An Analysis on Secure Millimeter Wave NOMA Communications in Cognitive Radio Networks

YI SONG1,2,3, WEIWEI YANG2, ZHONGWU XIANG2, NAN SHA2, HUI WANG1,3, AND YUCUI YANG1,3
1School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huai’an 223001, China
2College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
3Jiangsu Province Key Construction Laboratory of Modern Measurement Technology and Intelligent System, Huai’an 223300, China
Corresponding author: Yi Song (hysongyi@163.com)

ABSTRACT In this paper, an easy analysis framework is developed to evaluate the reliability and security of the secondary receivers (SU-Rxs) in millimeter wave (mmWave) non-orthogonal multiple access (NOMA) aided cognitive radio (CR) networks, where secondary transmitters (SU-Txs) transmit confidential messages to SU-Rxs belonging to different regions under the interference temperature constraint of the primary receiver (PU-Rx). Considering that randomly located eavesdroppers and primary user may be in the signal beam emitted by the SU-Txs, information leakage and interference to the primary network will be inevitable issues. Motivated by these challenges, combining the key features of multi-cell mmWave networks and NOMA communications, the closed-form expressions of three key performance metrics of connection outage probability (COP), secrecy outage probability (SOP), and secrecy throughput (ST) are derived by using the sector eavesdropper-exclusion zone, and the reliability and secrecy performance of the secondary networks are measured by different system parameters. The obtained performance evaluation results have demonstrated that the interference temperature constraint of the PU-Rx can be used to balance the security and reliability of the secondary networks. The reliability and security of paired NOMA users can be improved by using reasonable power allocation factor and sector eavesdropper-exclusion zone. Meanwhile, the connection performance of paired NOMA users is better than orthogonal multiple access (OMA). Furthermore, various system parameters can be reasonably set in conjunction with blockage and inter-cell interference to achieve optimal network’s performance.

INDEX TERMS Non-orthogonal multiple access (NOMA), millimeter wave (mmWave), cognitive radio (CR), stochastic geometry.

I. INTRODUCTION

With the rapid advancement of wireless communication and artificial intelligence technology, Internet of things (IoT) has become one of the main driver for the development of future communications, and will face many challenges. In order to achieve high data rate and spectrum efficiency, and to meet the requirements of massive connectivity and low latency, more advanced communication technologies and means need to be incorporated. On the one hand, in order to achieve higher spectral efficiency, non-orthogonal multiple access (NOMA) can apply power domain to serve a large number of users at different power levels simultaneously within the same resource block [1], [2]. On the other hand, mmWave has a widely available spectrum bandwidth in the 30 to 300 GHz range, directional beamforming can be used to provide array gains due to its short wavelength [3]. Therefore, integrating NOMA techniques into mmWave systems has great potential for improving data rate, spectrum utilization, massive connectivity, and low latency [4]–[6].

Another promising candidate technique is cognitive radio (CR), which is mainly used to alleviate the scarcity of wireless spectrum [7]–[9]. Using CR features in ultra-dense networks can optimize spectrum utilization while avoiding interference with other operating networks [10]. In order to achieve this objective, we need to design the physical layer adaptively and flexibly. Besides, security has become an important requirement in the design of...
communication systems. In view of the broadcast nature of wireless media, especially the openness and dynamic of CR networks, security is critical because it is more vulnerable to external security attacks [11]–[13]. Traditionally, cryptographic algorithms are used at the upper layers of the communication protocol stack to enhance the security of the communication networks. However, for ultra-dense networks with many low-complexity nodes, the generation, distribution, and management of secret key may be complex, time-consuming, and sometimes difficult to implement. Moreover, NOMA trades for improved spectrum utilization at the expense of serious interference, making the system vulnerable to security threat [14]. To address those issues, physical layer security (PLS) as a supplement to encryption is more attractive than encryption used at the upper layer because it eliminates the need for keys by exploiting the randomness of wireless channels for security [15]–[17].

In recent years, technologies such as beamforming [16], [18], artificial noise [19], [20], and cooperative transmission [21], [22] have been extensively studied in mmWave systems to enhance PLS. The sensitivity to blockages may cause significant differences in path loss characteristics between signal line-of-sight (LOS) and non-line-of-sight (NLOS) links of mmWave signals, and thus different propagation laws may lead to different path loss rules. In addition, a large number of antennas can be deployed on the transmitter and receiver to achieve directional beamforming, so that the receiver can obtain a sufficiently high array gain [23]. Compared with the traditional microwave networks, the PLS issues in mmWave systems needs to be re-evaluated. Moreover, for mathematical tractability, it makes sense to approximate the antenna pattern with a sectorial model when simple maximum signal-to-noise ratio beam steering is assumed, where constant directional gains are assumed for both main lobe and side lobe [24]. By using a sectored antenna model, PLS of mmWave systems with different secure on-off transmission strategies in the presence of randomly distributed eavesdroppers was studied in [25]. The work in [20] investigated the secrecy performance of the noise-limited and the AN-assisted mmWave networks. Similarly, the secrecy performance of mmWave ad hoc network and hybrid mmWave network were analyzed in [19] and [22], respectively.

At the same time, the use of NOMA in conjunction with mmWave was investigated in [26]–[33]. Specifically, user grouping and power allocation strategies for mmWave NOMA network were analyzed in [26], [27]. The work in [28] proposed an angle-based user pairing strategy in the mmWave downlink NOMA networks, in which LOS user with the minimum relative angle difference to typical users was selected. A new mmWave-NOMA transmission scheme was introduced in [29], which can satisfy the quality of service (QoS) provided to machine type communication devices in cellular machine-to-machine communications for IoT, and analyzed its performance. To reduce channel estimation overhead, random beamforming is applied to mmWave NOMA networks in [30], [31]. A recent work [32] showed that the outage performance of NOMA was superior to OMA in multi-cell mmWave network. In [33], the capacity of mmWave NOMA networks under the condition of noise-limited and interference-limited scenarios was analyzed.

On the other hand, recent years have witnessed the research advancement in the field of cognitive mmWave networks, most of which are developing various technologies to minimize the mutual interference between other operating networks and cognitive users [34]–[36]. In addition, there are also literatures to study the secrecy performance of cognitive mmWave networks from the perspective of security. Reference [37] investigated the secrecy performance of the mmWave CR networks by modeling the mmWave channel through the fluctuating two-ray channels. The secrecy performance of the secondary sensor network was studied under the interference temperature constraint of a primary sensor node [38]. The secrecy performance of mmWave CR wiretap networks was investigated by complete transmission scheme and threshold-based scheme [39].

It is clear from all the above mentioned references that mmWave may support the high bandwidth requirements required for significantly increasing data rates. NOMA may support massive connectivity by simultaneously serving multiple users in the same resource block, which improves spectrum efficiency while reducing latency through its unlicensed scheduling. CR may not only improve the efficiency of spectrum utilization, but also control the mutual interference between networks. Therefore, mmWave NOMA aided CR would be a natural choice to improve the performance of ultra-dense networks, especially like the Internet of Vehicles (IoV). In addition, when the randomly located eavesdroppers and primary user may be in the signal beam emitted by the SU-Txs, information leakage and interference to the primary network will be inevitable issues. Furthermore, in ultra-dense networks, inter-cell interference is also an important factor affecting the performance of network users. Unfortunately, to the best of the authors’ knowledge, the existing literature did not carry out the related analysis of secrecy performance in mmWave NOMA aided CR networks.

To fill the aforementioned gap, in this paper we concentrates on the PLS of a mmWave NOMA aided CR network, where the random deployment of primary receiver (PU-Rx), secondary transmitters (SU-Txs), secondary users (SU-Rxs), and eavesdroppers is modeled by stochastic geometry. The positions of SU-Txs are located at the origin of a sectorial disc, and the locations of the SU-Rxs are uniformly distributed in different zones for NOMA. The SU-Txs equipped with multi-antenna sends confidential messages to SU-Rxs under the interference temperature constraint of the PU-Rx in the presence of the randomly located eavesdroppers. A sectorial eavesdropper-exclusion zone is introduced around SU-Txs to ameliorate the secrecy performance of the networks. Considering that randomly located eavesdroppers and PU-Rx may be in the signal beam emitted by the SU-Txs, combining the key features of multi-cell mmWave networks
and mmWave communications, we provide a comprehensive performance analysis of the mmWave NOMA aided CR networks. We summarize the main contributions as follows:

- We consider an underlay mmWave NOMA aided CR network, consisting of a PU-Rx, multiple SU-Txs, multiple paired NOMA SU-Rxs, multiple eavesdroppers. A sectorial eavesdropper-exclusion zone is introduced around SU-Txs to improve the secrecy performance of the networks. We then derive the cumulative distribution function (CDF) and the probability density function (PDF) of the PU-Rx’s channel gain and the signal-to-noise-and-interference ratio (SINR) of the most malicious eavesdropper.
- We derive the connection outage probability (COP) of each NOMA paired user, and compare it with the COP of OMA scheme, and conclude that the reliability of NOMA scheme is better than OMA scheme. We also derive the secrecy outage probability (SOP) of each NOMA paired user to evaluate the factors affecting the secrecy performance of the system. In addition, in order to measure the reliability and security of the proposed system, the secrecy throughput (ST) of every NOMA paired user is derived, and the effects of various system parameters on ST are studied.
- Finally, our results show that in mmWave NOMA aided CR networks, the SOP obtained by pairing NOMA users is constrained by the sectorial eavesdropper-exclusion zone’s radius. Moreover, the interference temperature constraint of the PU-Rx can be used to balance the security and reliability of the secondary networks. The power allocation factor is critical to the reliability and security of paired NOMA users. Furthermore, the different parameters can be reasonably set in conjunction with blockage and inter-cell interference to achieve optimal network’s performance.

The rest of this paper is organized as follows. The underlay mmWave NOMA aided CR networks and user pairing strategy are presented in Section II. A set of the exact analytical expressions for the COP, SOP, and ST of paired NOMA users is derived in Section III. In Section IV, numerical and simulation results verified our theoretical analyses are presented. Finally, we conclude this paper in Section V.

II. SYSTEM MODEL

A. NETWORK TOPOLOGY

We consider an underlay mmWave NOMA aided CR communication scenario, where a primary transmitter-receiver pair and a number of secondary base station (BS) user pair. The BSs (SU-Txs) send confidential messages to the SU-Rxs (denoted by SU-Rn and SU-Rm) by applying the NOMA transmission protocol in the present of spatial random distributed eavesdroppers aiming to interpret the signal but without trying to modify it, as shown in Fig. 1. The locations of the SU-Txs, denoted by \( x_i \), are modeled as a homogeneous Poisson point process (HPPP) \( \Phi_b \) with the density \( \lambda \), i.e., \( x_i \in \Phi_b \). Particularly, we assume that each SU-Tx is located at the origin of a sector coverage area. The sector coverage area is divided into two regions, which are denoted by \( D_1 \) and \( D_2 \), respectively. Similar topologies are used in [40]. The radius of the internal sector coverage area \( D_1 \) is denoted by \( R_{D_1} \), and the group of SU-Rn is randomly located in this region. The external sector ring spanning the radius distance from \( R_{D_1} \) to \( R_{D_2} \) is denoted by \( D_2 \), and the group of SU-Rm is randomly located in this region. In the rest of this paper, we assume that SU-Rn and SU-Rm are the selected user from each group for simplicity. In addition, the locations of randomly distributed eavesdroppers are modeled as a finite two-dimensional independent HPPP, denoted by \( \Phi_E \) with the density \( \lambda_E \). Furthermore, we assume that each SU-Tx has \( M \) antennas, while all SU-Rxs and eavesdroppers are equipped with a single antenna.

The designs of future wireless systems need to embed cognitive features, including the ability to sense interference power to utilize available spectrum [35]. Therefore, in the proposed networks, the PU-Rx allows the SU-Rxs to share the spectrum and requires the instantaneous interference power generated by the SU-Tx at the PU-Rx to be less than a fixed threshold \( I_w \). We assume that an extreme case is that a PU-Rx happens to be in the beam coverage area of the nearest SU-Tx, because in this case the SU-Tx will have the greatest interference to PU-Rx, and \( R_{SP} \) is used to represent the radius of its coverage area.

B. DIRECTIONAL BEAMFORMING

To compensate high path loss at mmWave frequencies, the SU-Txs deploy highly directional beamforming antenna arrays to perform the directional beamforming. In our model, using a sector model to analyze the antenna pattern [19], [20], [22]. In particular, \( G_S (\theta) = \begin{cases} M_S, & \text{if } |\theta| \leq \theta_S, \\ m_S, & \text{Otherwise}, \end{cases} \) (1)

where the directivity gains of the main lobe and side lobe are \( M_S \) and \( m_S \), respectively. The beamwidth of the main lobe is \( \theta_S \). For simplicity, assuming that the SU-Txs know the instantaneous channel state informations (CSI) of the

FIGURE 1. Illustration of a mmWave NOMA aided CR network consisting of a primary transmitter-receiver pair, multiple SU-Txs (BSs) and multiple paired NOMA SU-Rxs in presence of multiple eavesdroppers.
SU-Rn and SU-Rm, then the SU-Rn and SU-Rm can obtain the maximum array gain $M_S$. It is assumed that SU-Txs can detect the existence of eavesdroppers in a limited range. This assumption applies to networks that combine broadcast and multicast transmissions when the eavesdroppers are active [25], [40], [41]. Furthermore, even for a passive eavesdropper, recent studies have shown that we can still detect the presence of passive eavesdroppers by unintentionally leaking local oscillator power from the radio frequency frontend of the eavesdropper receiver [42]. Therefore, a sector eavesdropper-exclusion zone with radius $r$ and central angle $\theta_S$ is introduced.

C. CHANNEL MODEL

Blockages in the networks are usually concrete buildings that cannot be penetrated by mmWave, the transmitted signals may reach the receivers via LOS or NLOS path [19]. Let’s define $P_L(r_d)$ as a probability function of LOS links with distance $r_d$, which follows $P_L(r_d) = e^{-\beta r_d}$, while the NLOS probability of a link is given as $P_N(r_d) = 1 - e^{-\beta r_d}$, where $\beta$ is the density of blockages. We model the fading as a Nakagami random variable, ignoring the potential correlation of blockage effects between links. Just as [20], [22] and [43], we consider independent Nakagami fading for each link, and the Nakagami fading parameter of the LOS (NLOS) link is $N_L(N_N)$. Both $N_L$ and $N_N$ are assumed to be positive integers for simplicity. Note that, Nakagami-m fading is usually used to simulate small-scale fading in literatures [5], [25] and [32]. Thus, $M_S|h|^2L(r_i), i \in \{m, n\}$ denotes the channel gains received by SU-Rm and SU-Rn, and $M_S|h|^2L(r_r)$ denotes the channel gains received by the eavesdroppers, where both $|h|^2$ and $|h|^2$ are normalized Gamma random variable with following $\Gamma(N_L, 1/N_L)$ and $\Gamma(N_N, 1/N_N)$. $r_i$ and $r_r$ denote the distance from the SU-Tx to the SU-Rn and SU-Rm and the eavesdroppers, respectively. Furthermore, $L(r_i)$ and $L(r_r)$ denote the path loss function, which can be calculated by $L(r_i) = C_L r^{-\alpha L}$ for a LOS link and $L(r_j) = C_{N_L} r^{-\alpha N}$ for a NLOS link, $j \in \{i, e\}$. $C_L$ and $\alpha_L$ are the constant and path loss exponent depending on the LOS, $C_N$ and $\alpha_N$ depend on the NLOS.

D. DOWNLINK NOMA TRANSMISSION

Just as [40] and [44], we consider the case in which two SU-Rxs from different regions will be selected to implement NOMA. This approach is primarily to create more obvious channel quality differences between the paired users, because existing NOMA studies have proved that pairing of two users with quite different channel conditions is beneficial [40], [45]. Specifically, one user $m$ is selected from the external sector ring and another user $n$ from the internal sector for pairing them for NOMA in the same resource slot. Moreover, in the proposed network, to guarantee that the SU-Tx does not cause interference to the PU-Rx beyond the predefined threshold $I_{sw}$, its transmit power is defined as $P_U = \min \left( \frac{I_{sw}}{M_S P_U |h|^2L(r_i)}, P \right)$, where $P$ is the total available power at the SU-Tx. It should be pointed out that we consider that only the SU-Tx closest to the primary user can enable cognitive characteristics, and its transmission power is constrained by the primary user, denoted as $P_U$, and the transmission power of other SU-Txs are $P$.

E. RECEIVED SINR

According to the 3GPP Long Term Evolution Advanced (LTE-A) standard including a two-user NOMA scheme, in the rest of this paper we focus on a single selected pair of users. We assume that the internal sector SU-Rn can be capable of cancelling the interference of the external sector ring SU-Rm using successive interference cancellation (SIC) techniques. The SINR at the SU-Rm is defined as

$$\gamma_m = \frac{(1 - \alpha) M_S P_U |h|^2L(r_m)}{\alpha M_S P_U |h|^2L(r_m) + I_m + \sigma_n^2},$$

where $\alpha$ is denoted the power allocation coefficient, In the light of the principle of power-domain NOMA, $\alpha < 0.5$. The interference from multiple interfering SU-Txs: $I_k = \sum_{j \in \Phi_k} \frac{P_{G_{jk}} |h|^2L(r_{jk})}{\alpha^2_k}$ is the noise power, $k \in \{m, n, e\}$. It is worth pointing out that the directivity gain of the link between SU-Tx $j$ and SU-Rx $k$ is distributed as $G_{jk} = a_q$ with probability $h_{jk}$, where $q \in \{1, 2\}, a_1 = M_S, a_2 = M_Sb_1 = b_2/\pi, b_2 = 1 - b_1$.

According to the principle of SIC, SU-Rn should decode the signal of SU-Rm before detecting its own signal, and its SINR is expressed as

$$\gamma_n \rightarrow m = \frac{(1 - \alpha) M_S P_U |h|^2L(r_n)}{\alpha M_S P_U |h|^2L(r_n) + I_n + \sigma_n^2},$$

After eliminating the interference of the signal intended to SU-Rm, the SINR of SU-Rn is given by

$$\gamma_n = \frac{\alpha M_S P_U |h|^2L(r_n)}{I_n + \sigma_n^2}.$$
where

\[ y_{\rightarrow m} = \max_{E \in \Phi_E} \left( \frac{(1 - \alpha) M_S P_U |h_m|^2 L(r_m) + I_e + \sigma^2_e}{\alpha M_S P_U |h_m|^2 L(r_m) + I_e + \sigma^2_e} \right) \]  

respectively.

### III. PERFORMANCE ANALYSIS

In this section, a set of expressions of COP, SOP, and ST of the paired users are derived, and using those key performance metrics to further investigate the performance of the mmWave NOMA aided CR networks.

#### A. COP OF PAIRED USERS

The connection outage occurs when the codeword rate of the main channel is higher than the channel capacity \([10]\). We adopt the COP as a measure of the reliability performance. According to Shannon channel capacity formula, the COPs of the SU-Rn and SU-Rm are given by

\[ P_{co}^{n} = \text{Pr} \left( \frac{(1 - \alpha) M_S P_U |h_n|^2 L(r_n) + I_n + \sigma^2_n}{\alpha M_S P_U |h_n|^2 L(r_n) + I_n + \sigma^2_n} < 2^{R_n} - 1 \right) \]  

and

\[ P_{co}^{m} = \text{Pr} \left( \frac{(1 - \alpha) M_S P_U |h_m|^2 L(r_m) + I_m + \sigma^2_m}{\alpha M_S P_U |h_m|^2 L(r_m) + I_m + \sigma^2_m} < 2^{R_m} - 1 \right), \]

where \( R_n \) and \( R_m \) are the codeword rates of the SU-Rn and SU-Rm, respectively. For deriving the closed-form expressions of (7) and (8), we first give the following Lemma.

**Lemma 1:** The CDF and the PDF of the PU-Rx’s channel gain are given by

\[ F_{ksp}|^2_{(x)} = \sum_{n=1}^{N} \frac{\pi c_{m1}}{NR_{SP}} \sqrt{1 - \theta_m^2} \frac{\Gamma \left( N_L, \frac{N_{ksp} x_{n1}}{C_{m1}} \right) e^{-\beta c_{n1}}}{\Gamma \left( N_L \right)} \]

and

\[ f_{ksp}|^2_{(x)} = \sum_{n=1}^{N} \frac{\pi c_{m1}}{NR_{SP}} \sqrt{1 - \theta_m^2} \frac{\Gamma \left( N_L, \frac{N_{ksp} x_{n1}}{C_{m1}} \right) \left( 1 - e^{-\beta c_{n1}} \right)}{\Gamma \left( N_L - 1 \right)} \]

where \( \theta_m = \cos \left( \frac{2^{n} - 1}{2} \theta_1 \right), c_{n1} = \frac{RS}{2} (1 + \theta_n), N \) is the parameter of Gaussian-Chebyshev approximation. Here \( \Gamma (., \cdot) \) is the lower incomplete gamma function \([47]\).

**Proof:** See Appendix A.

Then, the following theorem gives COP of the paired users.

**Theorem 1:** The COP of the SU-Rn can be given by

\[ P_{co}^{n} = Z_1 \times F_{ksp}|^2_{(x)} \left( \frac{I_n}{P M_S} \right) + \int_{\frac{I_n}{P M_S}}^{\infty} Z_2 f_{ksp}|^2_{(x)} (dx), \]

where \( Z_q \) is shown at the bottom of the next page, \( q = 1, T_1 = \epsilon / M_S P, q = 2, T_2 = e / I_n, \theta_n = \cos \left( \frac{2^{n} - 1}{2} \theta_1 \right), c_{n1} = \frac{RS}{2} (1 + \theta_n), \epsilon = \max \left\{ \frac{\epsilon_1}{\epsilon_2 - \epsilon_1}, \frac{\epsilon_2}{\epsilon_1} \right\}, \epsilon_1 = 2^{R_n} - 1, \epsilon_2 = 2^{R_m} - 1. \]

**Proof:** See Appendix B.

According to **Theorem 1**, the reliability of the SU-Rn can be improved by increasing the transmission power, while the primary user interference temperature constraint will become the bottleneck to constrain and control the reliability level of the SU-Rn. Following the NOMA rule, the SU-Rn decodes the SU-Rm’s signal before decoding its own signal. Therefore, the value of power allocation factor \( \alpha \) and the codeword rate of the SU-Rm have a direct impact on the COP of the SU-Rn. In addition, the greater the inter-cell interference, the more unfavorable the COP of the SU-Rn.

**Theorem 2:** The COP of the SU-Rm can be given by

\[ P_{co}^{m} = Z_3 \times F_{ksp}|^2_{(x)} \left( \frac{I_n}{P M_S} \right) + \int_{\frac{I_n}{P M_S}}^{\infty} Z_2 f_{ksp}|^2_{(x)} (dx), \]

where \( Z_q \) is shown at the bottom of the next page, \( q = 1, T_3 = \delta / M_S P, q = 2, T_4 = e / I_n, \delta = \max \left\{ \frac{\delta_1}{\delta_2 - \delta_1}, \frac{\delta_2}{\delta_1} \right\}, \theta_n = \cos \left( \frac{2^{n} - 1}{2} \theta_1 \right), c_{n1} = \frac{RS}{2} (1 + \theta_n), \delta_1 = 2^{R_m} - 1, \delta_2 = 2^{R_n} - 1. \]

**Proof:** See Appendix C.

It can be deduced from **Theorem 2** that the COP of the SU-Rm decreases with the increase of power allocation factor. This means that when the system satisfies the interference temperature constraint of the PU-Rx, more power...
is allocated to the SU-Rm by increasing the transmission power, which is conducive to improving the reliability of the SU-Rm. In addition, the SU-Rm is subject to the common interference between the SU-Rn and the inter-cell networks. The reliability of the SU-Rm will deteriorate with the increase of common interference.

B. SOP OF PAIRED USERS

The secrecy outage happens when eavesdropping channel capacity grows up to the redundancy rate of wiretap code [10]. We consider a most detrimental eavesdropper who receives the highest SINR. The SOP equals to the probability that at least one of the eavesdopers in $\Phi_E$ causes a secrecy outage. We adopt the SOP as a measure of the security performance. The SOPs of the SU-Rn and SU-Rm and SU-Rm can be written as

$$P_{so}^n = \Pr \left( \max_{E \in \Phi_E} \left( \frac{\alpha M_SP_U|h|^2 L(r_e)}{I_e + \sigma_r^2} \right) > 2^{R_n} - 1 \right),$$

(18)

and

$$P_{so}^m = \Pr \left( \max_{E \in \Phi_E} \left( \frac{(1-\alpha) M_SP_U|h|^2 L(r_e)}{\alpha M_SP_U|h|^2 L(r_e) + I_e + \sigma_r^2} \right) > 2^{R_m} - 1 \right),$$

(19)

where $R_n$ and $R_m$ are the confidential information rates of the SU-Rn and SU-Rm, respectively. For deriving the closed-form expressions of (18) and (19), we first give the following Lemma.

Lemma 2: The CDF of the SINR of the most malicious eavesdropper are given by

$$F_{\gamma}(x) \approx \sum_{i=1}^{N} \frac{\sqrt{1 - \bar{\theta}_m^2}}{4N \cos^2 \bar{\theta}_m} \frac{f_{1+\alpha}^L(\tan \bar{\tau}_m)}{x} \exp \left( -\bar{\theta}_m \lambda_E \sum_{\tau \in [L,N]} \sigma_r (x, \zeta) \right),$$

(20)

where $\bar{\theta}_m = \cos \left( \frac{(2m-1)^{\pi}}{2N} \right)$, $\bar{\tau}_m = \frac{\pi}{4} (1 + \bar{\theta}_m)$, and

$$f_{1+\alpha}^L(\zeta) \approx \frac{2^{-\Delta} e^{-\frac{\Delta}{2}}}{\zeta} \sum_{b=0}^{B} \binom{B}{b} \sum_{c=0}^{C+b} \frac{(-1)^c x c_n}{D_c} \Re \left( \mathcal{L}_{x+\sigma_r^2}(u) \right),$$

(21)

where $D_c$ equal to 2 or 1 with the condition of $c = 0$ or $c = 1, 2, \ldots, s = \frac{(A+2\pi c)}{\pi}$. $Re(y)$ represents the real part of $y$, $\bar{\tau}_m = \cos \left( \frac{(2m-1)^{\pi}}{2N} \right)$, $\bar{\theta}_m = \frac{\pi}{4} (1 + \bar{\theta}_m)$, and $\sigma_r (x, \zeta)$ is shown at the bottom of the next page, and the value of $\Delta$ for the SU-Rm is as follows:

$$\Delta = \begin{cases} N_{T} \left( \frac{\bar{\tau}_m}{\alpha M_SP_C}, \frac{P}{I_w} \right), & P \leq M_S|h|^2 L(r_{sp}), \\ N_{T} \left( \frac{\bar{\tau}_m}{\alpha M_SP_C}, \frac{P}{I_w} \right), & P > M_S|h|^2 L(r_{sp}), \end{cases}$$

(23)

The value of $\Delta$ for the SU-Rm is as follows:

$$\Delta = \begin{cases} N_{T} \left( \frac{\bar{\tau}_m}{(1-\alpha) M_SP_C}, \frac{P}{I_w} \right), & P \leq M_S|h|^2 L(r_{sp}), \\ N_{T} \left( \frac{\bar{\tau}_m}{(1-\alpha) M_SP_C}, \frac{P}{I_w} \right), & P > M_S|h|^2 L(r_{sp}), \end{cases}$$

(24)

Proof: See Appendix D.

Then, the following theorem gives SOP of the NOMA users.

Theorem 3: The SOP achieved by the $k$-th SU-Rx, $k \in \{n, m\}$, can be written as (25), as shown at the bottom of the next page, where $\epsilon_{nm} = 2^{R_n} - 1$, $\epsilon_{ms} = 2^{R_m} - 1$.

Proof: See Appendix E.

It can be deduced from Theorem 3 that the decrease of the interference temperature constraint of the PU-Rx and the increase of the sector secrecy guard zone are both conducive to the improvement of the secrecy performance of the paired NOMA users. In addition, although the interference between networks is not helpful for the reliability of paired NOMA users, greater inter-cell interference is beneficial to the security of paired NOMA users.

C. ST OF PAIRED USERS

Although COP and SOP describe reliability and secrecy performance metrics for the NOMA users, respectively, they are insufficient to evaluate both reliability and secrecy performance for the NOMA users. In response to this, the proposed ST characterizes the joint security and reliability performance.

Theorem 4: The ST achieved by the SU-Rn can be written as

$$\eta^n = R^n F_{\gamma}(\epsilon_{nm}) (1 - Z_1) F_{|h|^2 L} \left( \frac{I_w}{PM_S} \right) + R^n \int_{\frac{I_w}{PM_S}}^{\infty} F_{\gamma}(\epsilon_{nm}) (1 - Z_2) f_{|h|^2 L}(x) \, dx,$$

(26)

$$Z_q \approx 1 - \sum_{n=1}^{N} \sum_{k \in [L,N]}^{N-1} \frac{\pi c_{n1}}{\sigma_n R_D1} \sqrt{1 - \theta_n^2 I_{n1} P_t (c_{n1})} \left( \frac{N_{T} T_{q1} \alpha^2}{C_t} \right) \mathcal{L}_{x+\sigma_{n1}^2}^{(j)} \left( \frac{N_{T} T_{q1} \alpha^2}{C_t} \right),$$

(12)

$$Z_p \approx 1 - \sum_{n=1}^{N} \sum_{k \in [L,N]}^{N-1} \frac{\pi c_{n3}}{N \eta R_D1 + R_D2} \sqrt{1 - \theta_n^2 I_{n3} P_t (c_{n3})} \left( \frac{N_{T} T_{p1} \alpha^2}{C_t} \right) \mathcal{L}_{x+\sigma_{n3}^2}^{(j)} \left( \frac{N_{T} T_{p1} \alpha^2}{C_t} \right),$$

(17)
It should be noted that in (26), $\varepsilon$ in $Z_1$ and $Z_2$ need to be replaced by $\varepsilon_2/\alpha$.

**Proof:** See Appendix F.

**Theorem 5:** The ST achieved by the SU-Rm is given by

$$
\eta^m = R_m^o F_{\gamma_m} (\varepsilon_{ms}) (1 - Z_3) F_{|\beta_{SP}|^2} \left( \frac{I_w}{PM_S} \right)
+ R_m^o \int_{\frac{I_w}{\alpha_m}}^\infty F_{\gamma_m} (\varepsilon_1) (1 - Z_4) f_{|\beta_{SP}|^2} (x) \, dx.
$$

(27)

**Proof:** See Appendix H.

As can be seen from **Theorem 4** and **Theorem 5**, the security and reliability of paired SU-Rn or SU-Rm are equally important to ST, but it is elusive to improve ST by improving security and reliability at the same time. Therefore, ST can compromise the security and reliability of such network. In addition, ST can be increased by increasing the radius of sector guard zone. Increasing the antenna gain or transmitting power of SU-Tx can enhance the reliability of such system. Meanwhile, it may reduce the secrecy performance, resulting in limited improvement of ST. The power allocation factor between paired NOMA users is also an important parameter of system performance, which should be carefully designed to obtain better system performance and user fairness. Furthermore, the interference temperature constraint $I_w$ of the PU-Rx and the inter-cell interference play a key role in the security and reliability of the paired SU-Rn or SU-Rm of the secondary network. It is necessary to reasonably design network parameters according to the actual network situation to achieve better network’s performance.

**IV. NUMERICAL RESULTS**

In this section, we provide more representative simulation results to characterize the reliability and secrecy performance of mmWave NOMA aided CR networks and the impact of different system parameters. Unless otherwise stated, the results of the following system parameter values have been obtained. The carrier frequency is 28 GHz, in which their LOS and NLOS path loss exponents are $\beta_L = 2$ and $\beta_N = 2.92$ [5]. The density of the SU-Txs is $\lambda = 10^{-3} / m^2$. The thermal noise power is -90 dBm. The Nakagami fading parameters of the LOS (NLOS) link are $N_L = 3$ ($N_N = 2$), the path-loss model:

$$
\alpha_L = 61.4 \, dB, \alpha_N = 72 \, dB. \quad C_L = 10^{-10} / \gamma \quad \text{and} \quad C_N = 10^{-10} / \gamma
$$

can be regarded as path-loss intercepts on the reference distance of LOS and NLOS links [48]. The parameter of the blockage is $\beta = 1/141.4$. BPCU is the abbreviation for bit per channel use. The main lobe and side lobe transmit the directivity gains are $M_S = 200$ and $m_S = 0.1$, respectively.

Fig. 2 plots the COP versus the transmit power $P$ for different paired NOMA users. As a benchmark for comparison, OMA adopts TDMA, and SU-Rn and SU-Rm each is allocated half time slot. The results show that: 1) The COP of paired NOMA users decreases gradually with the increase of $P$, and then reaches to error floor as $P$ further increases. This is due to the fact that $P$ on SU-Tx is constrained by $I_w$; 2) For the different paired NOMA users, the COP of NOMA is better than that of OMA. It can be seen that under reasonable design conditions, reliability performance of NOMA may outperform OMA in mmWave NOMA aided CR networks.

**Fig. 2.** The COP versus $P$ with $\lambda_L = 0.0002$ nodes/m$^2$, $R_n = 2$ BPCU, $R_m = 1$ BPCU, $R_{D1} = 40$ m, $R_{D2} = 70$ m, $\mu = 1/2$, $\sigma = 0.25$.

Fig. 3 plots the COP versus the power allocation factor $\alpha$ for different paired NOMA users, where Case I: $R_n = 1$ BPCU, $R_m = 0.5$ BPCU, Case II: $R_n = 1$ BPCU, $R_m = 1$ BPCU and Case III: $R_n = 1$ BPCU, $R_m = 1.5$ BPCU. We observe that: 1) The COP of the SU-Rm increases gradually with the increase of $\alpha$. The reason is that the power allocated to the SU-Rm will decreases with the increase of $\alpha$;
the increase of $\alpha$ that: 1) The SOP of the SU-Rn increases gradually with the increase of $\alpha$; 2) The SOP of the SU-Rm decreases gradually with the increase of $\alpha$. This is because that the power allocated to SU-Rm decreases with the increase of $\alpha$, which makes it more difficult for eavesdropper to intercept SU-Rm’s message; 3) The secrecy performance of paired NOMA users is improved with the increase of security redundancy rate.

Fig. 5 presents the SOP as a function of the interference temperature constraint $I_w$ for the different paired NOMA users. The results show that: 1) With the increase of $I_w$, the SOP curve gradually rises, which indicates that the secrecy performance of the paired NOMA users becomes worse; 2) For the paired NOMA users, increasing the radius of the sector secrecy guard zone is more conducive to improve the secrecy performance. In addition, under the same radius of sector secrecy guard zone, the secrecy performance of SU-Rn is better than that of SU-Rm. This is mainly because according to the NOMA power domain principle, the power allocated by SU-Rm is greater than that of SU-Rn, which increases the risk of information eavesdropping of SU-Rm; 3) Each SOP curve has a floor with the increase of $I_w$, which is mainly caused by the mmWave NLOS or LOS link.

Fig. 6 shows the ST as a function of the transmit power $P$ for the different paired NOMA users. The results show that: 1) Both SU-Rn and SU-Rm, the curves of ST first increase and then decrease as a function of $P$, which indicates that there exists a maximized ST optimized by the transmit power; 2) When the value of $P$ is large, the interference temperature constraint threshold $I_w$ of primary user could limit the transmit power at SU-Tx, which affects the performance of the secondary user’s ST. Moreover, in the region of high transmission power, the floor reached by ST is relatively low whether the threshold $I_w$ is large or small. This is due to the fact that when the value of $I_w$ is too small, reliability is the main factor restricting the system. When the value of $I_w$ is large, security becomes the main factor limiting the system. Therefore, from the perspective of considering the security
and reliability of the system, $I_w$ plays a vital role in the performance of the secondary networks; 3) The transmission power corresponding to the maximum value of ST obtained by SU-Rn and SU-Rm is different, which means that in the actual network design, the network parameters should be designed reasonably according to the different needs of users.

When the environment is full of physical obstacles, the probability of reaching the paired user’s information decreases, and the ST decreases until it saturates. On the other hand, when $\beta$ increases first and then decreases, an optimal $\beta$ is shown to make ST reach the maximum value; 2) For a given small $\lambda w$ value, when $\lambda$ takes a larger value, the ST of the paired users increases first and then decreases, and there is an optimal $\beta$ to make ST reach the maximum value; 2) For a given small $\lambda$ value, when $I_w$ takes a smaller value, the ST of the paired users also increases first and then decreases, and there is an optimal $\beta$ to make ST reach the maximum value. When $I_w$ takes a larger value, it means that the interference threshold of the PU-Rx increases. At this time, the ST of SU-Rm gradually decreases, while an optimal ST still exists in SU-Rn; 3) For the far SU-Rm, the larger $\lambda$ value will increase the interference and lead to the decrease of reliability. Therefore, a smaller $\lambda$ value is more beneficial to the PU-Rx. For the near SU-Rn, although a larger $\lambda$ value can increase the interference, it can also further increase the secrecy performance. Therefore, a larger $\lambda$ value is more beneficial to the SU-Rn. From the above analysis, it can be seen that increasing $\beta$ or $\lambda$ does not result in a strict decrease in ST for paired NOMA users. This is mainly because with the increase of $\beta$, NLOS communication is dominant in mmWave networks, and the ST of the paired users is obtained by using multipath signals. When the environment is full of physical obstacles, the probability of reaching the paired user’s information decreases, and the ST decreases until it saturates. On the other hand, with the increase of $\lambda$, the inter-cell interference increases, but at the same time, the secrecy performance is improved. Therefore, in some environments with high blockage density, $\beta$ and $\lambda$ can be set reasonably to achieve the best network’s performance.

**Fig. 8** presents the ST of the different paired NOMA users as a function of the blockage density $\beta$ for the different density $\lambda$ of the SU-Txs and interference temperature constraint $I_w$. The results show that: 1) For a given small $I_w$ value, when $\lambda$ takes a larger value, the ST of the paired users increases first and then decreases, and there is an optimal $\beta$ to make ST reach the maximum value; 2) For a given small $\lambda$ value, when $I_w$ takes a smaller value, the ST of the paired users also increases first and then decreases, and there is an optimal $\beta$ to make ST reach the maximum value. When $I_w$ takes a larger value, it means that the interference threshold of the PU-Rx increases. At this time, the ST of SU-Rm gradually decreases, while an optimal ST still exists in SU-Rn; 3) For the far SU-Rm, the larger $\lambda$ value will increase the interference and lead to the decrease of reliability. Therefore, a smaller $\lambda$ value is more beneficial to the SU-Rm. For the near SU-Rn, although a larger $\lambda$ value can increase the interference, it can also further increase the secrecy performance. Therefore, a larger $\lambda$ value is more beneficial to the SU-Rn. From the above analysis, it can be seen that increasing $\beta$ or $\lambda$ does not result in a strict decrease in ST for paired NOMA users. This is mainly because with the increase of $\beta$, NLOS communication is dominant in mmWave networks, and the ST of the paired users is obtained by using multipath signals. When the environment is full of physical obstacles, the probability of reaching the paired user’s information decreases, and the ST decreases until it saturates. On the other hand, with the increase of $\lambda$, the inter-cell interference increases, but at the same time, the secrecy performance is improved. Therefore, in some environments with high blockage density, $\beta$ and $\lambda$ can be set reasonably to achieve the best network’s performance.

**Fig. 7** shows the ST as a function of the density $\lambda$ of the SU-Txs for the different paired NOMA user. The results show that: 1) For paired NOMA users, ST increases first and then decreases with the increase of $\lambda$. This shows that there is an optimal $\lambda$ to maximize ST; 2) When $\lambda$ is in a small region, $\lambda$ decreases with the increase of $\lambda$, which means that in the actual design of the network, the interference between the networks should be fully considered to achieve the optimal network performance; 3) With the different interference temperature constraints of primary users, the ST obtained by pairing NOMA users is different. For SU-Rn and SU-Rm, it is found that a corresponding to the maximum value of ST is different, which shows that it needs to be reasonably constructed according to different needs of users in the actual network design.
The first term in (29), as shown at the bottom of the next page, can be found as follows:

\[ A_1 = \int_0^{\frac{2\pi}{R_{d_F}}} \Pr \left( |h_{s'|}^2 < \frac{e \left( I_n + \sigma_n^2 \right)}{M_S PL \left( r_n \right)} \right) f_{|h_{s'|}^2} (x) \, dx, \quad (30) \]

In the following, we calculate \( Z_1 \) in detail, \( Z_1 \) can be calculated as

\[ Z_1 = \sum_{\tau \in [L, N]} \Pr \left( |h_{s'|}^2 < \frac{e \left( I_n + \sigma_n^2 \right)}{M_S PL \left( r_n \right)} \right) \quad (31) \]

Then, \( \Omega_1 \) can be calculated as follows:

\[ \Omega_1 = \Pr \left( |h_{s'|}^2 < \frac{e \left( I_n + \sigma_n^2 \right)}{M_S PL \left( r_n \right)} \right) \]

\[ \Omega_1 = 1 - \sum_{i = 0}^{N_i - 1} \frac{(-u)^i}{i!} \mathcal{L}(\lambda\sigma_n^2\alpha_s \frac{r_{n,\tau}}{M_S PC_{\tau}}) \left( u \right) \bigg|_{u = \frac{N_r\sigma_n^2\alpha_s}{M_S PC_{\tau}}} \quad (32) \]

where step (c) follows the channel assumption previously that \( |h_{s'|}^2 \) is a normalized Gamma random variable with following \( \Gamma \left( N_L, 1/1 \right) \) and \( \Gamma \left( N_N, 1/1 \right) \). \( \mathcal{L}(\lambda\sigma_n^2\alpha_s \frac{r_{n,\tau}}{M_S PC_{\tau}}) \left( u \right) = \exp \left( -u \frac{\sigma_n^2\alpha_s}{M_S PC_{\tau}} \right) \) is the Laplace transform of the interference \( I_n \) multiplied by the coefficient associated with signal-to-noise ratio (SNR).

The Laplace transform for calculating \( I_n \) is as follows:

\[ E \{ \exp (-u_l,\tau) \} = E_{\Phi_L} \left\{ \exp (-u_l,\tau,\tau) \right\} \quad (33) \]

where \( I_n,\tau = \sum_{\tau \in \Phi_L, \tau_0} P_{G,f_n} |h_{j,\tau}^2| L_L \left( r_{j,\tau} \right) \), \( I_n,\tau = \sum_{\tau \in \Phi_L, \tau_0} P_{G,f_n} |h_{j,\tau}^2| L_N \left( r_{j,\tau} \right) \), \( \Phi_L \) and \( \Phi_N \) are the point processes of the LOS and NLOS of the SU-Txs, respectively. \( y_0 = \Phi_L + \Phi_N \). According to the Laplace transform, the calculation of \( I_n,\tau \) can be expressed as

\[ E_{\Phi_L} \left\{ \exp (-u_l,\tau,\tau) \right\} = \exp \left( -\lambda \int_{\mathbb{R}^2} \left( 1 - \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \frac{P_L \left( \|x\| \right)}{dx} \right) \]

\[ = \exp \left( -\lambda \int_{\mathbb{R}^2} \left( 1 - \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \frac{P_L \left( r \right)}{dr} \right) \]

\[ = \exp \left( -2\pi \lambda \int_0^\infty \sum_{q = 1}^{2} b_q \int_0^\infty \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \]

\[ = \exp \left( x \int_{\mathbb{R}^2} \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \]

\[ = \exp \left( -2\pi \lambda \int_0^\infty \sum_{q = 1}^{2} b_q \int_0^\infty \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \]

\[ = \exp \left( -\lambda \int_{\mathbb{R}^2} \left( 1 - \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \frac{P_L \left( |x| \right)}{dx} \right) \]

\[ = \exp \left( -\lambda \int_{\mathbb{R}^2} \left( 1 - \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \frac{P_L \left( r \right)}{dr} \right) \]

\[ = \exp \left( -2\pi \lambda \int_0^\infty \sum_{q = 1}^{2} b_q \int_0^\infty \frac{1}{1 + \frac{u \frac{P_{G,f_n} C_s \lambda} {N_s^{\lambda}} \|x\|^\lambda}} \right) \]
\[ \begin{align*}
&= \exp \left( -2\pi \lambda \sum_{q=1}^{2} b_q \int_{0}^{z} \left( 1 - \frac{1}{1 + \frac{uPA_qC_{Lm}}{N_L\tan \ell z_o}} \right) \right) \\
&\times p_L \left( \tan z_o \right) \sin z_o \cos^2(z_o) dz_o \\
&\approx \exp \left( -\frac{\pi^3}{2N} \sum_{q=1}^{2} \sum_{m=1}^{N} b_q \sqrt{1 - \vartheta_m^2} \right) \\
&\times \sin \frac{\tau_m}{\cos \frac{\tau_m}{\cos \frac{\tau_m}{\cos \frac{\tau_m}{\cos \frac{\tau_m}}}} \left( 1 - \left( 1 + \frac{uPA_qC_{Lm}}{N_L\tan \ell \tau_m} \right)^{-N} \right) \right), \quad (34)
\end{align*} \]

where step (d) applies the Laplace transform of the gamma random variable \(|h_{m}|^2\), step (e) averages the random directional gain and applies PGFL of HPPP, step (f) applies the polar coordinate transformation, step (g) takes \(z_o = \arctan r\) to replace, step (h) adopts Gauss-Chebyshev approximation.

Similar to the process of obtaining (34), the Laplace transform of \(I_{n,N}\) can be expressed as

\[ \begin{align*}
E_{\phi N} \{ \exp \{ -\alpha I_{n,N} \} \} \\
&= \exp \left( -\frac{\pi^3}{2N} \sum_{q=1}^{2} \sum_{m=1}^{N} b_q \sqrt{1 - \vartheta_m^2} \right) \\
&\times \sin \frac{\tau_m}{\cos \frac{\tau_m}{\cos \frac{\tau_m}{\cos \frac{\tau_m}}}} \left( 1 - \left( 1 + \frac{uPA_qC_{Lm}}{N_L\tan \ell \tau_m} \right)^{-N} \right), \quad (35)
\end{align*} \]

Based on (33)-(35), we obtain \(L_{(I_n+\sigma_n)}(u) = \exp(\eta(u))\). With the help of Leibniz rule, we finally get (15). After some mathematical manipulations, upon substituting \(\Omega_1\) into (31), we obtain \(Z_1\).

The second term in (29) can be expressed as follows:

\[ \begin{align*}
\Lambda_2 &= \int_{\frac{I_{n,N}}{P_{in}}}^{\infty} \Pr \left( \frac{N_{m}|h|^2}{\alpha M_S P^L} - \frac{\varphi}{\ell} \left( \frac{I_{n,N}}{\alpha M_S P^L} \right) \right) x f_{|h|^2}(x) dx, \quad (36)
\end{align*} \]

where \(Z_2\) can be calculated by a procedure similar to \(Z_1\), which can be omitted for brevity.

Substituting (30) and (36) into (29), (11) can be obtained.

**APPENDIX C**

Base on (8), \(P_{in}^{m}\) can be further divided into two terms, shown at the bottom of the next page.

The first term in (37), as shown at the bottom of the next page, can be found as follows:

\[ \Lambda_3 = \int_{\frac{I_{n,N}}{P_{in}}}^{\infty} \Pr \left( \frac{N_{m}|h|^2}{\alpha M_S P^L} - \frac{\varphi}{\ell} \left( \frac{I_{n,N}}{\alpha M_S P^L} \right) \right) x f_{|h|^2}(x) dx, \quad (38) \]

Correspondingly, the second term in (37) can be expressed as follows:

\[ \Lambda_4 = \int_{\frac{I_{n,N}}{P_{in}}}^{\infty} \Pr \left( \frac{N_{m}|h|^2}{\alpha M_S P^L} - \frac{\varphi}{\ell} \left( \frac{I_{n,N}}{\alpha M_S P^L} \right) \right) x f_{|h|^2}(x) dx. \quad (39) \]

Based on (38) and (39), \(Z_3\) and \(Z_4\) can be calculated by a procedure similar to \(Z_1\), which can be omitted for brevity.

Substituting (38) and (39) into (37), (16) can be obtained.

**APPENDIX D**

**Lemma 2** can be derived as

\[ \begin{align*}
F_{y_c}(x) &= \Pr \left( \max_{E \in \Phi E} \left( \frac{\alpha M_S P|h|^2}{\ell} + \frac{\sigma^2_n}{\ell} \right) < x \right) \\
&= E_{\phi E, I_e} \left\{ \prod_{E \in \Phi E} \Pr \left( \frac{\alpha M_S P|h|^2 \ell}{\ell} + \frac{\sigma^2_n}{\ell} < x \right) \right\} \\
&\approx E_{I_e} \left\{ \exp \left( -\theta_{I_e} \sum_{r \in [L,N]} \int_{r}^{\infty} \Pr \left( \frac{|h|^2}{\ell} + \frac{\sigma^2_n}{\ell} \right) r e^{\frac{\ell}{\alpha M_S P^L}} r d r \right) \right\}, \quad (40)
\end{align*} \]

where step (i) applies PGFL of HPPP.

To further derive (40), we can formulate

\[ \begin{align*}
\sigma_{\alpha}(x, \varphi) &= \int_{r}^{\infty} \Pr \left( \frac{|h|^2}{\ell} + \frac{\varphi}{\ell} \left( \frac{I_{n,N}}{\alpha M_S P^L} \right) \right) r e^{\frac{\ell}{\alpha M_S P^L}} r d r \\
&= \int_{r}^{\infty} \Gamma \left( \frac{N_{m}|h|^2}{\alpha M_S P^L} \right) r e^{\frac{\ell}{\alpha M_S P^L}} r d r \\
&\approx \int_{\frac{\ell}{\alpha M_S P^L}}^{\infty} \Gamma \left( \frac{N_{m}|h|^2}{\alpha M_S P^L} \right) r e^{\frac{\ell}{\alpha M_S P^L}} r d r \sin z_p \cos \frac{\ell}{\alpha M_S P^L} d z_p, \quad (41)
\end{align*} \]
where step (j) takes \( z_p = \arctan r_e \) to replace. \( \Gamma (\cdot, \cdot) \) is the upper incomplete gamma function \([47]\). After Gaussian-Chebyshev approximation, (22), as shown at the bottom of page 7, can be obtained.

Now, we turn our attention on (40), which is given by

\[
F_{\gamma_e}(x) = \int_{0}^{\infty} f_{\left(t_{w+\frac{z_{\gamma}}{2}}(x)\right)}(\sigma) \exp \left(-\theta_\lambda L_E \sum_{\tau \in \{L, N\}} \sigma_\tau (x, \xi)\right) d\sigma \leq \sum_{i=1}^{N} \left(1-\frac{\bar{I}_e}{\theta_\lambda L_E} \right)^{2}(4N \cos^2 \bar{\gamma}_m) f_{\left(t_{w+\frac{z_{\gamma}}{2}}(x)\right)}(\tan \bar{\gamma}_m) \times \exp \left(-\theta_\lambda L_E \sum_{\tau \in \{L, N\}} \sigma_\tau (x, \tan \bar{\gamma}_m)\right). \tag{42}
\]

where step (w) applies the polar coordinate transformation and Gaussian-Chebyshev approximation. Combined with SU-Rm, after a similar mathematical manipulation, (20) can be obtained.

**APPENDIX E**

Base on (18), the SOP of the SU-Rn is given by

\[
P_{n} = \Pr \left\{ \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ns}} \right\} = \Pr \left\{ \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ns}} \right\} \leq \int_{0}^{\tau_{\text{ns}}} \left(1 - F_{\gamma_e} \left( \frac{(I_e + \sigma_e^2) \varepsilon_{\text{ns}} \bar{\gamma}_e}{\alpha M_s P C_\tau} \right) \right) f_{|h|^2 (x)}(\sigma) \, d\sigma \leq \int_{0}^{\tau_{\text{ns}}} \left(1 - F_{\gamma_e} \left( \frac{(I_e + \sigma_e^2) \varepsilon_{\text{ns}} \bar{\gamma}_e}{\alpha M_s P C_\tau} \right) \right) f_{|h|^2 (x)}(\sigma) \, d\sigma. \tag{43}
\]

Combined with SU-Rm, after a similar mathematical manipulation, (25) can be obtained. The proof is completed.

**APPENDIX F**

To measure the joint performance of a paired user that is both reliable and secure, ST of the SU-Rn is given by

\[
\eta'' = R_n \Pr \left( \gamma_{e-n} < 2(R_{r_n} - R_m) - 1, \gamma_m > 2R_m - 1 \right)
\]

\[
= R_n \Pr \left( \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ns}}, \frac{\alpha M_s p L_m}{|h|^2 L (r_m) + \sigma_m^2} > \varepsilon_1, P \leq \frac{I_w}{M_s |h|^2 L (r_m) + \sigma_m^2} \right) + R_n \Pr \left( \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ns}}, \frac{\alpha M_s p L_m}{|h|^2 L (r_m) + \sigma_m^2} > \varepsilon_1, P > \frac{I_w}{M_s |h|^2 L (r_m) + \sigma_m^2} \right)
\]

\[
= R_n \int_{0}^{\tau_{\text{ns}}} F_{\gamma_e} (\varepsilon_{\text{ns}}) (1 - Z_1) f_{|h|^2} (x) \, dx + R_n \int_{0}^{\tau_{\text{ms}}} F_{\gamma_m} (\varepsilon_{\text{ms}}) (1 - Z_1) f_{|h|^2} (x) \, dx. \tag{44}
\]

Upon substituting (20), (12), as shown at the bottom of page 6, and (10) into (44), we can obtain (26).

Furthermore, ST of the SU-Rm can be calculated as follows:

\[
\eta'' = R_m \Pr \left( \gamma_{e-m} < 2(R_{r_m} - R_m) - 1, \gamma_m > 2R_m - 1 \right)
\]

\[
= R_m \Pr \left( \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ms}}, \frac{\alpha M_s p L_m}{|h|^2 L (r_m) + \sigma_m^2} > \varepsilon_1, P \leq \frac{I_w}{M_s |h|^2 L (r_m) + \sigma_m^2} \right) + R_m \Pr \left( \max_{E \in \Phi_E} \left( \frac{\alpha M_s p L_m}{|h|^2 L (r_e)} \right) > \varepsilon_{\text{ms}}, \frac{\alpha M_s p L_m}{|h|^2 L (r_m) + \sigma_m^2} > \varepsilon_1, P > \frac{I_w}{M_s |h|^2 L (r_m) + \sigma_m^2} \right)
\]

\[
= R_n \int_{0}^{\tau_{\text{ms}}} F_{\gamma_m} (\varepsilon_{\text{ms}}) (1 - Z_1) f_{|h|^2} (x) \, dx + R_n \int_{0}^{\tau_{\text{ms}}} F_{\gamma_m} (\varepsilon_{\text{ms}}) (1 - Z_1) f_{|h|^2} (x) \, dx. \tag{44}
\]
\begin{equation}
R_m^s \int_0^{\text{max}_m} \int_{-\infty}^{\infty} F_{Y \epsilon}(\epsilon_m) (1 - Z_2) f_{[\text{mu}]}(x) \, dx \\
+ R_m^s \int_0^{\text{max}_m} \int_{-\infty}^{\infty} F_{Y \epsilon}(\epsilon_1) (1 - Z_2) f_{[\text{mu}]}(x) \, dx.
\end{equation}
(45)

Following similar steps, upon substituting (20), (17), as shown at the bottom of page 6, and (10) into (45), we can obtain (27). The proof is completed.

REFERENCES

[1] Z. Ding, R. Schober, and H. V. Poor, “A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment,” IEEE Trans. Wireless Commun., vol. 15, no. 6, pp. 4438–4454, Jun. 2016.

[2] 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., vol. 8, no. 3, pp. 905–908, Jun. 2019.

[3] M. Xiao, S. Munttaz, Y. Huang, L. Dai, Y. Li, M. Matthaiou, G. K. Karagiannidis, E. Bjornson, K. Yang, I. Chih-Lin, and A. Ghosh, “Millimeter wave communications for future mobile networks (Guest Editorial), Part I,” IEEE J. Sel. Areas Commun., vol. 35, no. 7, pp. 1425–1431, Jul. 2017.

[4] J. G. Andrews, T. Bai, M. Kulkarni, A. Alkhateeb, A. 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.

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

[6] K. Guan, D. He, B. Ai, D. W. Matolak, Q. Wang, Z. Zhong, and T. Kurner, “Millimeter wave communications against randomly located eavesdroppers,” IEEE Trans. Commun., vol. 67, no. 1, pp. 83–96, Jan. 2019.

[7] L. Zhu, J. Zhang, Z. Xiao, X. Cao, D. O. Wu, and X.-G. Xia, “Millimeter-wave NOMA with user grouping, power allocation and hybrid beamforming,” IEEE Trans. Wireless Commun., vol. 18, no. 11, pp. 5065–5079, Nov. 2019.

[8] Y. Sun, Y. W. S. Wong, and R. Schober, “Performance analysis of millimeter wave NOMA networks with beam misalignment,” IEEE Wireless Commun., vol. 17, no. 12, pp. 1–7, Dec. 2018.

[9] 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.

[10] Z. Ding, L. Dai, R. Schober, and H. V. Poor, “NOMA meets finite resolution analog beamforming in massive MIMO and millimeter-wave wireless communications,” IEEE Commun. Mag., vol. 57, no. 8, pp. 1879–1882, Aug. 2019.

[11] 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.

[12] Y. Sun, Z. Ding, and X. Dai, “On the performance of downlink NOMA in multi-cell mmWave networks,” IEEE Commun. Lett., vol. 22, no. 11, pp. 2366–2369, Nov. 2018.

[13] T. Bai, Z. Zhou, C. Xu, Y. Zhang, J. Rodrigue, and T. Sato, “Capacity analysis of NOMA with mmWave massive MIMO systems,” IEEE J. Sel. Areas Commun., vol. 35, no. 7, pp. 1606–1618, Jul. 2017.

[14] H. Hosseini, A. Anpalagan, S. Habib, K. Raahemifar, and S. Erkucuk, “Joint wavelet-based spectrum sensing and FBMC modulation for cognitive mmWave small cell networks,” IET Commun., vol. 10, no. 14, pp. 1803–1809, Sep. 2016.

[15] H. Hosseini, A. Anpalagan, K. Raahemifar, and S. Erkucuk, “Wavelet-based cognitive SCMA system for mmWave 5G communication networks,” IET Commun., vol. 11, no. 6, pp. 831–836, Apr. 2017.

[16] J. Park, J. G. Andrews, and R. W. Heath, Jr., “Inter-operator base station coordination in spectrum-shared millimeter wave cellular networks,” IEEE Trans. Cognit. Commun. Netw., vol. 4, no. 3, pp. 513–528, Sep. 2018.

[17] H. Zhao, J. Zhang, L. Yang, G. Pan, and M.-S. Alouini, “Secure mmWave communications in cognitive radio networks,” IEEE Wireless Commun. Lett., vol. 8, no. 4, pp. 1171–1174, Aug. 2019.

[18] Y. Song, W. Yang, Z. Xiang, B. Wang, and Y. Cai, “On the performance of random cognitive mmWave,” Sensors, vol. 19, no. 44, pp. 1–14, Jul. 2019.

[19] Y. Song, W. Yang, X. Zhang, X. Bai, and B. Wang, “Physical layer security in cognitive millimeter wave networks,” IEEE Access, vol. 7, pp. 109162–109180, 2019.

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

[21] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, “Physical layer security in heterogeneous cellular networks,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 2, pp. 1204–1219, Mar. 2019.

[22] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Processing. (ICASSP), Mar. 2012, pp. 2809–2812.
[43] 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.

[44] Y. Song, W. Yang, Z. Xiang, B. Wang, and Y. Cai, “Secure transmission in mmWave NOMA networks with cognitive power allocation,” IEEE Access, vol. 7, pp. 76104–76119, 2019.

[45] 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.

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

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

[48] 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, Army Engineering University of PLA. His research interests include millimeter-wave, non-orthogonal multiple access, physical-layer security, and cognitive radio.

WEIWEI YANG 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 the 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, Army Engineering University of PLA. His research interests include non-orthogonal multiple access, physical-layer security, and cognitive radio.

NAN SHA received the B.S., M.S., and Ph.D. degrees in communications engineering from the College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2005, 2006, and 2014, respectively. He is currently a Lecturer with the Communications Engineering College, Army Engineering University of PLA. His research interests include physical-layer network coding, physical-layer security, and cooperative communications.

HUI WANG received the B.S. degree from the University of Electronic Science and Technology of China, in 2009, and the M.S. degree from Southeast University, in 2012, where he is currently pursuing the Ph.D. degree. His research interests include high-speed SerDes and optical transceivers circuits.

YUCUI YANG received the M.S. degree from the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, in 2006. She is currently with the School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, and also with the Jiangsu Province Key Construction Laboratory of Modern Measurement Technology and Intelligent System. Her current research interests include pattern recognition and image retrieval.

***