\right)}\sum_{i=0}^{\infty}\frac{(-1)^i}{i!}\\
&\times\left(\frac{\left(N_Lb\varepsilon_1\right)^{N_L+i}}{\left(N_L+i\right)\Gamma\left(N_L\right)}\times\frac{\Upsilon\left(\alpha_L\left(N_L+i\right)+2,\beta R_{D2}\right)-\Upsilon\left(\alpha_L\left(N_L+i\right)+2,\beta R_{D1}\right)}{\beta^{\alpha_L\left(N_L+i\right)+2}}+\frac{\left(N_Nc\varepsilon_1\right)^{N_N+i}}{\left(N_N+i\right)\Gamma\left(N_N\right)}\right.\\
&\times\left.\left(\frac{\Upsilon\left(\alpha_N\left(N_N+i\right)+2,\beta R_{D1}\right)-\Upsilon\left(\alpha_N\left(N_N+i\right)+2,\beta R_{D2}\right)}{\beta^{\alpha_N\left(N_N+i\right)+2}}+\frac{\left(R_{D2}\right)^{\alpha_N\left(N_N+i\right)+2}-\left(R_{D1}\right)^{\alpha_N\left(N_N+i\right)+2}}{\alpha_N\left(N_N+i\right)+2}\right)\right).
\end{aligned}\tag{9}$$

$$\begin{aligned}
F_\kappa\left(x\right) = &\sum_{j=0}^{\infty}\frac{2\times(-1)^j}{j!\left(R_{D2}^2-R_{D1}^2\right)}\left(\frac{\Upsilon\left(\alpha_L\left(N_L+j\right)+2,\beta R_{D2}\right)-\Upsilon\left(\alpha_L\left(N_L+j\right)+2,\beta R_{D1}\right)}{\left(N_L+j\right)\Gamma\left(N_L\right)\beta^{\alpha_L\left(N_L+j\right)+2}}\right.\\
&\times\left(\left(N_L\left(bx-b\varepsilon_1\right)\right)^{N_L+j}-\left(\frac{N_Lb\varepsilon_1\varepsilon_2\left(1+\varepsilon_1\right)}{x-\varepsilon_2\left(1+\varepsilon_1\right)}\right)^{N_L+j}\right)\\
&+\left(\frac{\Upsilon\left(\alpha_N\left(N_N+j\right)+2,\beta R_{D1}\right)-\Upsilon\left(\alpha_N\left(N_N+j\right)+2,\beta R_{D2}\right)}{\left(N_N+k_2\right)\Gamma\left(N_N\right)\beta^{\alpha_N\left(N_N+j\right)+2}}+\frac{\left(R_{D2}\right)^{\alpha_N\left(N_N+j\right)+2}-\left(R_{D1}\right)^{\alpha_N\left(N_N+j\right)+2}}{\left(N_N+k_2\right)\Gamma\left(N_N\right)\alpha_N\left(N_N+j\right)+2}\right)\\
&\times\left.\left(\left(N_N\left(bx-b\varepsilon_1\right)\right)^{N_N+j}-\left(\frac{N_Nb\varepsilon_1\varepsilon_2\left(1+\varepsilon_1\right)}{x-\varepsilon_2\left(1+\varepsilon_1\right)}\right)^{N_N+j}\right)\right),
\end{aligned}\tag{10}$$

$$\begin{aligned}
P_{co}^{n} &= P_{co}^{m}+\left(1-P_{co}^{m}\right)\times\Pr\left(\frac{a_mPM_S|h_n|^2L\left(r_n\right)}{a_nPM_S|h_n|^2L\left(r_n\right)+\sigma_n^2} < 2^{R_m}-1or\frac{a_nM_SP|h_n|^2L\left(r_n\right)}{\sigma_n^2} < 2^{R_n}-1\right)\\
&= 1-\left(1-P_{co}^{m}\right)\times\left(\frac{2F_\kappa\left(a\right)}{R_{D1}^2}\sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\left(\frac{\left(aN_Lb\right)^{N_L+k}}{\left(N_L+k\right)\Gamma\left(N_L\right)}\times\frac{\Upsilon\left(\alpha_L\left(N_L+k\right)+2,\beta R_{D1}\right)}{\beta^{\alpha_L\left(N_L+k\right)+2}}\right.\right.\\
&\quad+\left.\frac{\left(aN_Nb\right)^{N_N+k}}{\left(N_N+k\right)\Gamma\left(N_N\right)}\left(\frac{\left(R_{D1}\right)^{\alpha_N\left(N_N+k\right)+2}}{\alpha_N\left(N_N+k\right)+2}-\frac{\Upsilon\left(\alpha_N\left(N_N+k\right)+2,\beta R_{D1}\right)}{\beta^{\alpha_N\left(N_N+k\right)+2}}\right)\right)\\
&\quad-\frac{2(bN_L)^{N_L}}{R_{D1}^2\Gamma\left(N_L\right)}\sum_{k=0}^{\infty}\frac{(-\beta)^k}{k!}\int_a^\infty F_\kappa\left(x\right)x^{N_L-1}\frac{\Upsilon\left(\frac{\alpha_LN_L+k+2}{\alpha_L},bxN_LR_{D1}^{\alpha_L}\right)}{\alpha_L(bxN_L)^{\frac{\alpha_LN_L+k+2}{\alpha_L}}}dx\\
&\quad-\left.\frac{2(bN_N)^{N_N}}{R_{D1}^2\Gamma\left(N_N\right)}\int_a^\infty F_\kappa\left(x\right)\left(\frac{\Upsilon\left(\frac{\alpha_NN_N+2}{\alpha_N},bxN_NR_{D1}^{\alpha_N}\right)}{\alpha_N(bxN_N)^{\frac{\alpha_NN_N+2}{\alpha_N}}}-\sum_{k=0}^{\infty}\frac{(-\beta)^k}{k!}\times\frac{\Upsilon\left(\frac{\alpha_NN_N+k+2}{\alpha_L},bxN_NR_{D1}^{\alpha_N}\right)}{\alpha_N(bxN_N)^{\frac{\alpha_NN_N+k+2}{\alpha_N}}}\right)dx\right).
\end{aligned}\tag{11}$$

decreasing R_n and R_{D1} can reduce the COP of user n, this means that reducing R_n and the distance between user n and BS are conducive to improving the reliability without changing the transmission power.

B. SOP OF PROPOSED NOMA SCHEME

Theorem 3: Assuming that the eavesdroppers can decode confidential information from BS by applying multiuser detection techniques. The SOP of user n can be given by

$$\begin{aligned}
P_{so}^{n} &= \Pr\left(\gamma_{e\to n} > 2^{R_n-R_n^s}-1\right) = \int_{2^{R_n-R_n^s}-1}^{\infty}f_{\gamma_{e\to n}}\left(x\right)dx\\
&= 1-\exp\left(-\theta_s\lambda_e\left(-A_1\times B_1+A_2-B_2-C_1+D_1\times E_1\right)\right),
\end{aligned}\tag{12}$$

where

$$A_1 = \sum_{n_1=0}^{\infty}\frac{(-1)^{n_1}\left(N_Lxb\right)^{N_L+n_1}\Gamma\left(\alpha_L\left(N_L+n_1\right)+2,\beta r\right)}{n_1!\left(N_L+n_1\right)\Gamma\left(N_L\right)\beta^{\alpha_L\left(N_L+n_1\right)+2}},$$

$$A_2 = \frac{\left(N_N-1\right)!}{\Gamma\left(N_N\right)}\sum_{n_2=0}^{N_N-1}\frac{\Gamma\left(\frac{\alpha_Nn_2+2}{\alpha_L},\left(\varepsilon_1+1\right)N_Nxbr^{\alpha_N}\right)}{n_2!\alpha_N\left(\left(\varepsilon_1+1\right)N_Nxb\right)^{\frac{\alpha_Nn_2+2}{\alpha_N}}}.$$

R_n^s is the secrecy rate of the user n.

$$\begin{aligned}
Q_1 = &\frac{2\times(-1)^p\left(N_Lb\varepsilon_1\left(\varepsilon_1+1\right)\right)^{N_L+p}}{\left(R_{D2}^2-R_{D1}^2\right)p!\left(N_L+p\right)\Gamma\left(N_L\right)}\\
&\times\frac{\Upsilon\left(\alpha_L\left(N_L+p\right)+2,\beta R_{D2}\right)-\Upsilon\left(\alpha_L\left(N_L+p\right)+2,\beta R_{D1}\right)}{\beta^{\alpha_L\left(N_L+p\right)+2}},
\end{aligned}$$

here $\Upsilon(\cdot,\cdot)$ is the lower incomplete gamma function [29] and its expansion [Eq.(8.352)]

$$D_1=\sum_{n_4=0}^{\infty}\frac{(-1)^{n_4}(N_N xb)^{N_N+n_4}\Gamma\left(\alpha_N\left(N_N+n_4\right)+2,\beta r\right)}{n_4!\left(N_N+n_4\right)\Gamma\left(N_N\right)\beta^{\alpha_N\left(N_N+n_4\right)+2}},$$

and $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function [29] and its expansion [Eq.(8.352)],

$$\begin{aligned}Q_2=&\frac{2\times(-1)^q(N_N c\varepsilon_1\left(\varepsilon_1+1\right))^{N_N+q}}{q!\left(R_{D2}^2-R_{D1}^2\right)\left(N_N+q\right)\Gamma\left(N_N\right)}\\&\times\left(\frac{\Upsilon\left(\alpha_N\left(N_N+q\right)+2,\beta R_{D1}\right)-\Upsilon\left(\alpha_N\left(N_N+q\right)+2,\beta R_{D2}\right)}{\beta^{\alpha_N\left(N_N+q\right)+2}}\right.\\&\left.+\frac{\left(R_{D2}\right)^{\alpha_N\left(N_N+q\right)+2}-\left(R_{D1}\right)^{\alpha_N\left(N_N+q\right)+2}}{\alpha_N\left(N_N+q\right)+2}\right).\end{aligned}$$

The parametersB_1,B_2, C_1, E_1 of the (12) are shown in (13), as shown at the top of the next page.

Proof: See Appendix C.

According to ***Theorem 3***, the SOP of user n increases with the enlargement of power allocation factor a_n, which means that when the system satisfies user m's QoS, increasing transmission power may lead to more confidential information of user n leaking to eavesdroppers. Moreover, increasing r can reduce the SOP of user n.

Theorem 4: Assuming that the eavesdroppers can decode confidential information from BS by applying multiuser detection techniques. The SOP of user m can be given by

$$\begin{aligned}&P_{so}^m\\&=\Pr\left(\gamma_{e\to m}>2^{R_m-R_m^s}-1\right)=\int_{2^{R_m-R_m^s}-1}^{\infty}f_{\gamma_{e\to m}}(x)dx\\&=1-\exp\left(-\theta_s\lambda_e\left(-A_3\times B_3+A_4-B_4-C_2\times D_2+E_2\right)\right),\end{aligned}\tag{14}$$

where

$$A_4=\frac{\left(N_N-1\right)!}{\Gamma\left(N_N\right)}\sum_{t_2=0}^{N_N-1}\frac{\Gamma\left(\frac{\alpha_N t_2+2}{\alpha_N},\frac{(\varepsilon_1+1)N_N xbr^{\alpha_N}}{(\varepsilon_1-x)}\right)}{t_2!\alpha_N\left(\frac{(\varepsilon_1+1)N_N xb}{(\varepsilon_1-x)}\right)^{\frac{\alpha_N t_2+2}{\alpha_N}}},$$

$$\begin{aligned}C_2=&\frac{\left(N_N-1\right)!}{\Gamma\left(N_N\right)}\sum_{t_2=0}^{N_N-1}\sum_{w_3}^{\frac{\alpha_N t_2+2}{\alpha_N}-1}\\&\times\frac{\left(\alpha_N t_2+2\right)\left(\frac{\alpha_N t_2+2}{\alpha_N}-1\right)!\left(1+x\right)r^{\alpha_N w_3}}{t_2!\alpha_N^2 w_3!(N_N xb)^{\frac{\alpha_N t_2+2}{\alpha_N}-w_3}},\end{aligned}$$

R_m^s is the secrecy rate of the user m. The parameters A_3, B_3, B_4, D_2, E_2 of the (14) are shown in (15), as shown at the top of the 8th page.

Proof: See Appendix D.

It can be deduced from ***Theorem 4*** that the SOP of user m increases with the enlargement of transmitting power, which means that when the system transmits more power to satisfy user m's QoS, it also increases the possibility of leakage of confidential information. Moreover, increasing r can reduce the SOP of user m.

C. ST OF PROPOSED NOMA SCHEME

The ST represents the average secrecy rate when information is both secure and reliable transmitted.

Theorem 5: From the point of view of the user m and the most malicious eavesdropper, system performance is investigated, which represents the probability of reliable and secure transmission. The ST of user m is given by

$$\begin{aligned}\eta^m&=R_m^s\Pr\left(\log\left(1+\gamma_{e\to m}\right)<\left(R_m-R_m^s\right)\right)\\&=R_m^s\Pr\left(\max_{E\in\phi_E}\left(\frac{a_m M_S P|h_e|^2L\left(r_e\right)}{a_n M_S P|h_e|^2L\left(r_e\right)+\sigma_e^2}\right)<\varepsilon_3\right)\\&=R_m^s\exp\left(\theta_s\lambda_e\left(A_5\times B_3-A_6+B_5+C_3\times D_3-E_2\right)\right),\end{aligned}\tag{16}$$

where $\varepsilon_3=2^{\left(R_m-R_m^s\right)}-1, A_5, A_6, B_5, C_3, D_3$ can be obtained by substituting ε_3 for x of A_3, A_4, B_4, C_2, D_2.

Proof: See Appendix E.

According to ***Theorem 5***, since user m has a higher priority, the system must allocate more power to satisfy its QoS requirements first, which may lead to information leakage to eavesdroppers. Therefore, for user m's ST, the main consideration is the optimal power allocation. Moreover, increasing r can enlarge the ST of user m.

Theorem 6: From the point of view of the user n and the most malicious eavesdropper, system performance is investigated, which represents the probability of reliable and secure transmission. The ST of user n is given by (17), as shown at the bottom of the 9th page, where $\varepsilon_4=2^{\left(R_n-R_n^s\right)}-1$.

Proof: See Appendix F.

According to ***Theorem 6***, with the increasing of transmitting power, the ST of user n increases, which means that when the system transmits more power to satisfy user m's QoS, user n can also be served, but at the same time, it increases the possibility of leaking confidential information to eavesdroppers. Therefore, there is also an optimal power allocation for user n. In addition, adding r can increase the ST of user n.

D. OMA TRANSMISSION BASED ON SLOT DYNAMIC DIVISION

In order to make a fair comparison with the proposed NOMA scheme, without loss of generality, Time Division Multiple Access (TDMA) is used as the representative of OMA. Similar to the cognitive power allocation strategy in the proposed NOMA scheme, in OMA, according to the QoS requirements of the primary user m, we divide a slot dynamically, when the primary user m satisfies its QoS, the remaining part of the time slot is allocated to the user n. Specifically, a portion of the whole time slot, expressed as α, $0<\alpha\leq 1$, is allocated to satisfy user m. if $\alpha\neq 1$, the remaining time $(1-\alpha)$ will be allocated to user n. Similar OMA policy is presented in [13].

Similar to (2), in order to satisfy the QoS requirements of user m in the OMA scheme considered, the time allocation factor α must satisfy the following constraints:

$$R_m\leq\alpha\log\left(1+\frac{PM_S|h_m|^2L\left(r_m\right)}{\sigma_m^2}\right),\tag{18}$$

$$
\begin{aligned}
B_1 &= \left(\sum_{p=0}^{\infty} (N_L+p) \times \frac{Q_1\left(n_1-p+2+u_1\right)\left(\varepsilon_1+1\right)^{n_1-p+2}}{\sum\limits_{u_1=0}^{N_L+p+1} \binom{N_L+p+1}{u_1} (-1)^{u_1}} \right. \\
&\quad \left. + \sum_{q=0}^{\infty} (N_N+q) \times \frac{Q_2\left(N_L+n_1-N_N-q+2+l_1\right)\left(\varepsilon_1+1\right)^{N_L+n_1-N_N-q+2}}{\sum\limits_{l_1=0}^{N_N+q+1} \binom{N_N+q+1}{l_1} (-1)^{l_1}} \right), \\
B_2 &= \sum_{n_2=0}^{N_N-1} \frac{(N_N-1)!\, r^{\alpha_N n_2+2}}{n_2!\,\alpha_N \Gamma\left(N_N\right)} \left(\sum_{p=0}^{\infty} \frac{Q_1 \Gamma\left(\left(n_5-N_L-p\right), \left(\varepsilon_1+1\right) N_N x b r^{\alpha_N}\right)\left(-\left(\varepsilon_1+1\right)\right)^{-n_5}}{\left(N_N x b r^{\alpha_N}\right)^{n_5-N_L-p} \sum\limits_{n_5=0}^{N_L+p} \binom{N_L+p}{n_5}} \right. \\
&\quad \left. + \sum_{q=0}^{\infty} \frac{Q_2 \Gamma\left(\left(n_6-N_N-q\right), \left(\varepsilon_1+1\right) N_N x b r^{\alpha_N}\right)\left(-\left(\varepsilon_1+1\right)\right)^{-n_6}}{\left(N_N x b r^{\alpha_N}\right)^{n_6-N_N-q} \sum\limits_{n_6=0}^{N_n+q} \binom{N_N+q}{n_6}} \right), \\
C_1 &= \frac{(N_N-1)!}{\Gamma\left(N_N\right)} \sum_{n_2=0}^{N_N-1} \sum_{n_3=0}^{\frac{\alpha_N n_2+2}{\alpha_N}-1} \frac{\left(\alpha_N n_2+2\right)\left(\frac{\alpha_N n_2+2}{\alpha_N}-1\right)!}{n_2!\,\alpha_N^2 n_3!} \left(N_N x b\right)^{-\frac{\alpha_N n_2+2}{\alpha_N}+n_3} r^{\alpha_N n_3} \\
&\quad \times \left(\sum_{p=0}^{\infty} \frac{Q_1 (\varepsilon_1+1)^{-n_7} \Gamma\left(\left(n_7+n_3-N_L-p-\frac{\alpha_N n_2+2}{\alpha_N}\right), \left(\varepsilon_1+1\right) N_N x b r^{\alpha_N}\right)}{\left(N_N x b r^{\alpha_N}\right)^{n_7-N_L-p+n_3+\frac{\alpha_N n_2+2}{\alpha_N}} \sum\limits_{n_5=0}^{N_L+p} \binom{N_L+p}{n_7} (-1)^{n_7}} \right. \\
&\quad \left. + \sum_{q=0}^{\infty} \frac{Q_2 (\varepsilon_1+1)^{-n_8} \Gamma\left(\left(n_8+n_3-N_N-q-\frac{\alpha_N n_2+2}{\alpha_N}\right), \left(\varepsilon_1+1\right) N_N x b r^{\alpha_N}\right)}{\left(N_N x b r^{\alpha_N}\right)^{n_8-N_N-q+n_3+\frac{\alpha_N n_2+2}{\alpha_N}} \sum\limits_{n_8=0}^{N_N+q} \binom{N_N+q}{n_8} (-1)^{n_8}} \right), \\
E_1 &= \sum_{p=0}^{\infty} \frac{(N_L+p)\, Q_1\left(N_N+n_4-N_L-p+2+u_2\right)}{\sum\limits_{u_2=0}^{N_L+p+1} \binom{N_L+p+1}{u_2} (-1)^{u_2} (\varepsilon_1+1)^{N_L-N_N-n_4+p-2}} + \sum_{q=0}^{\infty} \frac{(N_N+q) \times Q_2\left(n_4-q+2+l_2\right)}{\sum\limits_{l_2=0}^{N_N+q+1} \binom{N_N+q+1}{l_2} (-1)^{l_2} (\varepsilon_1+1)^{q-n_4-2}}.
\end{aligned} \tag{13}
$$

Therefore the slot division factor α can be set as follows:

$$
\alpha = \min \left\{ 1, \frac{R_m}{\log\left(1+\frac{PM_S|h_m|^2 L(r_m)}{\sigma_m^2}\right)} \right\}, \tag{19}
$$

From (18), we find that α is related to the channel coefficient, path loss and target rate of user m.

Given that the BS allocates the whole time to user m, user m still cannot demodulate its signal correctly, and the COP event occurs. The COP of user m can be given by

$$
P_{co}^{O-m} = \Pr\left(\log\left(1+\frac{PM_S|h_m|^2 L\left(r_m\right)}{\sigma_m^2}\right) < R_m \right), \tag{20}
$$

Considering the COP of user n, it can be divided into two parts, namely, the COP of user n when the connection of user m is interrupted, and the COP of user n when the connection of user m is succeeded. The COP of user n can be given by

$$
\begin{aligned}
P_{co}^{O-n} &= P_{co}^{O-m} + \left(1-P_{co}^{O-m}\right) \\
&\quad \times \Pr\left((1-\alpha)\, log\left(1+\frac{M_S P|h_n|^2 L\left(r_n\right)}{\sigma_n^2}\right) < R_n \right),
\end{aligned} \tag{21}
$$

$$
\begin{aligned}
A_3 &= \sum_{t_1=0}^{\infty} \frac{(-1)^{t_1}(N_L xb)^{N_L+t_1}\Gamma\left(\alpha_L\left(N_L+t_1\right)+2,\beta r\right)}{t_1!\left(N_L+t_1\right)\Gamma\left(N_L\right)\beta^{\alpha_L(N_L+t_1)+2}\sum\limits_{w_1=0}^{N_L+t_1}\binom{N_L+t_1}{w_1}\left(-(1-x)\right)^{w_1}},\\
B_3 &= \sum_{p=0}^{\infty}(N_L+p)\times Q_1\times\frac{\left(w_1-N_L-p+2+u_2\right)\left(\varepsilon_1+1\right)^{w_1-N_L-p+2}}{\sum\limits_{u_2=0}^{N_L+p+1}\binom{N_L+p+1}{u_2}(-1)^{u_2}}\\
&\quad+\sum_{q=0}^{\infty}(N_N+q)\times Q_2\times\frac{\left(w_1-N_N-q+2+l_2\right)\left(\varepsilon_1+1\right)^{w_1-N_N-q+2}}{\sum\limits_{l_2=0}^{N_N+q+1}\binom{N_N+q+1}{l_2}(-1)^{l_2}},\\
B_4 &= \frac{(N_N-1)!}{\Gamma\left(N_N\right)}\\
&\quad\times\sum_{t_2=0}^{N_N-1}\frac{r^{\alpha_N t_2+2}}{t_2!\alpha_N}\left(\sum_{p=0}^{\infty}\frac{Q_1\sum\limits_{w_4=1}^{\infty}\sum\limits_{w_5=0}^{N_L+p+w_4-n_5-1}\binom{N_L+p+w_4-n_5-1}{w_5}\Gamma\left(w_5+n_5-N_L-p-w_4,N_N xbr^{\alpha_N}\right)}{\sum\limits_{n_5=0}^{N_L+p}\binom{N_L+p}{n_5}\left(\varepsilon_1+1\right)^{n_5}(1+x)^{N_L+p-n_5}(-1)^{-N_L-p-3w_4+3+2n_5+w_5}\left(N_N xbr^{\alpha_N}\right)^{-N_L-p-w_4+w_5+n_5}}\right.\\
&\quad\left.+\sum_{q=0}^{\infty}\frac{Q_2\sum\limits_{w_4=1}^{\infty}\sum\limits_{w_6=0}^{N_N+q+w_4-n_6-1}\binom{N_N+q+w_4-n_6-1}{w_6}\Gamma\left(w_6+n_6-N_N-q-w_4,N_N xbr^{\alpha_N}\right)}{\sum\limits_{n_6=0}^{N_N+q}\binom{N_N+q}{n_6}\left(\varepsilon_1+1\right)^{n_6}(1+x)^{N_N+q-n_6}(-1)^{-N_N-q-3w_4+3+2n_6+w_6}\left(N_N xbr^{\alpha_N}\right)^{-N_N-q-w_4+w_6+n_6}}\right),\\
D_2 &= \left(\sum_{p=0}^{\infty}\frac{Q_1\sum\limits_{w_7=1}^{\frac{\alpha_N t_2+2}{\alpha_N}-1-w_3}\binom{\frac{\alpha_N t_2+2}{\alpha_N}-1-w}{w_7}\sum\limits_{w_8=0}^{N_L+p+w_7-n_5}\binom{N_L+p+w_7-n_5}{w_8}\Gamma\left(w_8+n_5-N_L-p-w_7-1,N_N xbr^{\alpha_N}\right)}{\sum\limits_{n_5=0}^{N_L+p}\binom{N_L+p}{n_5}\left(\varepsilon_1+1\right)^{n_5}(1+x)^{N_L+p+1-n_5}(-1)^{-N_L-p-2w_7+2n_5+w_8}\left(N_N xbr^{\alpha_N}\right)^{-N_L-p-w_7+w_8+n_5-1}}\right.\\
&\quad\left.+\sum_{p=0}^{\infty}\frac{Q_1\sum\limits_{w_7=1}^{\frac{\alpha_N t_2+2}{\alpha_N}-1-w_3}\binom{\frac{\alpha_N t_2+2}{\alpha_N}-1-w}{w_7}\sum\limits_{w_9=0}^{N_N+p+w_7-n_6}\binom{N_N+p+w_7-n_6}{w_9}\Gamma\left(w_9+n_6-N_N-p-w_7-1,N_N xbr^{\alpha_N}\right)}{\sum\limits_{n_6=0}^{N_N+p}\binom{N_N+p}{n_6}\left(\varepsilon_1+1\right)^{n_6}(1+x)^{N_N+p+1-n_6}(-1)^{-N_N-p-2w_7+2n_6+w_9}\left(N_N xbr^{\alpha_N}\right)^{-N_N-p-w_7+w_9+n_6-1}}\right),\\
E_2 &= \sum_{t_3=0}^{\infty}\frac{(-1)^{t_3}(N_N xb)^{N_N+t_3}\Gamma\left(\alpha_N\left(N_N+t_3\right)+2,\beta r\right)}{t_3!\left(N_N+t_3\right)\Gamma\left(N_N\right)\beta^{\alpha_N(N_N+t_3)+2}}\times\left(\sum_{p=0}^{\infty}\frac{(N_L+p)\times Q_1\times\left(u_3-N_L-p+2+u_2\right)\left(\varepsilon_1+1\right)^{u_3-N_L-p+2}}{\sum\limits_{u_3=0}^{N_N+t_3}\binom{N_N+t_3}{u_3}\sum\limits_{u_2=0}^{N_L+p+1}\binom{N_L+p+1}{u_2}(-1)^{u_2+u_3}(x+1)^{u_3}}\right.\\
&\quad\left.\left.+\sum_{q=0}^{\infty}\frac{(N_N+q)\times Q_2\times\left(u_3-N_N-q+2+l_2\right)\left(\varepsilon_1+1\right)^{u_3-N_N-q+2}}{\sum\limits_{u_3=0}^{N_N+t_3}\binom{N_N+t_3}{u_3}\sum\limits_{l_2=0}^{N_N+q+1}\binom{N_N+q+1}{l_2}(-1)^{l_2+u_3}(x+1)^{u_3}}\right)\right). \qquad (15)
\end{aligned}
$$

Assuming that the eavesdroppers can decode confidential information from BS by applying multiuser detection techniques. The SOP of user m can be given by

$$
\begin{aligned}
&P_{so}^{O-m}\\
&=\Pr\left(\max\left(\alpha\log\left(1+\frac{PM_S|h_e|^2L\left(r_e\right)}{\sigma_e^2}\right)\right)>\left(R_m-R_m^s\right)\right),
\end{aligned} \qquad (22)
$$

Assuming that the eavesdroppers can decode confidential information from BS by applying multiuser detection techniques. The SOP of user n can be given by

$$
\begin{aligned}
&P_{so}^{O-n}\\
&=\Pr\left(\max\left((1-\alpha)\log\left(1+\frac{PM_S|h_e|^2L(r_e)}{\sigma_e^2}\right)\right)>\left(R_n-R_n^s\right)\right),
\end{aligned} \qquad (23)
$$

From the point of view of the user m and the most malicious eavesdropper, system performance is investigated, which represents the probability of reliable and secure transmission. The ST of user m is given by

$$\eta_m^O = R_m^s \Pr\left(\max\left(\alpha \log\left(1+\frac{PM_S|h_e|^2L\left(r_e\right)}{\sigma_e^2}\right)\right) < \left(R_m - R_m^s\right)\right), \tag{24}$$

From the point of view of the user n and the most malicious eavesdropper, system performance is investigated, which represents the probability of reliable and secure transmission. The ST of user n is given by

$$\begin{aligned}\eta_n^O &= R_n^s \Pr\left(\left(1-\alpha\right) log\left(1+\frac{M_SP|h_n|^2L\left(r_n\right)}{\sigma_n^2}\right) > R_n\,,\right.\\ &\quad \left(\max\left(\left(1-\alpha\right)\log\left(1+\frac{PM_S|h_e|^2L\left(r_e\right)}{\sigma_e^2}\right)\right)\right.\\ &\quad \left.\left.< \left(R_n - R_n^s\right)\right), \alpha \neq 1\right). \end{aligned} \tag{25}$$

IV. NUMERICAL RESULTS

In this section, numerical results of the proposed NOMA scheme are presented and compared with those of the OMA scheme. We assume that the thermal noise power is -90 dBm, and consider the carrier frequency at 28 GHz. According to [30], the parameters of Nakagami fading in the LOS (NLOS) link are $N_L = 3$ ($N_N = 2$), the path-loss model: $\beta_L = 61.4dB$, $\alpha_L = 2$, $\beta_N = 72dB$, $\alpha_N = 2.92$. $C_L = 10^{-\frac{\beta_L}{10}}$ and $C_N = 10^{-\frac{\beta_N}{10}}$ can be regarded as path-loss intercepts on the reference distance of LOS and NLOS links. BPCU is the abbreviation for bit per channel use.

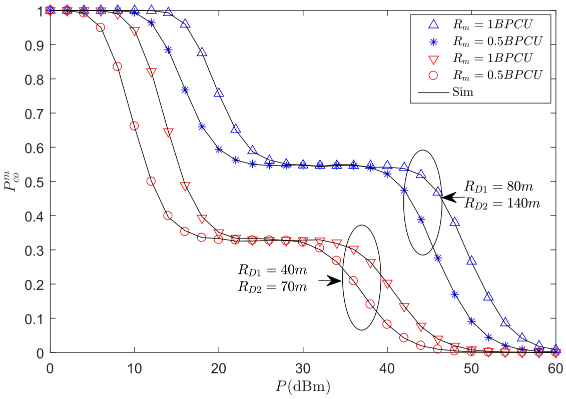

FIGURE 2. The P_{co}^m versus P with $\lambda_E = 0.0002$ *nodes*/m^2, $r = 140m$, $\theta_S = \frac{\pi}{3}$, $m_S = 0.1$ and $M_S = 200$.

Fig. 2 presents the COP of the user m versus the transmit power P at different user m's zone radius and target date rates R_m. The simulation (Sim) results are in good agreement with analytical (Ana) results, which verifies the performance analysis. As P increases, the COP decreases gradually under the given r. And there is one floor in the process, this is because the transmit power has different effects on the COP of LOS and NLOS. For different target data rate requirements of user m, the required transmit power is also different, and the transmit power required for small target data rate is also small, and vice versa. In addition, reducing COP can be achieved by

$$\begin{aligned}\eta^n &= R_n^s \Pr\left(\log\left(1+\gamma_n\right) > R_n, \log\left(1+\gamma_{e\to n}\right) < \left(R_n - R_n^s\right), |h_m|^2 > \frac{\varepsilon_1\sigma_m^2}{PM_sL\left(r_m\right)}\right)\\ &= R_n^s \int_0^{\frac{1}{\varepsilon_1+1}} \left(1-\frac{2}{R_{D1}^2}\left(\sum_{i=0}^{\infty}\frac{(-1)^i\left(\frac{\varphi_L\varepsilon_2N_L}{a_n}\right)^{N_L+i}\Upsilon\left(\alpha_L\left(N_L+i\right)+2, \beta R_{D1}\right)}{i!\left(N_L+i\right)\Gamma\left(N_L\right)\beta^{\alpha_L\left(N_L+i\right)+2}}\right.\right.\\ &\quad \left.\left.+\sum_{j=0}^{\infty}\frac{(-1)^j\left(\frac{\varphi_N\varepsilon_2N_N}{a_n}\right)^{N_N+j}}{j!\left(N_N+j\right)\Gamma\left(N_N\right)}\left(\frac{\left(R_{D1}\right)^{\alpha_N\left(N_N+j\right)+2}}{\alpha_N\left(N_N+j\right)+2}-\frac{\Upsilon\left(\alpha_N\left(N_N+j\right)+2, \beta R_{D1}\right)}{\beta^{\alpha_N\left(N_N+j\right)+2}}\right)\right)\right)\\ &\quad \times\left(\sum_{p=0}^{\infty}\frac{Q_1\left(N_L+p\right){a_n}^{N_L+p-1}}{\left(1-a_n\left(\varepsilon_1+1\right)\right)^{N_L+p+1}}+\sum_{q=0}^{\infty}\frac{Q_2\left(N_N+q\right){a_n}^{N_N+q-1}}{\left(1-a_n\left(\varepsilon_1+1\right)\right)^{N_N+q+1}}\right)\\ &\quad \times\exp\left(-\theta_s\lambda_e\left(-\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\varphi_L\varepsilon_4N_L}{a_n}\right)^{N_L+n}\Gamma\left(\alpha_L\left(N_L+n\right)+2, \beta r\right)}{n!\left(N_L+n\right)\Gamma\left(N_L\right)\beta^{\alpha_L\left(N_L+n\right)+2}}\right.\right.\\ &\quad \left.\left.+\frac{\left(N_N-1\right)!}{\Gamma\left(N_N\right)}\sum_{m=0}^{N_N-1}\frac{\left(\varphi_N\varepsilon_4N_N\right)^m}{a_n^{-\frac{2}{\alpha_N}}m!}\times\frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}, \frac{\varphi_N\varepsilon_4N_Nr^{\alpha_N}}{a_n}\right)}{\alpha_N\left(\varphi_N\varepsilon_4N_N\right)^{\frac{m\alpha_N+2}{\alpha_N}}}+\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\varphi_N\varepsilon_4N_N}{a_n}\right)^{N_N+n}}{n!\left(N_N+n\right)\Gamma\left(N_N\right)}\frac{\Gamma\left(\alpha_N\left(N_N+n\right)+2, \beta r\right)}{\beta^{\alpha_N\left(N_N+n\right)+2}}\right)\right)da_n \end{aligned} \tag{17}$$

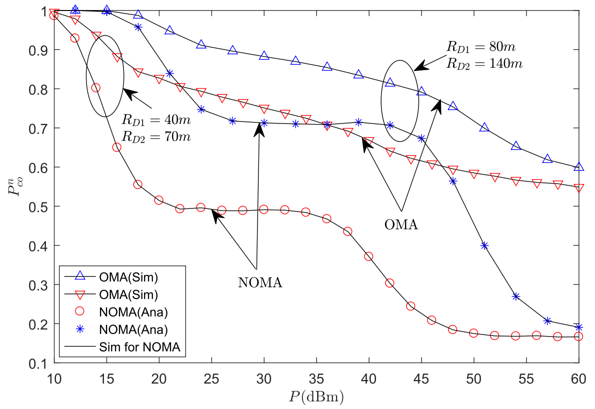

FIGURE 3. The P^n_{co} versus P with $\lambda_E = 0.0002$ *nodes*/m^2, $r = 140m$, $\theta_S = \frac{\pi}{3}$, $R_m = 1$ BPCU, $R_n = 0.4$ BPCU, $m_S = 0.1$ and $M_S = 200$.

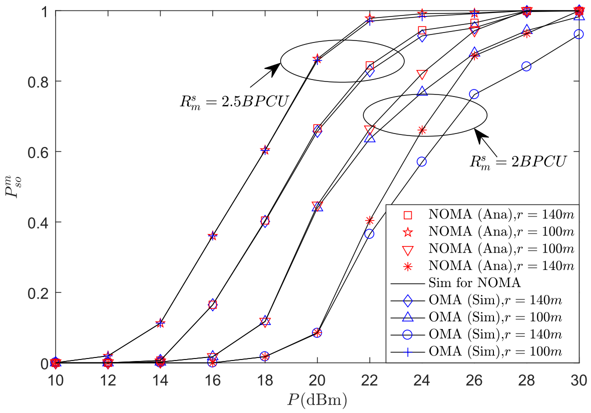

FIGURE 4. The P^m_{so} versus P with $\lambda_E = 0.0002$ *nodes*/m^2, $R_m = 3$ BPCU, $R_{D1} = 40m$, $R_{D2} = 70m$, $\theta_S = \frac{\pi}{3}$, $m_S = 0.1$ and $M_S = 200$.

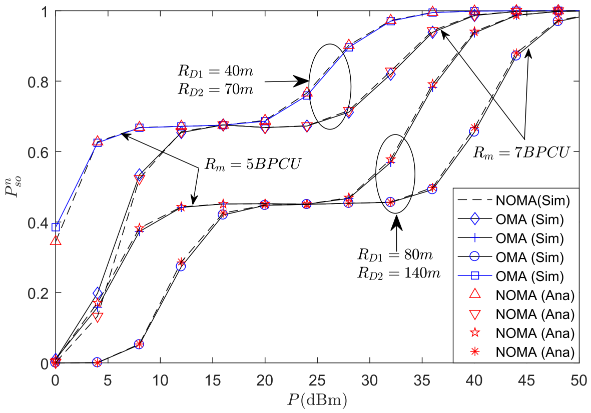

FIGURE 5. The P^n_{so} versus P with $\lambda_E = 0.0002$ *nodes*/m^2, $R_n = 3$ BPCU, $R^s_n = 1.5$ BPCU, $r = 50m$, $\theta_S = \frac{\pi}{3}$, $m_S = 0.1$ and $M_S = 200$.

reducing the zone radius of user m, this is because the smaller user m's zone will lead to a lower path-loss. It is noteworthy that user m has the same COP in NOMA and OMA schemes.

Fig. 3 presents the COP of the user n versus the transmit power P at different user n's zone radius. As the primary user, whether it is the proposed NOMA scheme or the OMA scheme, the QoS requirements of user m must be satisfied first. It can be observed that the COP of user n decreases gradually with the increase of P at a given r. Specifically, the smaller the radius of user zone, the better the connection performance will be. In addition, the performance gap between the proposed NOMA scheme and OMA scheme in a smaller user zone radius is significantly expansion than that in a larger user zone radius when the transmission power is not too high. From Fig.3, it can be also seen that the proposed NOMA scheme achieves better connection performance than that of OMA for the user n. This conclusion is similar to that obtained in [25] under fixed power allocation in downlink NOMA in multi-cell mmWave networks. At the same time, it is similar to the conclusion of [17] in microwave networks. In addition, there is also one floor in the process because the transmit power has different effects on the COP of the LOS and NLOS.

Fig. 4 presents the effects of the SOP of the user m versus the transmit power P with the different secrecy guard zone radius r and secrecy rate R^s_m. We can see that, in a given user zone, the SOP increases rapidly with increasing P. Note that, the proposed NOMA scheme has a slightly worse secrecy outage performance than OMA in high transmission power regions under the designed parameters. Another observation is that for both schemes, the greater the secrecy redundancy rate and secrecy guard zone radius, the better the secrecy performance of the system.

Fig. 5 plots the SOP of user n versus the transmit power P with the different user zone radius and target date rates R_m. It is obvious that the SOP of user n increases with the increasement of P. And there is one floor in the process, this is because the transmit power has different effects on the SOP of LOS and NLOS. We observe that the proposed NOMA scheme and OMA scheme have almost the same secrecy outage performance for user n. Specifically, in the low transmission power regions, NOMA is slightly better than OMA, while in the high transmission power regions, the opposite is true. In addition, we also see that the larger the radius of user zone, the better the secrecy performance of user n. This is because, with the increase of user zone radius, the power allocated to user m will enlarge to satisfy its QoS. Correspondingly, the power allocated by user n will decrease. Given secrecy guard zone radius, user n has better secrecy performance in small user zone radius than in large user zone radius. Similarly, the higher the target rate of user m, the better the secrecy performance of user n.

Fig. 6 presents the effects of transmit power on the ST for user m with different radius of secrecy guard zone. We note that there is an optimal transmit power that maximizes the ST of user m. That is to say, the proposed NOMA scheme exists an optimal transmit power allocation factor and the OMA scheme exists an optimal slot division factor, which can maximize the ST of user m. In Fig. 6, given the radius of the user zone, the ST of the user m increases with the expansion of the radius of the secrecy guard zone. Another important

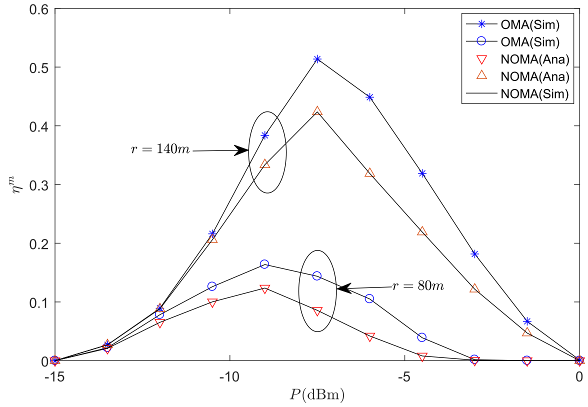

FIGURE 6. The η^m versus P with $R_m = 3$ BPCU, $R_m^s = 2$ BPCU, $R_{D1} = 40m$, $R_{D2} = 70m$, $\lambda_E = 0.0002$ *nodes*/m^2, $m_S = 0.1$ and $M_S = 200$.

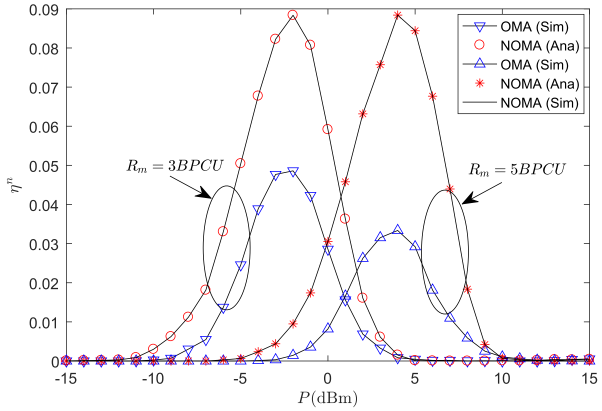

FIGURE 7. The η^n versus P with $R_m^s = 0.5$ BPCU, $R_n^s = 0.3$ BPCU, $R_{D1} = 40m$, $R_{D2} = 70m$, $\lambda_E = 0.0002$ *nodes*/m^2, $r = 80m$, $m_S = 0.1$ and $M_S = 200$.

observation is that user m's ST at OMA is superior to the proposed NOMA scheme regardless of how the secrecy guard zone changes. This is because, as the primary user, user m has the same COP under the two schemes. As can be seen from Fig. 4, user m's secrecy outage performance is slightly better than the proposed NOMA scheme.

Fig. 7 presents the effects of the ST for user n versus the transmit power P with the different target date rates R_m. We note that there is an optimal transmit power to maximize the ST of user n. It means that there are optimal power allocation factor and slot division factor in the proposed NOMA and OMA schemes, respectively, so that the ST of user n can reach the maximum value. Furthermore, the figure shows that the ST of user n can be significantly improved by using NOMA compared with OMA. For example, the ST of user n under the NOMA scheme is nearly three times as high as that of the OMA scheme when the transmission power is $P = 5\ dBm$ and $R_m = 5$BPCU. We also observe that when the target rate of user m is different, the proposed NOMA scheme achieves almost the same ST, while the larger the target rate of user m under OMA scheme, the smaller the ST of user n.

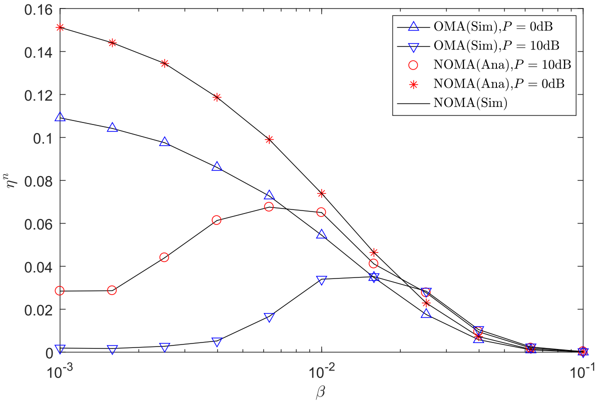

FIGURE 8. The η versus β with $R_m = 3$ BPCU, $R_m^s = 2$ BPCU, $R_n = 3$ BPCU, $R_n^s = 0.3$ BPCU, $R_{D1} = 40m$, $R_{D2} = 70m$, $\lambda_E = 0.0002$ *nodes*/m^2, $r = 140m$, $m_S = 0.1$ and $M_S = 200$.

Fig. 8 shows the relationship between the ST of user n and the blockage density β with the different transmit power P. We observe that for user n, when the given transmission power is low, the ST of user n decreases with the expansion of blocking density β. The main reason for this behavior is that in low given transmit power, the signal experiences high path loss as β increases. When the given transmit power is higher, the risk of information leakage is increased, ST is smaller than that at a given low transmit power. Nevertheless, increasing β does not cause a strict drop in the ST of the user n. In fact, there is an optimal blocking density β^*, resulting in a maximum ST achievement. When we increase β up to the optimal point, as NLOS communication dominates the mmWave networks, the ST of user n is increased to the maximum by using multipath signals. However, as the environment becomes full of physical barriers, the probability of information reaching user n decreases, ST is reduced to zero.

V. CONCLUSION

In this paper, we investigated secrecy performance for downlink NOMA transmission in mmWave wiretap networks. The locations of NOMA users and eavesdroppers are modeled using stochastic geometry. We proposed the NOMA scheme of cognitive power allocation. Specifically, after the QoS of primary user with high priority is satisfied, the cognitive power allocation scheme is adopted to serve secondary user. Considering beam pattern, link blockage and user pairing, the COP, SOP and ST of the proposed NOMA scheme are derived and compared with OMA. Our results show that under the reasonable design of system parameters, user with lower priority can also achieve better performance than OMA scheme. Moreover, our results have certain reference value for different needs of each NOMA user, especially in the Internet of Things (IoT), some users have higher priority of services, while some users need general services. In future works, more practical and complex application scenarios, such as imperfect CSI, user fairness and artificial noise will be considered. Furthermore, the results of this paper can be combined with unmanned aerial vehicle (UAV) to analyze the secrecy transmission capability.

APPENDIX A

To derive P_{co}^{m}, based on ***Theorem 1***, applying the probability generating functional (PGFL) of the PPP and polar coordinates, we can formulate

$$\begin{aligned}
P_{co}^{m} &= \Pr\left(\frac{PM_S|h_m|^2L\left(r_m\right)}{\sigma_m^2} < 2^{R_m}-1\right)\\
&= \Pr\left(|h_m|^2 < \frac{\left(2^{R_m}-1\right)\sigma_m^2}{PM_SL\left(r_m\right)}\right)\\
&= \frac{2}{R_{D2}^2-R_{D1}^2}\left(\int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_L,\frac{(2^{R_m}-1)\sigma_m^2}{PM_SL(r_m)}N_L\right)}{\Gamma\left(N_L\right)}e^{-\beta r_m}r_mdr_m\right.\\
&\quad\left.+\int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_N,\frac{(2^{R_m}-1)\sigma_m^2}{PM_SL(r_m)}N_N\right)}{\Gamma\left(N_N\right)}\left(1-e^{-\beta r_m}\right)r_mdr_m\right),
\end{aligned} \tag{26}$$

Applying [29](eq.(8.354.1)), we arrive at

$$\begin{aligned}
P_{co}^{m} = &\sum_{i=0}^{\infty}\frac{2\times(-1)^i(N_Lb\varepsilon_1)^{N_L+i}}{i!\left(N_L+i\right)\Gamma\left(N_L\right)\left(R_{D2}^2-R_{D1}^2\right)}\\
&\times\left(\int_0^{R_{D2}}r_m^{\alpha_L(N_L+i)+1}e^{-\beta r_m}d\right.\\
&\left.-\int_0^{R_{D1}}r_m^{\alpha_L(N_L+i)+1}e^{-\beta r_m}dr_m\right)\\
&+\sum_{j=0}^{\infty}\frac{2\times(-1)^j(N_Nc\varepsilon_1)^{N_N+j}}{j!\left(N_N+j\right)\Gamma\left(N_N\right)\left(R_{D2}^2-R_{D1}^2\right)}\\
&\times\left(\int_0^{R_{D2}}r_m^{\alpha_N(N_N+j)+1}\left(1-e^{-\beta r_m}\right)dr_m\right.\\
&\left.-\int_0^{R_{D1}}r_m^{\alpha_N(N_N+j)+1}\left(1-e^{-\beta r_m}\right)dr_m\right)
\end{aligned} \tag{27}$$

Applying [29](eq.(3.351.1)), we obtain the (9).

APPENDIX B

Base on (2), in other words, when user m satisfy its QoS, we express the COP for user n as

$$\begin{aligned}
P_n^o &= \Pr\left(\frac{a_mPM_S|h_n|^2L\left(r_n\right)}{a_nPM_S|h_n|^2L\left(r_n\right)+\sigma_n^2} < \varepsilon_1\right.\\
&\quad\left. or \frac{a_nM_SP|h_n|^2L\left(r_n\right)}{\sigma_n^2} < \varepsilon_2\right)\\
&= \sum_{i\in(L,N)}p_i\left(r_n\right)\int f_\kappa\left(x\right)\frac{\Upsilon\left(N_i,\frac{N_ix\sigma_n^2}{PM_SL(r_n)}\right)}{\Gamma\left(N_i\right)}dx\\
&= \sum_{i\in(L,N)}p_i\left(r_n\right)\left(\int\frac{\Upsilon\left(N_i,\frac{N_ix\sigma_n^2}{PM_SL(r_n)}\right)}{\Gamma\left(N_i\right)}dF_\kappa\left(x\right)\right),
\end{aligned} \tag{28}$$

where $\kappa = \max\left\{\varepsilon_1/1-a_n-\varepsilon_1a_n, \varepsilon_2/a_n\right\}$, $f_\kappa\left(x\right)$ is the probability density function (PDF) of κ, $F_\kappa\left(x\right)$ is the cumulative distribution function (CDF) of κ. Mentioned earlier, if $|h_m|^2 < \left(\varepsilon_1\sigma_m^2/PM_sL\left(r_m\right)\right)$, $a_n = 0$, so we express the CDF of κ as

$$\begin{aligned}
F_\kappa\left(x\right) &= \Pr\left(\frac{\varepsilon_1}{1-a_n-\varepsilon_1a_n} < x, \frac{\varepsilon_2}{a_n} < x\right)\\
&= \Pr\left(|h_m|^2 < \frac{x\sigma_m^2}{PM_sL\left(r_m\right)}, |h_m|^2\right.\\
&\quad\left. > \frac{\varepsilon_1x\sigma_m^2}{\left(x-\varepsilon_2\left(1+\varepsilon_1\right)\right)PM_sL\left(r_m\right)}\right)\\
&= \underbrace{\sum_{i\in\{L,N\}}p_i\left(r_m\right)\frac{\Upsilon\left(N_i,\frac{N_ix\sigma_m^2}{PM_sL(r_m)}-\frac{N_i\varepsilon_1\sigma_m^2}{PM_sL(r_m)}\right)}{\Gamma\left(N_i\right)}}_{Z_1}\\
&\quad-\underbrace{\sum_{i\in\{L,N\}}p_i\left(r_m\right)\frac{\Upsilon\left(N_i,\frac{N_i\varepsilon_1x\sigma_m^2}{(x-\varepsilon_2(1+\varepsilon_1))PM_sL(r_m)}-\frac{N_i\varepsilon_1\sigma_m^2}{PM_sL(r_m)}\right)}{\Gamma\left(N_i\right)}}_{Z_2},
\end{aligned} \tag{29}$$

Note that $F_\kappa\left(x\right)$ is valid when $x > \varepsilon_1+\varepsilon_2\left(1+\varepsilon_1\right)$, otherwise $F_\kappa\left(x\right) = 0$. In the following, we calculate Z_1 in detail, Z_2 can be calculated with a similar procedure which is omitted for brevity.

$$\begin{aligned}
Z_1 = &\frac{2}{R_{D2}^2-R_{D1}^2}\\
&\left(\int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_L,N_L\left(bx-b\varepsilon_1\right)r_m^{\alpha_L}\right)}{\Gamma\left(N_L\right)}e^{-\beta r_m}r_mdr_m\right.\\
&\left.+\int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_N,N_N\left(bx-b\varepsilon_1\right)r_m^{\alpha_N}\right)}{\Gamma\left(N_N\right)}\left(1-e^{-\beta r_m}\right)r_mdr_m\right)\\
= &\sum_{k_1=0}^{\infty}\frac{(-1)^{k_1}\left(N_L\left(bx-b\varepsilon_1\right)\right)^{N_L+k_1}}{k_1!\left(N_L+k_1\right)\Gamma\left(N_L\right)\left(R_{D2}^2-R_{D1}^2\right)}\\
&\times\left(\int_0^{R_{D2}}r_m^{\alpha_L(N_L+k_1)+1}e^{-\beta r_m}dr_m\right.\\
&\left.-\int_0^{R_{D1}}r_m^{\alpha_L(N_L+k_1)+1}e^{-\beta r_m}dr_m\right)\\
&+\sum_{k_2=0}^{\infty}\frac{(-1)^{k_2}\left(N_N\left(bx-b\varepsilon_1\right)\right)^{N_N+k_2}}{k_2!\left(N_N+k_2\right)\Gamma\left(N_N\right)\left(R_{D2}^2-R_{D1}^2\right)}\\
&\times\left(\int_0^{R_{D2}}r_m^{\alpha_N(N_N+k_2)+1}\left(1-e^{-\beta r_m}\right)dr_m\right.\\
&\left.-\int_0^{R_{D1}}r_m^{\alpha_N(N_N+k_2)+1}\left(1-e^{-\beta r_m}\right)dr_m\right),
\end{aligned} \tag{30}$$

After some mathematical manipulations, upon substituting Z_1 and Z_2 into (30), we obtain the CDF of κ as given in (10), as shown at the top of the 5th page. Based on (29), applying [29](eq.(8.356.4)) and integral subsection integration, P_{co}^{n} of user n is given by (11).

APPENDIX C

Recall that the SOP of the user n is given by

$$\begin{aligned} P_{so}^{n} &= \Pr\left(\gamma_{e\to n} > 2^{R_n - R_n^s} - 1\right) \\ &= \int_{2^{R_n-R_n^s}-1}^{\infty} f_{\gamma_{e\to n}}(x)dx = 1 - F_{\gamma_{e\to n}}(\varepsilon_4), \end{aligned} \tag{31}$$

To derive the CDF of $\gamma_{e\to n}$, based on (7), we can formulate

$$\begin{aligned} F_{\gamma_{e\to n}}(x) &= \Pr\left\{\max_{E\in\phi_E}\left(\frac{a_n M_S P|h_e|^2 L(r_e)}{\sigma_e^2}\right) < x\right\} \\ &= \underbrace{\Pr\left\{\max_{E\in\phi_E^L}\left(\frac{a_n M_S P|h_e|^2 L(r_e)}{\sigma_e^2}\right) < x\right\}}_{Z_3} \\ &\quad \times \underbrace{\Pr\left\{\max_{E\in\phi_E^N}\left(\frac{a_n M_S P|h_e|^2 L(r_e)}{\sigma_e^2}\right) < x\right\}}_{Z_4}, \end{aligned} \tag{32}$$

In the following, we calculate Z_3 in detail, Z_4 can be calculated with a similar procedure which is omitted for brevity.

$$\begin{aligned} Z_3 &= \Pr\left\{\max_{E\in\phi_E^L}\left(\frac{a_n M_S P|h_e|^2 L(r_e)}{\sigma_e^2}\right) < x\right\} \\ &= E\left\{\prod_{E\in\Phi_E^L}\Pr\left(|h_e|^2 < \frac{x\sigma_e^2}{a_n P M_S L(r_E)}\right)\right\} \\ &= \exp\left(-\theta_s\lambda_e\int_r^{\infty}\int_0^{\frac{1}{\varepsilon_1+1}}\left(1 - \frac{\Upsilon\left(N_L, \frac{N_L x b r_e^{\alpha_L}}{z}\right)}{\Gamma(N_L)}\right)\right. \\ &\qquad \left. \times f_{a_n}(z)\, e^{-\beta r_e} r_e dz dr_e\right) \\ &= \exp\left(-\theta_s\lambda_e\left(F_{a_n}(z)\,|_0^{\frac{1}{\varepsilon_1+1}}\frac{\Gamma(2,\beta r)}{\beta^2}\right.\right. \\ &\qquad - \sum_{n_1=0}^{\infty}\frac{(-1)^{n_1}(N_L x b)^{N_L+n_1}\Gamma(\alpha_L(N_L+n_1)+2,\beta r)}{n_1!(N_L+n_1)\Gamma(N_L)\beta^{\alpha_L(N_L+n_1)+2}} \\ &\qquad \left.\left. \times \underbrace{\left(\int_0^{\frac{1}{\varepsilon_1+1}} z^{-(N_L+n_1)} f_{a_n}(z)\,dz\right)}_{Q^1}\right)\right), \end{aligned} \tag{33}$$

Now let's turn our attention to the derivation of integral Q^1 in (33), $f_{a_n}(z)$ is the PDF of a_n, based on (3), we express the CDF of a_n as

$$\begin{aligned} &F_{a_n}(z) \\ &= \Pr\left\{\frac{PM_s|h_m|^2 L(r_m) - \varepsilon_1\sigma_m^2}{(\varepsilon_1+1)PM_s|h_m|^2 L(r_m)} < z\right\} = \sum_{i\in\{L,N\}} \\ &\quad \times \left(\frac{\Upsilon\left(N_i, N_i\left(\frac{\varepsilon_1\sigma_m^2}{(1-z(\varepsilon_1+1))PM_sL(r_m)} - \frac{\varepsilon_1\sigma_m^2}{PM_sL(r_m)}\right)\right)}{\Gamma(N_i)}\right) p_i(r_m) \\ &= \frac{2}{R_{D2}^2 - R_{D1}^2}\left(\int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_L, \frac{N_L b\varepsilon_1 z(\varepsilon_1+1)r_m^{\alpha_L}}{(1-z(\varepsilon_1+1))}\right)}{\Gamma(N_L)} e^{-\beta r_m} r_m dr_m\right. \\ &\quad \left. + \int_{R_{D_1}}^{R_{D2}}\frac{\Upsilon\left(N_N, \frac{N_N c\varepsilon_1 z(\varepsilon_1+1)r_m^{\alpha_N}}{(1-z(\varepsilon_1+1))}\right)}{\Gamma(N_N)}\left(1 - e^{-\beta r_m}\right) r_m dr_m\right) \\ &= \sum_{p=0}^{\infty}\frac{z^{N_L+p}Q_1}{(1-z(\varepsilon_1+1))^{N_L+p}} + \sum_{q=0}^{\infty}\frac{z^{N_N+q}Q_2}{(1-z(\varepsilon_1+1))^{N_N+q}}, \end{aligned} \tag{34}$$

Note that $F_{a_n}(z)$ is valid when $z < (1/\varepsilon_1 + 1)$, otherwise $F_{a_n}(z) = 1$. Q_1 and Q_2 are given by ***Theorem 3***, respectively. By taking the first derivative of $F_{a_n}(z)$, the PDF of the power allocation coefficient a_n is given by

$$\begin{aligned} f_{a_n}(z) = &\sum_{p=0}^{\infty}\frac{(N_L+p)z^{N_L+p-1}Q_1}{(1-z(\varepsilon_1+1))^{N_L+p+1}} \\ &+ \sum_{q=0}^{\infty}\frac{(N_N+q)z^{N_N+q-1}Q_2}{(1-z(\varepsilon_1+1))^{N_N+q+1}}, \end{aligned} \tag{35}$$

By integral subsection integration, upon substituting $f_{a_n}(z)$ and $F_{a_n}(z)$ into (33), after some mathematical manipulations, we obtain the CDF of $\gamma_{e\to n}$.

APPENDIX D

Recall that the SOP of the user m is given by

$$\begin{aligned} P_{so}^{m} &= \Pr\left(\gamma_{e\to m} > 2^{R_m - R_m^s} - 1\right) \\ &= \int_{2^{R_m-R_m^s}-1}^{\infty} f_{\gamma_{e\to m}}(x)\,dx = 1 - F_{\gamma_{e\to m}}(\varepsilon_3), \end{aligned} \tag{36}$$

To derive the CDF of $\gamma_{e\to m}$, based on (8), we can formulate

$$\begin{aligned} F_{\gamma_{e\to m}}(x) &= \Pr\left\{\max_{E\in\phi_E}\left(\frac{a_m M_S P|h_e|^2 L(r_e)}{a_n M_S P|h_e|^2 L(r_e) + \sigma_e^2}\right) < x\right\} \\ &= \underbrace{\Pr\left\{\max_{E\in\phi_E^L}\left(\frac{a_m M_S P|h_e|^2 L(r_e)}{a_n M_S P|h_e|^2 L(r_e) + \sigma_e^2}\right) < x\right\}}_{Z_5} \\ &\quad \times \underbrace{\Pr\left\{\max_{E\in\phi_E^N}\left(\frac{a_m M_S P|h_e|^2 L(r_e)}{a_n M_S P|h_e|^2 L(r_e) + \sigma_e^2}\right) < x\right\}}_{Z_6}, \end{aligned} \tag{37}$$

$$\begin{aligned}
Z_5 &= \Pr\left\{\max_{E\in\phi_E^L}\left(\frac{a_m M_S P|h_e|^2 L\left(r_e\right)}{a_n M_S P|h_e|^2 L\left(r_e\right)+\sigma_e^2}\right)<x\right\}\\
&= E\left\{\prod_{E\in\Phi_E^L}\Pr\left(|h_e|^2<\frac{x\sigma_e^2}{\left(1-a_n-a_n x\right)PM_S L\left(r_E\right)}\right)\right\}\\
&= \exp\left(-\theta_s\lambda_e\int_r^\infty\int_0^{\frac{1}{\varepsilon_1+1}}\left(1-\frac{\Upsilon\left(N_L,\frac{N_L xbr_e^{\alpha_L}}{(1-z-zx)}\right)}{\Gamma\left(N_L\right)}\right)\right.\\
&\quad\left.\times f_{a_n}(z)\,e^{-\beta r_e}r_e dr_e\right)\\
&= \exp\left(-\theta_s\lambda_e\left(F_{a_n}(z)\,|_0^{\frac{1}{\varepsilon_1+1}}\frac{\Gamma\left(2,\beta r\right)}{\beta^2}-\sum_{t_1=0}^{\infty}\frac{(-1)^{t_1}\left(N_L xb\right)^{N_L+t_1}\Gamma\left(\alpha_L\left(N_L+t_1\right)+2,\beta r\right)\left(-\left(1-x\right)\right)^{-w_1}}{t_1\left(N_L+t_1\right)\Gamma\left(N_L\right)\beta^{\alpha_L\left(N_L+t_1\right)+2}\sum\limits_{w_1=0}^{N_L+t_1}\binom{N_L+t_1}{w_1}}\right.\right.\\
&\quad\left.\left.\times\underbrace{\left(\int_0^{\frac{1}{\varepsilon_1+1}}z^{-w_1}f_{a_n}(z)\,dz\right)}_{Q^2}\right)\right),
\end{aligned}\tag{38}$$

We turn our attention on Z_5, following a procedure similar to that used for obtaining Z_6, which is omitted for brevity. Then Z_5 can be expressed as

Following similar steps, based on (34) and (35), after some calculations, we obtain the CDF of $\gamma_{e\to m}$ by integral subsection integration.

APPENDIX E

In the proposed NOMA scheme, user m, as the primary user, mainly considers its security while guaranteeing its connection. ST of the user m is given by

$$\begin{aligned}
\eta^m &= R_m^s\Pr\left(\log\left(1+\gamma_{e\to m}\right)<\left(R_m-R_m^s\right)\right)\\
&= R_m^s\Pr\left(\max_{E\in\phi_E}\left(\frac{a_m M_S P|h_e|^2 L\left(r_e\right)}{a_n M_S P|h_e|^2 L\left(r_e\right)+\sigma_e^2}\right)<\varepsilon_3\right)\\
&= \underbrace{R_m^s\Pr\left\{\max_{E\in\phi_E^L}\left(\frac{a_m M_S P|h_e|^2 L\left(r_e\right)}{a_n M_S P|h_e|^2 L\left(r_e\right)+\sigma_e^2}\right)<\varepsilon_3\right\}}_{Z_7}\\
&\quad\times\underbrace{\Pr\left\{\max_{E\in\phi_E^N}\left(\frac{a_m M_S P|h_e|^2 L\left(r_e\right)}{a_n M_S P|h_e|^2 L\left(r_e\right)+\sigma_e^2}\right)<\varepsilon_3\right\}}_{Z_8},
\end{aligned}\tag{39}$$

The process of calculating Z_7 and Z_8 is similar to that of Z_5. Substituting $x=\varepsilon_3$ into (38), as shown at the top of this page. Hence, we can obtain (16). The proof is completed.

APPENDIX F

In the proposed NOMA scheme, under the condition of guaranteeing user m's QoS, a part of power is dynamically allocated to user n. Therefore, the security and reliability of user n are considered jointly. Based on (6) and (7), ST of the user n is given by

$$\begin{aligned}
\eta^n &= R_n^s\Pr\left(\log\left(1+\gamma_n\right)>R_n,\right.\\
&\qquad\left.\log\left(1+\gamma_{e\to n}\right)<\left(R_n-R_n^s\right),|h_m|^2>\frac{\varepsilon_1\sigma_m^2}{PM_s L\left(r_m\right)}\right)\\
&= R_n^s\Pr\left(a_n|h_n|^2 L\left(r_n\right)>\frac{\sigma_n^2\varepsilon_2}{M_S P},\right.\\
&\qquad\left.\max_{E\in\phi_E}\left(a_n|h_e|^2 L\left(r_e\right)\right)<\frac{\sigma_e^2\varepsilon_4}{M_S P},|h_m|^2 L\left(r_m\right)>\frac{\varepsilon_1\sigma_m^2}{PM_s}\right)\\
&=R_n^s\Pr\left(\underbrace{\frac{a_n z}{\phi_i}>\varepsilon_2}_{P_1},\underbrace{\max_{E\in\phi_E}\left(\frac{a_n y}{\phi_i}\right)<\varepsilon_4}_{P_2},x>\varepsilon_1\phi_i\right),
\end{aligned}\tag{40}$$

where $x=|h_m|^2/r_m^{\alpha_i}$, $y=|h_e|^2/r_e^{\alpha_i}$, $z=|h_n|^2/r_n^{\alpha_i}$, $\varphi_i=\sigma_\vartheta^2/M_s PC_i$, $i\in\{L,N\}$, $\vartheta\in\{m,n,e\}$. Now, let's find CDF for P_1 and P_2, respectively. The CDF for P_1 can be calculated as follows:

$$\begin{aligned}
&F_{P_1}(x)\\
&\quad= \Pr\left\{\frac{a_n z}{\varphi_i}<x\right\}=\Pr\left\{|h_n|^2<\frac{\varphi_i x r_n^{\alpha_i}}{a_n}\right\}\\
&\quad= \frac{2}{R_{D1}^2}\left(\int_0^{R_{D1}}\frac{\Upsilon\left(N_L,\frac{\varphi_L x r_n^{\alpha_L}N_L}{a_n}\right)}{\Gamma\left(N_L\right)}e^{-\beta r_n}r_n dr_n\right.
\end{aligned}$$

$$
\begin{aligned}
&+ \int_0^{R_{D1}} \frac{\Upsilon\left(N_N, \frac{\varphi_N x r_n^{\alpha_N} N_N}{a_n}\right)}{\Gamma\left(N_N\right)} \left(1 - e^{-\beta r_n}\right) r_n d r_n \Bigg) \\
&= \frac{2}{R_{D1}^2} \left(\sum_{i=0}^{\infty} \frac{(-1)^i \left(\frac{\varphi_L x N_L}{a_n}\right)^{N_L+i}}{i!\left(N_L+i\right)\Gamma\left(N_L\right)} \right. \\
&\quad \times \frac{\Upsilon\left(\alpha_L\left(N_L+i\right)+2, \beta R_{D1}\right)}{\beta^{\alpha_L\left(N_L+i\right)+2}} + \sum_{j=0}^{\infty} \frac{(-1)^j \left(\frac{\varphi_N x N_N}{a_n}\right)^{N_N+j}}{j!\left(N_N+j\right)\Gamma\left(N_N\right)} \\
&\quad \left. \times \left(\frac{\left(R_{D1}\right)^{\alpha_N\left(N_N+j\right)+2}}{\alpha_N\left(N_N+j\right)+2} - \frac{\Upsilon\left(\alpha_N\left(N_N+j\right)+2, \beta R_{D1}\right)}{\beta^{\alpha_N\left(N_N+j\right)+2}} \right) \right), \qquad (41)
\end{aligned}
$$

Following similar steps, the CDF for P_2 can be calculated as follows:

$$
\begin{aligned}
&F_{P_2}(x) \\
&= \Pr\left\{ \max_{E \in \phi_E} \left(\frac{a_n y}{\varphi_i}\right) < x \right\} \\
&= \exp\Bigg(-\theta_s \lambda_e \Bigg(- \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{\varphi_L x N_L}{a_n}\right)^{N_L+n}}{n!\left(N_L+n\right)\Gamma\left(N_L\right)} \\
&\quad \times \frac{\Gamma\left(\alpha_L\left(N_L+n\right)+2, \beta r\right)}{\beta^{\alpha_L\left(N_L+n\right)+2}} + \left(\frac{\left(N_N-1\right)!}{\Gamma\left(N_N\right)}\right) \\
&\quad \times \sum_{m=0}^{N_N-1} \frac{\left(\frac{\varphi_N x N_N}{a_n}\right)^m}{m!} \times \frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}, \frac{\varphi_N x N_N r^{\alpha_N}}{a_n}\right)}{\alpha_N \left(\frac{\varphi_N x N_N}{a_n}\right)^{\frac{m\alpha_N+2}{\alpha_N}}} \\
&\quad + \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{\varphi_N x N_N}{a_n}\right)^{N_N+n}}{n!\left(N_N+n\right)\Gamma\left(N_N\right)} \frac{\Gamma\left(\alpha_N\left(N_N+n\right)+2, \beta r\right)}{\beta^{\alpha_N\left(N_N+n\right)+2}} \Bigg)\Bigg), \qquad (42)
\end{aligned}
$$

Based on (41) and (42), we can re-write (40) as

$$
\eta^n = R_n^s \int_0^{\frac{1}{\varepsilon_1+1}} \left(1 - F_{P_1}\left(\varepsilon_2\right)\right) F_{P_2}\left(\varepsilon_4\right) f_{a_n}\left(a_n\right) d a_n, \qquad (43)
$$

Upon substituting (35), (41) and (42) into (43), we can obtain (17). The proof is completed.

REFERENCES

[1] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, Jun. 2011.

[2] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular Wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[3] T. Bai and R. W. Heath, Jr., "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.

[4] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. Dai, and J. Rodriguez, "Millimeter-wave massive MIMO communication for future wireless systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 836–869, 2nd Quart., 2018.

[5] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2059–2071, Mar. 2017.

[6] T. Bai, A. Alkhateeb, and R. W. Heath, Jr., "Coverage and capacity of millimeter-wave cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 70–77, Sep. 2014.

[7] T. Bai and R. W. Heath, Jr., "Coverage analysis for millimeter wave cellular networks with blockage effects," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 727–730.

[8] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, and R. W. Heath, Jr., "Modeling and analyzing millimeter wave cellular systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 403–430, Jan. 2017.

[9] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[10] S. Vuppala, Y. J. Tolossa, 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.

[11] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, Jr., "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

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

[13] 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.

[14] Z. Xiang, W. Yang, Y. Cai, Y. Cheng, H. Wu, and M. Wang, "Exploiting uplink NOMA to improve sum secrecy throughput in IoT networks," *Wireless Commun. Mobile Comput.*, vol. 2018, no. 8, pp. 1–15, Jul. 2018.

[15] Q. C. Li, H. Niu, A. T. Papathanassiou, and G. Wu, "5G network capacity: Key elements and technologies," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 71–78, Mar. 2014.

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

[17] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[18] Y. Liu, Z. Ding, M. Elkashlan, and J. Yuan, "Nonorthogonal multiple access in large-scale underlay cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10152–10157, Dec. 2016.

[19] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.

[20] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8653906/

[21] Z. Xiang, W. Yang, G. Pan, Y. Cai, and X. Sun, "Secure transmission in non-orthogonal multiple access networks with an untrusted relay," *IEEE Wireless Commun. Lett.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8641340/

[22] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[23] Z. Ding, P. Fan, and H. V. Poor, "Random beamforming in millimeter-wave NOMA networks," *IEEE Access*, vol. 5, pp. 7667–7681, 2017.

[24] J. Cui, Y. Liu, Z. Ding, P. Fan, and A. Nallanathan, "Optimal user scheduling and power allocation for millimeter wave NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1502–1517, Mar. 2018.

[25] Y. Sun, Z. Ding, and X. Dai, "On the performance of downlink NOMA in multi-cell mm wave networks," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2366–2369, Nov. 2018.

[26] Y. Zhou, V. W. S. 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.

[27] Z. Xiao, L. Zhu, 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.

[28] E. Turgut and M. C. Gursoy, "Coverage in heterogeneous downlink millimeter wave cellular networks," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4463–4477, Oct. 2017.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[30] G. R. Maccartney, T. S. Rappaport, S. Sun, and S. Deng, "Indoor office wideband millimeter-wave propagation measurements and channel models at 28 and 73 GHz for ultra-dense 5G wireless networks," *IEEE Access*, vol. 3, pp. 2388–2424, 2015.

YI SONG received the M.S. degree from the Nanjing University of Aeronautics And Astronautics, in 2011. He is currently pursuing the Ph.D. degree with the Institution of Communications Engineering in Army Engineering University of PLA. His research interests include millimeter-wave, non-orthogonal multiple access, physical-layer security, and cognitive radio.

WEIWEI YANG (S'08-M'12) received the B.S., M.S., and Ph.D. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. His research interests include orthogonal frequency domain multiplexing systems, signal processing in communications, millimeter-wave, cooperative communications, wireless sensor networks, and network security.

ZHONGWU XIANG received the B.S. degree from South China Normal University, in 2014, and M.S. degree from the PLA University of Science and Technology, in 2017. He is currently pursuing the Ph.D. degree with the Institution of Communications Engineering in Army Engineering University of PLA. His research interests include non-orthogonal multiple access, physical-layer security, and cognitive radio.

BIAO WANG received the M.S. and Ph.D. degree in information and signal processing from Institute of Acoustics, Chinese Academy of Sciences (IACAS), Beijing, China, in 2005 and 2009, respectively. Since 2013, he is an Associate Professor with the College of Information and Electronic Engineering, Jiangsu University of Science and Technology, Zhenjiang, China. His research interests include underwater acoustic array signal processing, underwater acoustic communication, and underwater acoustic sensor networks.

YUEMING CAI (M'05-SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, the M.S. degree in microelectronics engineering, and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications, and wireless sensor networks.