

On Secure mmWave RSMA Systems

Hongjiang Lei, Sha Zhou, Xihu Chen, Imran Shafique Ansari,
Yun Li, Gaofeng Pan, and Mohamed-Slim Alouini

Abstract—Millimeter-wave (mmWave) communication is one of the effective technologies for the next generation of wireless communications due to the enormous amount of available spectrum resources. Rate splitting multiple access (RSMA) is a powerful multiple access, interference management, and multi-user strategy for designing future wireless networks. In this work, a multiple-input-single-output mmWave RSMA system is considered wherein a base station serves two users in the presence of a passive eavesdropper. Different eavesdropping scenarios are considered corresponding to the overlapped resolvable paths between the main and the wiretap channels under the considered transmission schemes. The analytical expressions for the secrecy outage probability (SOP) are derived respectively through the Gaussian–Chebyshev quadrature method. Monte Carlo simulation results are presented to validate the correctness of the derived analytical expressions and demonstrate the effects of system parameters on the SOP of the considered mmWave RSMA systems.

Index Terms—Millimeter-wave, rate splitting multiple access, uniform linear array, secrecy outage probability.

I. INTRODUCTION

A. Background and Related Work

Nowadays, a growing number of electronic devices and various emerging applications have entered our daily routines, which bring about significant growth in the wireless data traffic of wireless networks and is likely to leap 10000 fold in the next 20 years [1]–[3]. To tackle this incredible growth, millimeter-wave (mmWave) has become one of the most efficient resolutions due to the plentiful underutilized spectrum resources [4]. Recently, mmWave communication has received substantial attention, such as channel modelling and estimation, beamforming strategy design, and performance analysis. The authors in [5] provided a comprehensive

overview of mathematical models and analytical techniques of mmWave cellular systems. A baseline mathematical method and analysis in blocking and substantial directionality aspects was proposed and the result indicated that the ultra-dense deployments were more available in mmWave systems. In [6], an adaptive algorithm was developed to estimate the mmWave channel parameters exploiting the sparse scattering of the channel and was extended to the case of the multi-path channel. The result shows that the proposed low-complexity channel estimation algorithm achieves more precoding gains and spectral efficiency than exhaustive algorithms. In [7], a hybrid precoding/combining designs of full-duplex amplify-and-forward mmWave relay systems was proposed. Their simulation indicated that the proposed design is approaching an all-digital scheme. A downlink non-orthogonal multiple access (NOMA) mmWave system was investigated in [8]. An opportunistic beam-splitting NOMA scheme was proposed to inquire into the antenna gain and the closed-form expressions of the coverage probability and the ASR were derived.

In next-generation communication networks and beyond, interference management becomes a fundamental problem for multi-user communications and multiple access design [9]. Rate-splitting multiple access (RSMA) as a candidate multiple access scheme has been proposed in [10] and has been recognized as a powerful multiple access, interference management, and multi-user strategy [11]. Based on the rate-splitting (RS) principle, RSMA not only displays more flexibility in managing interference, i.e., partially decodes interference of inter-user and partially treats interference as noise, but also unifies and generalizes orthogonal multiple access (OMA), space-division multiple access, NOMA, physical-layer multicasting [12], [13], [14]. A more flexible and powerful cooperative scheme for a multiple-input-single-output (MISO) broadcast channel scenario was proposed based on the three-node relay channel in [15]. Their simulation results show that the proposed cooperative RS strategy can obtain an explicit rate improvement than NOMA. In [16], linearly-precoded 1-layer and multi-layer transmission strategies based on the RS were investigated in a Non-Orthogonal unicast and multicast transmission system, which the weighted sum rate and energy efficiency problems were solved by weighted minimum mean square error algorithm and successive convex approximation algorithm. The Numerical results indicated that the RS-assisted transmission strategies are more efficient in spectrum and energy compared with multi-user linear- precoding, OMA and NOMA in extensive user deployments and network loads. Compared to rate region, sum rate, spectral and energy efficiency improvement in terms of optimization, the benefit of RSMA for performance analysis, such as throughput, ergodic sum rate (ESR), and outage probability (OP), also needs to

Manuscript received.

This work was supported by the National Natural Science Foundation of China under Grant 61971080. (Corresponding author: *Hongjiang Lei*.)

Hongjiang Lei is with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China, also with Chongqing Key Lab of Mobile Communications Technology, Chongqing 400065, China (e-mail: leihj@cqupt.edu.cn).

Sha Zhou and Xihu Chen are with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: cquptzhous@163.com; chenxhcqupt@163.com).

Imran Shafique Ansari is with James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom (e-mail: imran.ansari@glasgow.ac.uk).

Yun Li is with Chongqing Key Lab of Mobile Communications Technology, Chongqing 400065, China (e-mail: liyun@cqupt.edu.cn).

Gaofeng Pan is with the School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China (e-mail: gaofeng.pan.cn@ieee.org).

Mohamed-Slim Alouini is with CEMSE Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia (e-mail: slim.alouini@kaust.edu.sa).

be explored. In [17], the downlink unmanned aerial vehicle systems based on the RSMA scheme were investigated and the closed-form expressions of the OP and throughput at each user were derived. The performance of a multi-cell RSMA network was investigated in [18] wherein the analytical expressions for ESR and spectral efficiency based on stochastic geometry theory were derived. Their results showed that the power splitting ratio between common and private streams significantly impacts performance. Bansal A. *et al.* in [19] studied a novel Intelligent reflecting surface (IRS) RS framework of multi-user communication system, the closed-form expressions of OP for the far and near users were derived. The simulation results showed that the proposed framework was superior to the decode-and-forward-RS, RS without IRS, and IRS-NOMA scenarios.

Physical layer security (PLS), which utilizes the inherent characteristics of wireless channels, is an exciting complement to sophisticated cryptographic techniques [20]. Since the mmWave's propagation characteristics, which support large antenna arrays and highly directional transmission, can reduce the leakage of confidential information. Thus, physical layer security in mmWave communications has attracted considerable recent attention. Specifically, by using a sectorized model to analyze the beam pattern, the secrecy transmission of a mmWave cellular network was investigated in [21], the secure connectivity probability was studied and their results indicated the array pattern and intensity of eavesdroppers are both important network parameters for improving the secrecy performance. The author studied the physical layer security of mmWave relaying networks In [22] wherein developed a new joint relay selection and power allocation method in multiple eavesdroppers and relays, the closed-form expressions of average secrecy rate (ASR) and secrecy outage probability (SOP) were derived respectively and demonstrated the superiority of proposed method. Ju *et al.* in [23] utilized the discrete angular domain channel (DADC) model to analyze the secrecy performance of the mmWave MISO systems. Three transmission schemes were proposed to improve the secure mmWave systems. Further, they investigated the security mmWave MISO systems in the presence of multiple randomly located eavesdroppers in [24]. In [25], the multiple input multiple output DADC were developed in mmWave decode-and-forward relay systems. The secrecy performance with three eavesdropping scenarios was investigated by designing the corresponding beamforming strategies. Huang *et al.* investigated the secure mmWave NOMA systems in which all the authorized and unauthorized receivers were randomly located in [26]. Then, they proposed two schemes to improve the secrecy transmission and the closed-form SOPs for two beamforming schemes with varying eavesdropper detection abilities were derived.

As a novel, general, and robust framework for the sixth generation mobile communications, RSMA has a high potential to be used for security applications [27]. In [28], two decoding strategies were adopted by a near user and a far user to explore outage and secrecy outage performance. The closed-form expressions of OP and tight approximations of SOP were derived, considering four decoding combinations.

The author in [29] proposed two RS schemes with one-layer-successive interference cancellation (SIC) and two-layer-SIC wherein there is an untrusted near user. The closed-form expressions of OP and SOP are obtained to analyze outage performance. In [30], the secrecy performance of RSMA in multi-user MISO systems was investigated and analytical expressions of the ESR and ASR were obtained with zero-forcing precoding and minimum mean square error approach. The result demonstrated that proposed power allocation methods could offer inherent tradeoffs over the ESR and ASR.

In the RSMA scheme, the messages are split into common and private parts, encoded into a single common stream and private streams, respectively. All the common and private streams are superimposed, linearly precoded, and transmitted simultaneously by the transmitter. By utilizing SIC technology, the common stream is decoded firstly by treating all private streams as interference, removing from the received signals, and the private stream is decoded by treating the private streams for other users as interference. In the mmWave systems with the DADC model, depending on the spatial correlation of the users, the spatially resolvable paths are split into overlapped and non-overlapped paths. As thus, the following questions naturally arise: *Should the common streams be transmitted on overlapped paths or all paths? What is the performance of the mmWave systems with the RSMA scheme?* To answer these questions, the performance of the mmWave RSMA systems was investigated, and two beamforming transmission schemes were proposed in [32]. The closed-form expressions for the exact and asymptotic OP with proposed schemes were derived using stochastic geometry theory. The results demonstrated that RSMA helps improve transmission reliability of the mmWave systems. TABLE I outlines the typical works discussed.

B. Motivation and Contributions

To the best of the authors' knowledge, based on the open literature, there is a lack of research focused on the following issue: *Is it beneficial to leverage the RSMA scheme in mmWave systems for security enhancement?* Hence, this work answers this question by analyzing the secrecy performance of the mmWave RSMA systems. Different eavesdropping scenarios are considered corresponding to the overlapped resolvable paths between the main and the wiretap channels under the considered transmission schemes. Technically speaking, it is much more challenging to obtain the analytical expression of the SOP than that of the OP for the mmWave RSMA system since there are multiple parameters (random variables) that must be considered. We summarize the contributions of this work as follows.

- 1) The secrecy performance of the MISO mmWave RSMA system is investigated wherein the common and private streams are transmitted on the overlapping and non-overlapping paths, respectively. Different scenarios are considered based on the spatial correlation of the legitimate and illegitimate user and the principle of the RSMA scheme. Subsequently, the analytical expressions for the SOP are derived respectively through the Gaussian–Chebyshev quadrature method.

TABLE I: Related Literature on RSMA or mmWave systems.

Reference	RSMA	mmWave	Multi-antenna technology	Channel Model	PLS	Performance metric
[17]	✓			Nakagami- m		OP
[18]	✓		Transmitter	Rayleigh		ESR
[19]	✓			Rayleigh		OP
[21]		✓		Nakagami- m	✓	SCP
[22]		✓	Transmitter	Rayleigh	✓	SOP
[23]		✓	Transmitter	DADC	✓	SOP
[24]		✓	Transmitter	DADC	✓	SOP
[25]		✓	Transmitter & destination	DADC	✓	SOP
[26]		✓	Transmitter	DADC	✓	SOP
[28]	✓			Rayleigh	✓	OP and SOP
[29]	✓		Transmitter	Rayleigh	✓	OP and SOP
[30]	✓		Transmitter	Rayleigh	✓	ESR & ASR
[32]	✓	✓	Transmitter	DADC		OP
Our Work	✓	✓	Transmitter	DADC	✓	SOP

- 2) We present Monte Carlo simulation results to validate the correctness of the derived analytical expressions and demonstrate the effects of system parameters on the SOP of the considered mmWave RSMA systems. The result shows that the power allocation between the common and private streams and the number of overlapped paths significantly affect the secrecy performance.
- 3) Relative to [26] wherein the security mmWave NOMA systems were enhanced by the proposed beamforming schemes, the security mmWave RSMA system is improved by the proposed beamforming scheme in this work wherein the scenarios considered in this work are more challenging.
- 4) Relative to [28]-[31] wherein the secrecy performance of the RSMA systems with *internal* untrusted users was investigated. In these scenarios, it was assumed that the common message could always be decoded and only the private message was wiretapped. Technically speaking, it is much more challenging to investigate the secrecy performance of the RSMA systems with an *external* eavesdropper than with an internal eavesdropper.

C. Organization

The rest of this paper is organized as follows. Section II describes the system model and beamforming scheme. The analytical expressions for the exact SOP of mmWave RSMA systems is derived under different scenarios in Sections III. The simulation results are presents to valid the analysis in Section IV. Section V concludes this work. Table II lists the notations and symbols utilized throughout this work.

II. SYSTEM MODEL

A. System Model

As shown in Fig. 1, a downlink mmWave RSMA system is considered where the base station (S) communicates with two users denoted by U_1 and U_2 ¹ while an external passive

¹Similar to [10], [12], [14], the RSMA system with two users is considered in this work. As such, the results in this paper can serve as a benchmark for the performance of such systems. The performance of RSMA systems with multiple users will be part of our future work.

TABLE II: Notation and Symbols

Notation	Description
Ω_l	The index set of resolvable paths at l
\mathbf{g}_l	The complex gain vector between S and l
\mathbf{U}	The spatially orthogonal basis
L_l	The number of resolvable paths of l
$\Delta_{l,o}$	The angular range between the o th and $(o+1)$ th paths at l
$\omega_{l,o}$	The width between the o th and $(o+1)$ th paths at l
Ω_c	The index set of overlapped paths between U_1 and U_2
$\Omega_{i,p}$	The index set of non-overlapping paths at U_i
Ω_{ec}	The index set of overlapped paths among E and Ω_c
$\Omega_{e,pi}$	The index set of overlapped paths between E and $\Omega_{i,p}$
τ_c	The power allocation coefficient for s_c
τ_i	The power allocation coefficient for s_i
$R_{1,c}^{\text{th}}$	The secrecy rate threshold for the common messages
$R_{1,p}^{\text{th}}$	The secrecy rate threshold for the private messages
$G_{c,d}^{a,b}[\cdot]$	Meijer's G -function
$H_{c,d}^{a,b,e,f}[\cdot]$	Extended generalized bivariate Fox's H -function
$\Gamma(x)$	Gamma function

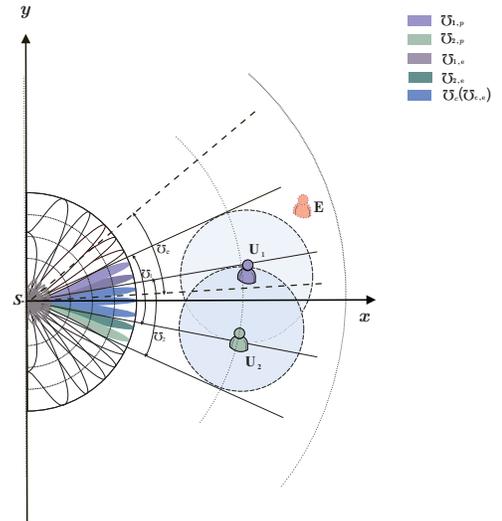


Fig. 1: A downlink mmWave RSMA system consists a base station (S), two user (U_1 and U_2), and a external passive eavesdropper (E).

eavesdropper denoted by E attempt to intercept the information. S is equipped with N_s antennas and both legitimate and illegitimate receivers are equipped with a single antenna.

Similar to [32], the message, W_i ($i = 1, 2$), is split into $W_{i,c}$

and $W_{i,p}$. $W_{1,c}$ and $W_{c,2}$ are encoded together into s_c , which is a common stream decoded by both users. At the same time, $W_{1,p}$ and $W_{p,2}$ are encoded into s_1 and s_2 , respectively. The transmitted signal from S is given by

$$\mathbf{x} = \mathbf{w}_c \sqrt{P\tau_c} s_c + \mathbf{w}_1 \sqrt{P\tau_1} s_1 + \mathbf{w}_2 \sqrt{P\tau_2} s_2, \quad (1)$$

where \mathbf{w}_c , \mathbf{w}_1 , and \mathbf{w}_2 are unit vectors that denote the beamforming direction, P signifies the transmit power, and τ_c and τ_i denote the power allocation coefficient for s_c and s_i , respectively.

The polar coordinate system is established with the position of S as the origin. The position of U_1 and U_2 are expressed as (r_1, θ_1) and (r_2, θ_2) respectively, where θ_i is the center angle of angles of departure (AODs) of U_i 's paths, i.e., $\theta_i = \frac{\theta_{i,\min} + \theta_{i,\max}}{2}$. The channels of between S and the receiver l is expressed as [23]-[25]

$$\mathbf{h}_l = \sqrt{\frac{N_s P(r_l)}{L_l}} \mathbf{g}_l \mathbf{U}^H, \quad (2)$$

where $l \in \{1, 2, e\}$, $P(r_l) = r_0 r_l^{-\alpha}$, $r_0 = 10^{-\frac{\beta_L}{10}}$, $\beta_L = 3.66 + 24.3 \log_{10}(f_c)$, $f_c = 28$ GHz [35], r_l denotes the distance between the transmitter and the receiver l , α signifies the path loss exponent, L_l denotes the number of resolvable paths of the receiver l , \mathbf{U} is the spatially orthogonal basis, $\mathbf{g}_l = [g_{l,1}, g_{l,2}, \dots, g_{l,N_s}]$. It is assumed that the AODs of the receiver l 's paths is distributed within the angular range $[\theta_{l,\min}, \theta_{l,\max}]$, where $g_{l,n} \sim CN(0, 1)$ if $\theta_{l,n} \in [\theta_{l,\min}, \theta_{l,\max}]$ otherwise $g_{l,n} = 0$ [23]. To facilitate analysis, we assumed that $\theta_1 = -\theta_2$ and $L_1 = L_2 = L_e = L$. We define sets $\Omega_l = \{I_{l,o} | I_{l,o} \in Z^+, \Psi_{I_{l,o}} \in [\sin(\theta_{l,\min}), \sin(\theta_{l,\max})], I_{l,1} < I_{l,2} < \dots < I_{l,L}\}$. So we have $\text{th}\Omega_l = \{\frac{N_{\text{ths}} \mp L_{\text{thc}}}{2} \pm 1, \frac{N_{\text{ths}} \mp L_{\text{thc}}}{2} \pm 2, \dots, \frac{N_{\text{ths}} \mp L_{\text{thc}}}{2} \pm L\}$, where $\Omega_{l,o} = \frac{N_s \mp L_c}{2} \pm o$. Define the angular range $\Delta_{l,o} = [\arcsin(\Psi_{\frac{N_s \mp L_c}{2} \pm o}), \arcsin(\Psi_{\frac{N_s \mp L_c}{2} \pm o + 1})]$ and the width $\omega_{l,o} = \arcsin(\Psi_{\frac{N_s \mp L_c}{2} \pm o + 1}) - \arcsin(\Psi_{\frac{N_s \mp L_c}{2} \pm o})$, where $\Delta_{l,o}$ ($1 \leq o < L$) describes the angular range of user l between the o th and $(o+1)$ th spatially resolvable paths, $\omega_{l,o}$ denote the width between the o th and $(o+1)$ th spatially resolvable paths.. Then we have $|\Omega_1| = |\Omega_2| = |\Omega_e| = L$.

Based on the spatial correlation of all receivers, the spatially resolvable paths are divided into overlapped and non-overlapping paths [23]. L_c and L_p are defined as the number of the overlapped and non-overlapping paths between U_1 and U_2 , respectively. Thus, we have $\Omega_c = \Omega_1 \cap \Omega_2$, $\Omega_{1,p} = \Omega_1 - \Omega_c$, $\Omega_{2,p} = \Omega_2 - \Omega_c$. $|\Omega_c| = L_c$, and $|\Omega_{1,p}| = |\Omega_{2,p}| = L_p$. Similarly, L_{ec} , L_{e1} , L_{e2} denote the number of the overlapped paths between Ω_e , and Ω_c , $\Omega_{1,p}$, $\Omega_{2,p}$, respectively. Thus, we have $\Omega_{ec} = \Omega_c \cap \Omega_e$ and $\Omega_{e,p1} = \Omega_{1,p} \cap \Omega_e$, $\Omega_{e,p2} = \Omega_{2,p} \cap \Omega_e$, $|\Omega_{e,c}| = L_{ec}$, $|\Omega_{e,p1}| = L_{e1}$, $|\Omega_{e,p2}| = L_{e2}$.

In this work, s_c is transmitted on the overlapped paths and s_i is transmitted on their non-overlapping paths to eliminate the inter-user interference of private signals by utilizing the spatial correlation of two users' channels [32]. Similar to [23] and [32], it is assumed that the perfect channel state information

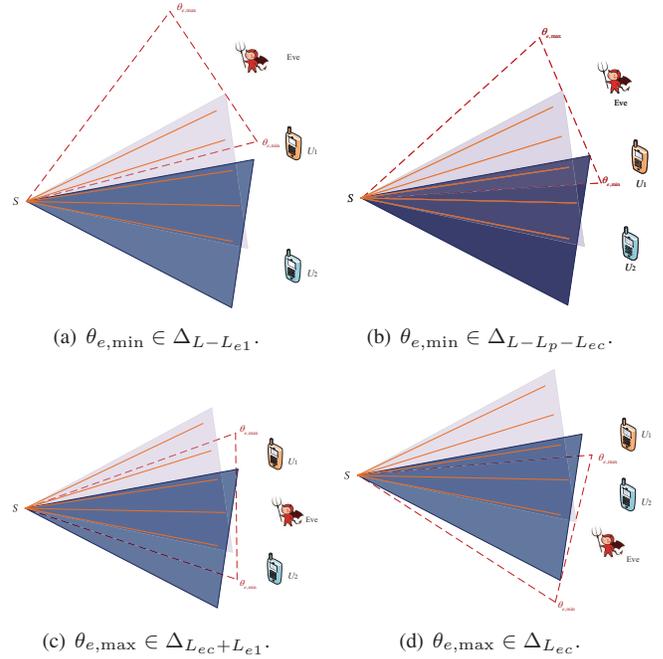


Fig. 2: Scenarios for the different number of the overlapped overlapped paths between U_i and E with $L = 5$ and $L_c = 3$.

(CSI) of the legitimate receivers is available at S , the beamforming for s_c is expressed as $\mathbf{w}_c = \mathbf{S}(\mathbf{U}, \Omega_c) \in N_s \times L_c$, where $\mathbf{S}(\mathbf{B}, D)$ is utilized to generate a new matrix with columns selected from \mathbf{B} based on the selected column index set D , and Ω_c denotes the index sets of common resolvable paths between the receiver U_1 and U_2 . Similarly, the beamforming for s_i is expressed as $\mathbf{w}_i = \mathbf{S}(\mathbf{U}, \Omega_{i,p}) \in N_s \times L_p$, where $\Omega_{i,p}$ denotes the index set of the non-overlapping paths of receiver U_i . Thus, the transmitted signal from S is rewritten as

$$\mathbf{x} = \mathbf{w}_c \sqrt{P\tau_c} s_c + \mathbf{w}_1 \sqrt{P\tau_1} s_1 + \mathbf{w}_2 \sqrt{P\tau_2} s_2, \quad (3)$$

where $\mathbf{s}_c \in \mathbb{C}^{L_c \times 1}$ and $\mathbf{s}_i \in \mathbb{C}^{L_p \times 1}$.

B. Signal to Interference Plus Noise Ratio

According to the RSMA principle, U_i decodes s_c firstly by treating all the other signals as noise. Then the instantaneous signal-to-interference and noise ratio (SINR) of decoding s_c at U_i is $\gamma_{i,c} = \frac{\delta_{i,c} \|\mathbf{g}_{i,c}\|^2}{\delta_i \|\mathbf{g}_{i,p}\|^2 + 1}$, where $\delta_{i,c} = \frac{\delta \tau_c}{r_i^\alpha}$, $\delta_i = \frac{\delta \tau_i}{r_i^\alpha}$, $\rho = \frac{P}{\sigma^2}$, and $\delta = \frac{N_s \rho \tau_0}{L}$. After performing SIC, i.e., s_c is re-encoded, precoded, and removed from the received signal, the SINR of decoding s_i at U_i is obtained as $\gamma_{i,p} = \delta_i \|\mathbf{g}_{i,p}\|^2$.

In this work, it is assumed that E is interested only in U_1 's message². Moreover, for tractability of analysis, $\Delta_{1,o}$ ($1 \leq o < L$) is represented by Δ_o , the users' locations are assumed to be fixed in this work³. Depending on the relative

²Since the analysis for both users is interchangeable, the secrecy performance of the scenarios in which E is interested in U_2 's message can be obtained based on the results of this manuscript.

³The secrecy performance of scenarios wherein the users are randomly distributed also can be easily obtained based on [32, (7)] and the results of this work.

positions of U_1 and E , as shown in Fig. 2, there are four scenarios for the SINR of E ⁴, where $\Delta_{L-L_{e1}}$ signifies the angular range of U_1 between the $(L - L_{e1})$ th and $(L - L_{e1} + 1)$ th spatially resolvable paths, similarly, $\Delta_{L-L_p-L_{ec}}$ signifies the angular range of U_1 between the $(L - L_p - L_{ec})$ th and $(L - L_p - L_{ec} + 1)$ th spatially resolvable paths.

1) Scenario I: $\theta_{e,\min} \in \Delta_{L-L_{e1}}$

As show in Fig. 2(a), only the private stream of U_1 is wiretapped by E , which denotes $\gamma_{e,c}^I = 0$. The SINR of E in eavesdropping private stream of U_1 is given as $\gamma_{e,p1}^I = \delta_{e1} \|\mathbf{g}_{e,p1}\|^2$, where $\delta_{e1} = \delta\tau_1 r_e^{-\alpha}$.

2) Scenario II: $\theta_{e,\min} \in \Delta_{L-L_p-L_{ec}}$

This scenario is shown in Fig. 2(b), where in both common and private streams of U_1 are eavesdropped by E . More Specifically, all non-overlapping resolvable paths of U_1 is wiretapped and overlapped paths of U_1 is partially wiretapped. Like [33], it is assumed that illegitimate has the same decoding capability as the legitimate users⁵. According to the RSMA principle, E decodes common streams of U_1 firstly by treating all the other signals as noise, and then decodes private streams of U_1 . Thus, the SINR of E in eavesdropping both the common stream and private stream of U_1 are given as

$$\gamma_{e,c}^{II} = \frac{\delta_{ec} \|\mathbf{g}_{e,c}\|^2}{\delta_{e1} \|\mathbf{g}_{e,p1}\|^2 + 1}, \quad (4)$$

$$\gamma_{e,p1}^{II} = \delta_{e1} \|\mathbf{g}_{e,p1}\|^2, \quad (5)$$

respectively, where $\delta_{ec} = \delta\tau_2 r_e^{-\alpha}$.

3) Scenario III: $\theta_{e,\max} \in \Delta_{L_{ec}+L_{e1}}$

As show in Fig. 2(c), all the overlapped paths and part of the non-overlapping paths for U_1 is intercepted. Similarly, the E firstly decodes common streams and then decodes private streams of U_1 . Thus, the SINR of E in eavesdropping the common stream and private stream of U_1 are given as

$$\gamma_{e,c}^{III} = \frac{\delta_{ec} \|\mathbf{g}_{e,c}\|^2}{\delta_{e1} \|\mathbf{g}_{e,p1}\|^2 + \delta_{e2} \|\mathbf{g}_{e,p2}\|^2 + 1}, \quad (6)$$

and

$$\gamma_{e,p1}^{III} = \frac{\delta_{e1} \|\mathbf{g}_{e,p1}\|^2}{\delta_{e2} \|\mathbf{g}_{e,p2}\|^2 + 1}, \quad (7)$$

respectively, where $\delta_{e2} = \delta\tau_2 r_e^{-\alpha}$.

4) Scenario IV: $\theta_{e,\max} \in \Delta_{L_{ec}}$

This case is shown in Fig. 2(d) wherein only the common stream of U_1 is eavesdropped by E , which denotes $\gamma_{e,p1}^{IV} = 0$ and

$$\gamma_{e,c}^{IV} = \frac{\delta_{ec} \|\mathbf{g}_{e,c}\|^2}{\varpi_0 \delta_{e2} \|\mathbf{g}_{e,p2}\|^2 + 1}. \quad (8)$$

⁴Except for the four scenarios considered here, there is another scenario wherein there is no overlapped path between E and U_1 and both the common and private messages are secure.

⁵There is another eavesdropping scenario, called the worst-case security scenario, considered in many works, such as [33], [34]. Specifically, by utilizing specific detection techniques, the data stream received can be distinguished by the eavesdropper by subtracting interference generated by the superposed signals from each other. This assumption has been utilized in a reasonable amount of literature focused on the physical layer security of NOMA systems. In fact, this assumption simplified the analysis but overestimated the eavesdropper's multi-user decodability.

To facilitate analysis, we define $X_{lq} = \|\mathbf{g}_{l,q}\|^2$ ($(l, q) \in \{(i, c), (i, p), (e, c1), (e, p1), (e, p2)\}$). The PDF and CDF of X_{lq} are expressed as

$$f_{X_{lq}}(x) = \frac{e^{-x} x^{\kappa_{lq}-1}}{\Gamma(\kappa_{lq})}, \quad (9)$$

and

$$F_{X_{lq}}(x) = 1 - e^{-x} \sum_{t=0}^{\kappa_{lq}-1} \frac{x^t}{t!}, \quad (10)$$

respectively, where $\kappa_{1c} = \kappa_{2c} = L_c$, $\kappa_{1p} = \kappa_{2p} = L_p$, $\kappa_{ec1} = L_{ec}$, $\kappa_{ep1} = L_{e1}$, and $\kappa_{ep2} = L_{e2}$.

III. SECRECY OUTAGE PROBABILITY ANALYSIS

In this work, U_1 is secure only when both the common and private stream are secrecy. Thus, the SOP of U_1 in the j th ($j \in \{I, II, III, IV\}$) scenario is expressed as

$$P_{\text{sop},1}^j = 1 - \Pr \left\{ \underbrace{C_{1,c}^{s,j} > R_{1,c}^{\text{th}}, C_{1,p}^{s,j} > R_{1,p}^{\text{th}}}_{\triangleq P_{\text{scp},1}^j} \right\}, \quad (11)$$

where $C_{1,c}^{s,j} = [\log_2(1 + \gamma_{1,c}) - \log_2(1 + \gamma_{e,c}^j)]^+$ denotes instantaneous secrecy capacity of common streams intended to U_1 , $C_{1,p}^{s,j} = [\log_2(1 + \gamma_{1,p}) - \log_2(1 + \gamma_{e,p1}^j)]^+$ denotes instantaneous secrecy capacity of private streams transmitted to the U_1 , $[x]^+ = \max\{x, 0\}$, and $R_{1,c}^{\text{th}}$ and $R_{1,p}^{\text{th}}$ signify the secrecy rate threshold for the common and private messages, respectively, and $P_{\text{scp},1}^j$ denotes the secrecy connection probability (SCP), which is the complementary of SOP. It should be noted that, when E can only wiretap the common streams or private streams, the SCP of U_1 is degenerated to $P_{\text{scp},1}^j = \Pr \{C_{1,c}^{s,j} > R_{1,c}^{\text{th}}\}$ or $P_{\text{scp},1}^j = \Pr \{C_{1,p}^{s,j} > R_{1,p}^{\text{th}}\}$ respectively.

1) Scenario I: $\theta_{e,\min} \in \Delta_{L-L_{e1}}$

In this case, E only eavesdrop on private streams of U_1 . Based on (9), (10) and (11), utilizing [36, (3.351.3)], $P_{\text{scp},1}^I$ is obtained as

$$\begin{aligned} P_{\text{scp},1}^I &= \Pr \left\{ \log_2 \left(\frac{1 + \gamma_{1,p}}{1 + \gamma_{e,p1}^I} \right) > R_{1,p}^{\text{th}} \right\} \\ &= \Pr \{X_{1p} > A_1 X_{ep1} + A_2\} \\ &= \mathbb{E}_{X_{ep1}} \left[e^{-(A_1 X_{ep1} + A_2)} \sum_{t=0}^{L_p-1} \frac{(A_1 X_{ep1} + A_2)^t}{t!} \right] \\ &= \sum_{t=0}^{L_p-1} \sum_{n=0}^t \frac{e^{-A_2} A_1^n A_2^{t-n}}{n! (t-n)! (L_{e1}-1)!} \\ &\times \int_0^\infty e^{-(A_1+1)x} x^{L_{e1}+n-1} dx \\ &= \sum_{t=0}^{L_p-1} \sum_{n=0}^t \frac{e^{-A_2} A_1^n A_2^{t-n} (L_{e1}+n-1)!}{n! (t-n)! (L_{e1}-1)! (A_1+1)^{L_{e1}+n}}, \end{aligned} \quad (12)$$

where $\mathbb{E}[\cdot]$ denotes the expectation operation, $\Theta_{1,p} = 2^{R_{1,p}^{\text{th}}}$, $A_1 = \frac{\Theta_{1,p} \delta_{e1}}{\delta_1} = \frac{\Theta_{1,p} r_e^\alpha}{r_e^\alpha}$, and $A_2 = \frac{\Theta_{1,p}-1}{\delta_1}$.

2) Scenario II: $\theta_{e,\min} \in \Delta_{L-L_p-L_{ec}}$

In this case, the private streams is eavesdropped completely while the common streams is partly eavesdropped. Thus, the SCP of U_1 is expressed as

$$\begin{aligned}
P_{\text{scp},1}^{\text{II}} &= \Pr \left\{ \log_2 \left(\frac{1 + \gamma_{1,c}}{1 + \gamma_{e,c}^{\text{II}}} \right) > R_{1,c}^{\text{th}}, \right. \\
&\quad \left. \log_2 \left(\frac{1 + \gamma_{1,p}}{1 + \gamma_{e,p1}^{\text{II}}} \right) > R_{1,p}^{\text{th}} \right\} \\
&= \Pr \left\{ \frac{1 + \frac{\delta_{1,c} X_{1c}}{X_1}}{1 + \frac{\delta_{ec} X_{ec}}{X_2}} > \Theta_{1,c}, \frac{X_1}{X_2} > \Theta_{1,p} \right\} \\
&= \int_1^\infty \int_{X_2 \Theta_{1,p}}^\infty \Delta_1 f_{X_1}(X_1) dX_1 f_{X_2}(X_2) dX_2,
\end{aligned} \tag{13}$$

where $\Delta_1 = \int_{X_1 \eta_1}^\infty F_{X_{ec}} \left(\left(\frac{y}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) X_2 \right) f_{X_{1c}}(y) dy$, $X_1 = 1 + \delta_1 X_{1p}$, $X_2 = 1 + \delta_{e1} X_{ep1}$, $\eta_1 = \frac{\Theta_{1,c} - 1}{\delta_{1,c}}$, $\eta_2 = \frac{\Theta_{1,c} \delta_{ec}}{\delta_{1,c}}$. Based on (9) and (10) and utilizing [36, (3.351.2)], Δ_1 is obtained as

$$\begin{aligned}
\Delta_1 &= \bar{F}_{X_{1c}}(X_1 \eta_1) \\
&\quad - \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \sum_{k=0}^{m+L_c-1} \frac{A_3 X_1^{L_c} X_2^t e^{-X_1 \eta_1}}{(X_2 + X_1 \eta_2)^{m+L_c-k}},
\end{aligned} \tag{14}$$

where $A_3 = \frac{(-1)^{t-m} (m+L_c-1)! \eta_1^{t-m+k} \eta_2^{m+L_c-k-t}}{k! m! (t-m)! \Gamma(L_c)}$ and $\bar{F}_{X_{1c}}(x) = 1 - F_{X_{1c}}(x)$. Define $X_I = 1 + \varepsilon X$, ($I = 1, 2$), the PDF of X_I is obtained as

$$f_{X_I}(x) = \frac{e^{-\frac{x-1}{\varepsilon}} (x-1)^{\kappa_X-1}}{\varepsilon^{\kappa_X} (\kappa_X - 1)!}. \tag{15}$$

Then, $P_{\text{scp},1}^{\text{II}}$ is obtained as

$$\begin{aligned}
P_{\text{scp},1}^{\text{II}} &= \sum_{t=0}^{L_c-1} \frac{\delta_1^{-L_p} \eta_1^t \delta_{e1}^{-L_{e1}} \Delta_2}{t! (L_p - 1)! (L_{e1} - 1)!} \\
&\quad - \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \sum_{k=0}^{m+L_c-1} \sum_{n=0}^{L_c} A_3 A_4 \Delta_3,
\end{aligned} \tag{16}$$

where $A_4 = \frac{(L_c)! e^{-\eta_1 \delta_1^{-L_p} \delta_{e1}^{-L_{e1}}}}{n! (L_c - n)! (L_p - 1)! (L_{e1} - 1)!}$, $\Delta_2 = \int_1^\infty \int_{y \Theta_{1,p}}^\infty e^{-x \eta_1} x^t e^{-\frac{x-1}{\delta_1}} (x-1)^{L_p-1} dx e^{-\frac{y-1}{\delta_{e1}}} (y-1)^{L_{e1}-1} dy$ and $\Delta_3 = \int_1^\infty \int_{y \Theta_{1,p-1}}^\infty \frac{e^{-(\eta_1 + \frac{1}{\delta_1})z} z^{n+L_p-1} dz y^t (y-1)^{L_{e1}-1} dy}{(z \eta_2 + y + \eta_2)^{m+L_c-k} \frac{y-1}{\delta_{e1}}}$.

Utilizing [36, (3.351.2), (3.351.3)], Δ_2 is obtained as (17), shown at the top of this page, where $A_5 = \frac{(m+L_p-1)! t! e^{\frac{1}{\delta_1} - \Theta_{1,p}} (\eta_1 + \frac{1}{\delta_1}) (-1)^{k-i} \Theta_{1,p}^i}{m! (t-m)! (\eta_1 + \frac{1}{\delta_1})^{m+L_p-k} (k-i)! j! (i-j)!}$. Similarly, based on (16) and utilizing [36, (7.811.5)] and (25.4.39), we obtain Δ_3 as (18), shown at the top of next page, where $A_6 = \frac{\pi \sqrt{b_1 - b_2^2} t! (n+L_p)! \Theta_{1,p}^j (\Theta_{1,p} - 1)^{n+L_p-j}}{I b_1^{a_3} q! (t-q)! j! (n+L_p-j)! e^{\left(\frac{\eta_1}{b_1} + \frac{1}{b_1 \delta_1}\right) (\Theta_{1,p} - 1)}}$, $b_1 = \frac{1}{2} \left(1 + \cos \frac{(2i-1)\pi}{2I} \right)$, $G_{p,q}^{m,n}[\cdot]$ is the Meijer's G -function as defined by [36, (9.301)], I is the summation items that reflect accuracy by complexity, $a_1 = n + L_p + 1 - m - L_c + k$, $a_2 = j + q + L_{e1} - m - L_c + k$, $b_2 = \eta_2 (\Theta_{1,p} - 1) + b_1 + b_1 \eta_2$ and $b_3 = \frac{b_2}{\eta_2 \Theta_{1,p} + b_1}$.

3) Scenario III: $\theta_{e,\max} \in \Delta_{L_{ec}+L_{e1}}$

In this case, the common streams is eavesdropped completely while the private streams is eavesdropped partly. Thus, $P_{\text{scp},1}^{\text{III}}$ is expressed as

$$\begin{aligned}
P_{\text{scp},1}^{\text{III}} &= \Pr \left\{ \log_2 \left(\frac{1 + \gamma_{1,c}}{1 + \gamma_{e,c}^{\text{III}}} \right) > R_{1,c}^{\text{th}}, \log_2 \left(\frac{1 + \gamma_{1,p}}{1 + \gamma_{e,p1}^{\text{III}}} \right) > R_{1,p}^{\text{th}} \right\} \\
&= \Pr \left\{ X_{ec} < \left(\frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) (X_3 + \delta_{e1} X_{ep1}), X_{ep1} < \right. \\
&\quad \left. \left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}}, X_{1c} > X_1 \eta_1, X_1 > \Theta_{1,p}, X_3 > 1 \right\} \\
&= \mathbb{E}_{X_{1c}, X_1, X_3} [\Delta_4],
\end{aligned} \tag{19}$$

where $X_3 = 1 + \delta_{e2} X_{ep2}$ and $\Delta_4 = \int_0^{\frac{Q X_3}{\delta_{e1}}} F_{X_{ec}}(P(X_3 + \delta_{e1} y)) f_{X_{ep1}}(y) dy$, $P = \frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2}$, and $Q = \frac{X_1}{\Theta_{1,p}} - 1$. Based on (9) and (10) and utilizing [36, (3.351.1)], Δ_4 is obtained as

$$\begin{aligned}
\Delta_4 &= 1 - e^{-\frac{Q X_3}{\delta_{e1}}} \sum_{t=0}^{L_{e1}-1} \frac{1}{t!} \left(\frac{Q X_3}{\delta_{e1}} \right)^t \\
&\quad - \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \frac{B_1 P^t X_3^{t-m} e^{-P X_3}}{(P \delta_{e1} + 1)^{m+L_{e1}}} \\
&\quad + \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \sum_{k=0}^{m+L_{e1}-1} \frac{B_1 P^t \left(\frac{Q X_3}{\delta_{e1}} \right)^k e^{-\frac{X_1}{\Theta_{1,p}} P X_3}}{k! X_3^{m-t} e^{\frac{Q X_3}{\delta_{e1}}} (P \delta_{e1} + 1)^{m+L_{e1}-k}},
\end{aligned} \tag{20}$$

where $B_1 = \frac{\delta_{e1}^{m(L_{e1}-1)!}}{m! (t-m)! \Gamma(L_{e1})}$. Substituting (20) into (19), $P_{\text{scp},1}^{\text{III}}$ is obtained as

$$\begin{aligned}
P_{\text{scp},1}^{\text{III}} &= \Delta_5 - \sum_{t=0}^{L_{e1}-1} \frac{1}{t!} \Delta_6 - \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \Delta_7 \\
&\quad + \sum_{t=0}^{L_{ec}-1} \sum_{m=0}^t \sum_{k=0}^{m+L_{e1}-1} \Delta_8,
\end{aligned} \tag{21}$$

where $\Delta_5 = \int_1^\infty \int_{\Theta_{1,p}}^\infty \int_{y \eta_1}^\infty f_{X_{1c}}(x) dx f_{X_1}(y) dy f_{X_3}(z) dz$, $\Delta_6 = \mathbb{E}_{X_{1c}, X_1, X_3} \left[e^{-\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}}} \left(\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}} \right)^t \right]$,

$\Delta_7 = \mathbb{E}_{X_{1c}, X_1, X_3} \left[\frac{B_1 X_3^{t-m} \left(\frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right)^t e^{-\left(\frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) X_3}}{\left(\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}} \right)^{m+L_{e1}}} \right]$,

and $\Delta_8 = \mathbb{E}_{X_{1c}, X_1, X_3} \left[\frac{B_1 \left(\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}} \right)^k \left(\frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right)^t}{\left(\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}} \right)^{m+L_{e1}-k}} \right]$, $\times \frac{e^{-\frac{X_1}{\Theta_{1,p}} \left(\frac{X_{1c}}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) X_3}}{k! X_3^{m-t} e^{\left(\frac{X_1}{\Theta_{1,p}} - 1 \right) \frac{X_3}{\delta_{e1}}}}$.

Utilizing [36, (3.351.2)], Δ_5 is obtained as

$$\begin{aligned}
\Delta_5 &= \int_1^\infty \int_{\Theta_{1,p}}^\infty \bar{F}_{X_{1c}}(y \eta_1) f_{X_1}(y) dy f_{X_3}(z) dz \\
&= \sum_{t=0}^{L_c-1} \frac{\eta_1^t}{t!} \int_{\Theta_{1,p}}^\infty \frac{e^{-y \eta_1} y^t e^{-\frac{y-1}{\delta_1}} (y-1)^{L_p-1}}{\delta_1^{L_p} (L_p - 1)!} dy \\
&= \sum_{t=0}^{L_c-1} \sum_{m=0}^t \frac{\eta_1^t e^{-\eta_1} \Gamma \left(m + L_p, \left(\eta_1 + \frac{1}{\delta_1} \right) (\Theta_{1,p} - 1) \right)}{\delta_1^{L_p} m! (t-m)! (L_p - 1)! \left(\eta_1 + \frac{1}{\delta_1} \right)^{m+L_p}}.
\end{aligned} \tag{22}$$

$$\begin{aligned}
\Delta_2 &= \sum_{m=0}^t \frac{t!e^{-\eta_1}}{m!(t-m)!} \int_1^\infty \int_{y\Theta_{1,p}-1}^\infty e^{-(\eta_1+\frac{1}{\delta_1})z} z^{m+L_p-1} dz e^{-\frac{y-1}{\delta_{e1}}(y-1)^{L_{e1}-1}} dy \\
&= \sum_{m=0}^t \sum_{k=0}^{m+L_p-1} \sum_{i=0}^k \sum_{j=0}^i A_5 \int_0^\infty e^{-(\Theta_{1,p}(\eta_1+\frac{1}{\delta_1})+\frac{1}{\delta_{e1}})z} z^{j+L_{e1}-1} dz \\
&= \sum_{m=0}^t \sum_{k=0}^{m+L_p-1} \sum_{i=0}^k \sum_{j=0}^i A_5 (j+L_{e1}-1)! \left(\Theta_{1,p} \left(\eta_1 + \frac{1}{\delta_1} \right) + \frac{1}{\delta_{e1}} \right)^{-j-L_{e1}}
\end{aligned} \tag{17}$$

$$\begin{aligned}
\Delta_3 &= \sum_{i=1}^I \frac{\pi \sqrt{b_1 - b_1^2}}{I b_1^{a_1}} \int_1^\infty \frac{e^{-(\eta_1+\frac{1}{\delta_1})\frac{y\Theta_{1,p}-1}{b_1}} (y\Theta_{1,p}-1)^{n+L_p} y^t (y-1)^{L_{e1}-1}}{(\eta_2(y\Theta_{1,p}-1) + b_1 y + b_1 \eta_2)^{m+L_c-k} e^{\frac{y-1}{\delta_{e1}}}} dy \\
&= \sum_{i=1}^I \sum_{j=0}^{n+L_p} \sum_{q=0}^t A_6 \int_0^\infty \frac{e^{-((\eta_1+\frac{1}{\delta_1})\frac{\Theta_{1,p}}{b_1} + \frac{1}{\delta_{e1}})u} u^{j+q+L_{e1}-1}}{((\eta_2\Theta_{1,p} + b_1)u + b_2)^{m+L_c-k}} dy \\
&= \sum_{i=1}^I \sum_{j=0}^{n+L_p} \sum_{q=0}^t \frac{A_6 b_3^{a_2} G_{1,2}^{2,1} \left[\left(\left(\eta_1 + \frac{1}{\delta_1} \right) \frac{\Theta_{1,p}}{b_1} + \frac{1}{\delta_{e1}} \right) b_3 \right]_{-a_2,0}^{1-j-q-L_{e1}}}{(\eta_2\Theta_{1,p} + b_1)^{m+L_c-k} \Gamma(m+L_c-k)}
\end{aligned} \tag{18}$$

Based on (10) and (15) and utilizing [36, (3.351.3), (7.811.5)], Δ_6 is obtained as

$$\begin{aligned}
\Delta_6 &= \sum_{m=0}^{L_c-1} \sum_{n=0}^m \sum_{i=0}^{L_p-1} B_2 \int_1^\infty \int_0^\infty e^{-(z+\frac{\Theta_{1,p}\delta_{e1}}{\delta_1}+\Theta_{1,p}\delta_{e1}\eta_1)u} \\
&\quad \times u^{t+n+i} du z^t \frac{e^{-\frac{z-1}{\delta_{e2}}(z-1)^{L_{e2}-1}}}{\delta_{e2}^{L_{e2}}(L_{e2}-1)!} dz \\
&= \sum_{m=0}^{L_c-1} \sum_{n=0}^m \sum_{i=0}^{L_p-1} \sum_{j=0}^t \frac{B_2 (t+n+i)! t! \Xi_1}{j! (t-j)! \delta_{e2}^{L_{e2}} (L_{e2}-1)!},
\end{aligned} \tag{23}$$

where $B_2 = \frac{(\Theta_{1,p}-1)^{L_p-1-i} \Theta_{1,p}^{m+1+i} \delta_{e1}^{i+n+1} \eta_1^m}{i!(L_p-1-i)!n!(m-n)! \delta_1^{L_p} e^{\eta_1 \Theta_{1,p} + \frac{\Theta_{1,p}-1}{\delta_1}}}$, $\Xi_1 = \frac{(1+\eta_3)^{a_4-a_3}}{\Gamma(a_3)} G_{1,2}^{2,1} \left[\frac{(1+\eta_3)}{\delta_{e2}} \right]_{a_3-a_4,0}^{1-a_4}$, $a_3 = t+n+i+1$, $a_4 = j+L_{e2}$, and $\eta_3 = \frac{\Theta_{1,p}\delta_{e1}}{\delta_1} + \Theta_{1,p}\delta_{e1}\eta_1$. Based on (9) and (15), Δ_7 is obtained as

$$\begin{aligned}
\Delta_7 &= B_1 \mathbb{E}_{X_1, X_3} \left[\frac{X_3^{t-m}}{\Gamma(L_c)} \int_{X_1 \eta_1}^\infty \frac{\left(\frac{x}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right)^t e^{-x X_1^{L_c-1}}}{\left(\left(\frac{x}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) \delta_{e1} + 1 \right)^{m+L_{e1}}} \right. \\
&\quad \left. \times e^{-\left(\frac{x}{X_1 \eta_2} - \frac{\eta_1}{\eta_2} \right) X_3} dx \right] \\
&= \sum_{n=0}^{L_c-1} B_3 \mathbb{E}_{X_1, X_3} \left[\frac{X_3^{t-m} X_1^{L_c} e^{-X_1 \eta_1}}{\Gamma(L_c)} \right. \\
&\quad \left. \times \int_0^\infty \frac{e^{-(X_3+X_1 \eta_2)u} u^{n+t}}{(u\delta_{e1}+1)^{m+L_{e1}}} du \right] \\
&= \sum_{n=0}^{L_c-1} \frac{B_3 \delta_1^{-L_p} \delta_{e2}^{-L_{e2}} \Xi_2}{\Gamma(L_c) (L_p-1)! (L_{e2}-1)!},
\end{aligned} \tag{24}$$

where $B_3 = \frac{B_1(L_c-1)! \eta_1^{L_c-1-n} \eta_2^{n+1}}{n!(L_c-1-n)!}$ and $\Xi_2 = \int_1^\infty \frac{\nabla_1 z^{t-m} (z-1)^{L_{e2}-1}}{e^{\frac{z-1}{\delta_{e2}}}} dz$,

$\nabla_1 = \int_{\Theta_{1,p}}^\infty \int_0^\infty \frac{e^{-(z+y\eta_2)u} u^{n+t}}{(u\delta_{e1}+1)^{m+L_{e1}}} du \frac{y^{L_c} (y-1)^{L_p-1}}{e^{\frac{y-1}{\delta_{e1}}}} dy$. Then, utilizing [36, (7.811.5)] and (25.4.39), ∇_1 is obtained as

$$\begin{aligned}
\nabla_1 &= \sum_{k=0}^{L_c} \frac{(L_c)! \delta_{e1}^{-a_5} e^{-\eta_1}}{k! (L_c-k)! \Gamma(m+L_{e1})} \\
&\quad \times \int_{\Theta_{1,p}-1}^\infty G_{1,2}^{2,1} \left[\frac{z + \lambda \eta_2 + \eta_2}{\delta_{e1}} \right]_{-a_5,0}^{-n-t} \frac{\lambda^{k+L_p-1}}{e^{(\eta_1+\frac{1}{\delta_1})\lambda}} d\lambda \\
&= \sum_{k=0}^{L_c} \frac{(L_c)! \delta_{e1}^{-a_5} e^{-\eta_1}}{k! (L_c-k)! \Gamma(m+L_{e1})} \\
&\quad \times \int_0^{\frac{1}{\Theta_{1,p}-1}} G_{1,2}^{2,1} \left[\frac{(z+\eta_2)u + \eta_2}{\delta_{e1}u} \right]_{-a_5,0}^{-n-t} \frac{e^{-(\eta_1+\frac{1}{\delta_1})\frac{1}{u}}}{u^{k+L_p+1}} du \\
&= \sum_{k=0}^{L_c} \sum_{i=1}^N B_4 G_{1,2}^{2,1} \left[\frac{b_4 z + (b_4+1)\eta_2}{\delta_{e1} b_4} \right]_{-a_5,0}^{-n-t},
\end{aligned} \tag{25}$$

where $a_5 = \frac{n+t+1}{\delta_{e1}} - m - L_{e1}$, $B_4 = \frac{\pi(Nk!(L_c-k)! \Gamma(m+L_{e1}) e^{(\eta_1+\frac{1}{\delta_1})\frac{1}{b_4}} (b_4)^{k+L_p+\frac{1}{2}})}{\pi(L_c)! \delta_{e1}^{-a_5} e^{-\eta_1} \sqrt{\frac{1}{\Theta_{1,p}-1} - b_4}}$, $b_4 = \frac{1+\cos(\frac{(2i-1)\pi}{2N})}{2(\Theta_{1,p}-1)}$ and N is the summation items that reflect accuracy versus complexity. Based on (25) and utilizing (25.4.45), Ξ_2 is obtained as (26), shown at the top of next page, where V is the summation items that reflect accuracy versus complexity, t_u is the u th zero of Laguerre polynomials and w_u is Gaussian weight, which are given in Table (25.9) of [37]. With the same method, Δ_8 is obtained as

$$\Delta_8 = \sum_{n=0}^{L_c-1} \frac{B_3 \delta_1^{-L_p} \delta_{e2}^{-L_{e2}} \Xi_3}{k! \Gamma(L_c) (L_p-1)! (L_{e2}-1)!}, \tag{27}$$

where $\Xi_3 = \int_1^\infty \frac{\nabla_2 (z-1)^{L_{e2}-1}}{z^{m-t} e^{\frac{z-1}{\delta_{e2}}}} dz$, $\nabla_2 = \int_{\Theta_{1,p}}^\infty \int_0^\infty \frac{e^{-(\frac{y}{\Theta_{1,p}}z+y\eta_2)u} u^{n+t}}{(u\delta_{e1}+1)^{m+L_{e1}-k}} du \frac{e^{-\left(\frac{y}{\Theta_{1,p}}-1\right)\frac{z}{\delta_{e1}}}}{\left(\frac{y}{\Theta_{1,p}}-1\right)\frac{z}{\delta_{e1}}} y^{L_c} (y-1)^{L_p-1} dy$.

$$\begin{aligned}
\Xi_2 &= \sum_{k=0}^{L_c} \sum_{i=1}^N \sum_{j=0}^{t-m} \frac{(t-m)! B_4}{j! (t-m-j)!} \int_0^\infty G_{1,2}^{2,1} \left[\frac{b_4 f + b_4 + (b_4 + 1) \eta_2}{\delta_{e1} b_4} \middle| \begin{matrix} -n-t \\ -a_5, 0 \end{matrix} \right] e^{-\frac{f}{\delta_{e2}}} f^{j+L_{e2}-1} df \\
&= \sum_{k=0}^{L_c} \sum_{i=1}^N \sum_{j=0}^{t-m} \frac{(t-m)! B_4 \delta_{e2}^{j+L_{e2}}}{j! (t-m-j)!} \sum_{u=1}^V w_u G_{1,2}^{2,1} \left[\frac{b_4 \delta_{e2} t_u + b_4 + (b_4 + 1) \eta_2}{\delta_{e1} b_4} \middle| \begin{matrix} -n-t \\ -a_5, 0 \end{matrix} \right] t_u^{j+L_{e2}-1} \\
&= \sum_{k=0}^{L_c} \sum_{i=1}^N \sum_{j=0}^{t-m} \sum_{u=1}^V \frac{(t-m)! B_4 \delta_{e2}^{j+L_{e2}} w_u}{j! (t-m-j)!} t_u^{j+L_{e2}-1} G_{1,2}^{2,1} \left[\frac{b_4 \delta_{e2} t_u + b_4 + (b_4 + 1) \eta_2}{\delta_{e1} b_4} \middle| \begin{matrix} -n-t \\ -a_5, 0 \end{matrix} \right]
\end{aligned} \tag{26}$$

$$\begin{aligned}
\nabla_2 &= \sum_{i=0}^{L_c} \sum_{j=0}^{L_p-1} B_5 z^k \int_0^\infty G_{1,2}^{2,1} \left[(z + \Theta_{1,p} \eta_2) \frac{(\lambda + 1)}{\delta_{e1}} \middle| \begin{matrix} -n-t \\ a_6, 0 \end{matrix} \right] \frac{\lambda^{i+j+k}}{e^{\left(\frac{z}{\delta_{e1}} + \Theta_{1,p} \eta_1 + \frac{\Theta_{1,p}}{\delta_1} \right) \lambda}} d\lambda \\
&= \sum_{i=0}^{L_c} \sum_{j=0}^{L_p-1} \sum_{v=1}^K \frac{q_v B_5 \delta_{e1}^{i+j+k+1} z^k}{(z + b_5)^{i+j+k+1}} u_v^{i+j+k} G_{1,2}^{2,1} \left[(z + \Theta_{1,p} \eta_2) \left(\frac{u_v}{z + b_5} + \frac{1}{\delta_{e1}} \right) \middle| \begin{matrix} -n-t \\ a_6, 0 \end{matrix} \right]
\end{aligned} \tag{28}$$

By utilizing [36, (7.811.5)] and (25.4.45), ∇_2 is obtained as as (28), shown at the top of next page, where $B_5 = \frac{(L_c)! (L_p-1)! \Theta_{1,p}^{L_c+j+1} (\Theta_{1,p-1})^{L_p-1-j} e^{-\left(\Theta_{1,p} \eta_1 + \frac{\Theta_{1,p}}{\delta_1} \right)}}{i! (L_c-i)! j! (L_p-1-j)! \delta_{e1}^{k+n+t+1} \Gamma(m+L_{e1}-k)}$, $a_6 = m + L_{e1} - k - n - t - 1$, $b_5 = \delta_{e1} \Theta_{1,p} \eta_1 + \delta_{e1} \frac{\Theta_{1,p}}{\delta_1}$, K is the summation items that reflect accuracy versus complexity, u_v is the v th zero of Leguerre polynomials and q_v is Gaussian weight, which are given in Table (25.9) of [37]. Based on (28) and utilizing (25.4.45), Ξ_3 is obtained as

$$\begin{aligned}
\Xi_3 &= \sum_{i=0}^{L_c} \sum_{j=0}^{L_p-1} \sum_{v=1}^K \sum_{q=0}^{k+t-m} \sum_{u=1}^D B_6 \varepsilon_u \\
&\times \frac{G_{1,2}^{2,1} \left[\left(\frac{s_u \delta_{e2}}{\delta_{e1}} + \frac{u_v (\Theta_{1,p} \eta_2 - b_5)}{\delta_{e2} s_u + 1 + b_5} + b_6 \right) \middle| \begin{matrix} -n-t \\ a_6, 0 \end{matrix} \right]}{(\delta_{e2} s_u + 1 + b_5)^{i+j+k+1} \delta_{e2}^{-q-L_{e2}} s_u^{1-q-L_{e2}}},
\end{aligned} \tag{29}$$

where $B_6 = \frac{(k+t-m)! q_v B_5 \delta_{e1}^{i+j+k+1} u_v^{i+j+k}}{q! (k+t-m-q)}$, $b_6 = u_v + \frac{1 + \Theta_{1,p} \eta_2}{\delta_{e1}}$, D is the summation items that reflect accuracy versus complexity, s_u is the u th zero of Leguerre polynomials and ε_u is Gaussian weight, which are given in Table (25.9) of [37].

4) Scenario IV: $\theta_{e,\max} \in \Delta_{L_{ec}}$

In this case, E only eavesdrop on common streams. It should noted that $\gamma_{1,c}$ and $\gamma_{e,c}^{IV}$ are independent of each other in this case. Based on (9) and (10) and utilizing [36, (3.351.3)], the CDF of $\gamma_{1,c}$ and PDF of $\gamma_{e,c}^{IV}$ are obtained as

$$F_{\gamma_{1,c}}(x) = 1 - \sum_{t=0}^{L_c-1} \sum_{m=0}^t \varpi_{1,c} x^t e^{-\frac{x}{\delta_{1,c}}} \left(\frac{\delta_1}{\delta_{1,c}} x + 1 \right)^{-m-L_p}, \tag{30}$$

$$\begin{aligned}
f_{\gamma_{e,c}}(y) &= \frac{1}{\delta_{ec}} \sum_{s=0}^{L_{ec}-1} \sum_{n=0}^s (s+1-n) \varpi_{e,c} y^s e^{-\frac{y}{\delta_{ec}}} \left(\frac{\delta_{e2}}{\delta_{ec}} y + 1 \right)^{-n-L_{e2}} \\
&+ \frac{\delta_{e2}}{\delta_{ec}} \sum_{s=0}^{L_{ec}-1} \sum_{n=0}^s (s+1-n) (n+L_{e2}) \varpi_{e,c} y^s e^{-\frac{y}{\delta_{ec}}} \left(\frac{\delta_{e2}}{\delta_{ec}} y + 1 \right)^{-n-L_{e2}-1} \\
&- \sum_{s=0}^{L_{ec}-2} \sum_{n=0}^{s+1} \frac{1}{\delta_{ec}} \varpi_{e,c} (s+1) y^s e^{-\frac{y}{\delta_{ec}}} \left(\frac{\delta_{e2}}{\delta_{ec}} y + 1 \right)^{-n-L_{e2}},
\end{aligned} \tag{31}$$

respectively, where $\varpi_{1,c} = \frac{\delta_1^m (m+L_p-1)!}{m! \delta_{1,c}^m (L_p-1)! (t-m)!}$ and $\varpi_{e,c} = \frac{\delta_{e2}^n (n+L_{e2}-1)!}{n! \delta_{ec}^n (L_{e2}-1)! (s+1-n)!}$.

To facilitate the following analysis, we define

$$\phi(c_1, c_2, c_3, c_4, c_5, c_6) = \int_0^\infty \frac{e^{-c_1 y} y^{c_2}}{(c_3 y + 1)^{c_4} (c_5 y + 1)^{c_6}} dy. \tag{32}$$

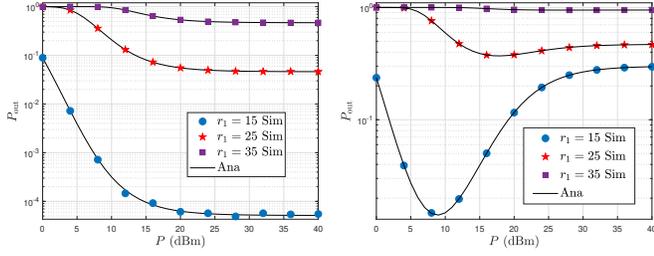
By utilizing [38, (10), (11)], [36, (9.31.5)], and [39, (1.2)] in turn, we obtain

$$\begin{aligned}
\phi(c_1, c_2, c_3, c_4, c_5, c_6) &= \frac{(c_1)^{-c_2}}{\Gamma(c_4) \Gamma(c_6)} \\
&\times \int_0^\infty G_{0,1}^{1,0} [c_1 y | c_2] G_{1,1}^{1,1} [c_3 y | c_4] G_{1,1}^{1,1} [c_5 y | c_6] dy \\
&= \frac{(c_1)^{-c_2}}{\Gamma(c_4) \Gamma(c_6) c_1} \\
&\times H_{1,0:1,1:1,1}^{1,0:1,1:1,1} \left(\begin{matrix} c_2+1 \\ - \end{matrix} \middle| \begin{matrix} 1-c_4 \\ 0 \end{matrix} \middle| \begin{matrix} 1-c_6 \\ 0 \end{matrix} \middle| \frac{c_3}{c_1}, \frac{c_5}{c_1} \right),
\end{aligned} \tag{33}$$

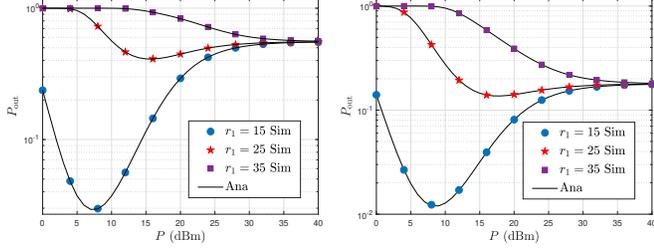
where $H_{c,d;p,r;\alpha,\beta}^{b,0:m,n;\gamma,\varepsilon}[\cdot]$ is the extended generalized bivariate Fox's H-function as defined by [39, (2.57)].

The SCP of U_1 in this scenario, $P_{\text{scp},1}^{IV}$ is obtained as

$$\begin{aligned}
P_{\text{scp},1}^{IV} &= \Pr \left\{ \frac{1 + \gamma_{1,c}}{1 + \gamma_{e,c}^{IV}} > \Theta_{1,c} \right\} \\
&= \int_0^\infty \bar{F}_{\gamma_{1,c}}(\Theta_{1,c} y + \Theta_{1,c} - 1) f_{\gamma_{e,c}^{IV}}(y) dy \\
&= \sum_{t=0}^{L_c-1} \sum_{m=0}^t \varpi_{1,c} \sum_{s=0}^{L_{ec}-1} \sum_{n=0}^s \varpi_{e,c} \\
&\times (s+1-n) \left(\frac{\Delta_9}{\delta_{ec}} + \frac{\delta_{e2}}{\delta_{ec}} (n+L_{e2}) \Delta_{10} \right) \\
&- \sum_{t=0}^{L_c-1} \sum_{m=0}^t \varpi_{1,c} \sum_{s=0}^{L_{ec}-2} \sum_{n=0}^{s+1} \frac{\varpi_{e,c}}{\delta_{ec}} (s+1) \Delta_9,
\end{aligned} \tag{34}$$



(a) $P^I_{\text{sop},1}$ for varying r_1 with $L_{e1} = 2$. (b) $P^{II}_{\text{sop},1}$ for varying r_1 with $L_{ec} = 2$ and $L_{e1} = L_n$.



(c) $P^{III}_{\text{sop},1}$ for varying r_1 with $L_{e1} = 1$, $L_{ec} = L_c$ and $L_{e2} = L - L_{ec} - 2$ and $L_{e2} = L - L_{ec}$. L_{e1} . (d) $P^{IV}_{\text{sop},1}$ for varying r_1 with $L_{ec} = L_c$.

Fig. 3: SOP versus the P with $\tau_c = \tau_1 = \tau_2 = \frac{1}{3}$, $r_e = 30$, $L = 8$, $L_c = 4$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.

where

$$\begin{aligned} \Delta_9 &= e^{-\frac{\Theta_{1,c}-1}{\delta_{1,c}}} \sum_{o=0}^t \frac{\Theta_{1,c}^o t!}{o! (t-o)!} (\Theta_{1,c} - 1)^{t-o} \\ &\times \left(\frac{\delta_1}{\delta_{1,c}} (\Theta_{1,c} - 1) + 1 \right)^{-m-L_p} \phi \left(\frac{\Theta_{1,c}}{\delta_{1,c}} + \frac{1}{\delta_{ec}}, s + o, \right. \\ &\left. \frac{\delta_1 \Theta_{1,c}}{\delta_1 (\Theta_{1,c} - 1) + \delta_{1,c}}, m + L_p, \frac{\delta_{e2}}{\delta_{ec}}, n + L_{e2} \right), \end{aligned} \quad (35)$$

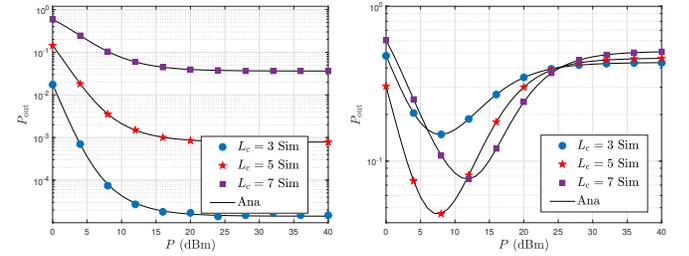
and

$$\begin{aligned} \Delta_{10} &= e^{-\frac{\Theta_{1,c}-1}{\delta_{1,c}}} \sum_{o=0}^t \frac{\Theta_{1,c}^o t!}{o! (t-o)!} (\Theta_{1,c} - 1)^{t-o} \\ &\times \left(\frac{\delta_1}{\delta_{1,c}} (\Theta_{1,c} - 1) + 1 \right)^{-m-L_p} \phi \left(\frac{\Theta_{1,c}}{\delta_{1,c}} + \frac{1}{\delta_{ec}}, s + o, \right. \\ &\left. \frac{\delta_1 \Theta_{1,c}}{\delta_1 (\Theta_{1,c} - 1) + \delta_{1,c}}, m + L_p, \frac{\delta_{e2}}{\delta_{ec}}, n + L_{e2} + 1 \right). \end{aligned} \quad (36)$$

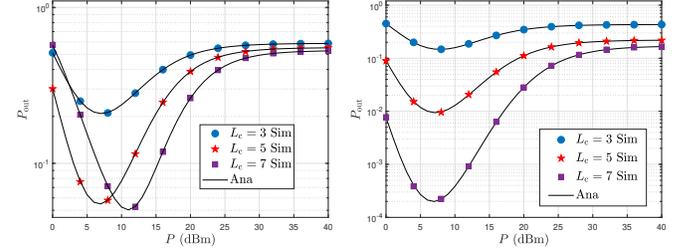
The analytical expressions provided in this section are complicated since many factors affect the secrecy performance of U_1 , specifically, the transmit power, power allocation coefficient, the target data rate, and relative locations between all the legitimate users and illegitimate receivers.

IV. NUMERICAL RESULTS

This section presents simulation and numerical results to verify the secrecy outage performance of mmWave RSMA systems with the considered beamforming scheme. The noise power is set at $\sigma^2 = -71$ dBm, and the path-loss model is set as $\alpha = 4.14$ [21], [25], [35]. In all the figures, ‘Sim’ and ‘Ana’ denote the simulation and numerical results, respectively.



(a) $P^I_{\text{sop},1}$ for varying L_c with $L_{e1} = 2$. (b) $P^{II}_{\text{sop},1}$ for varying L_c with $L_{ec} = 2$, $L_{e1} = L_n$.

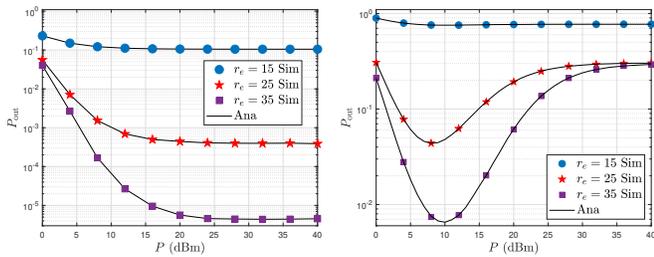


(c) $P^{III}_{\text{sop},1}$ for varying L_c with $L_{e1} = 1$, $L_{ec} = L_c$, $L_{e2} = L - L_{ec} - 2$, $L_{e2} = L - L_{ec}$. $L_{ec} - L_{e1}$. (d) $P^{IV}_{\text{sop},1}$ for varying L_c with $L_{ec} = L_c$.

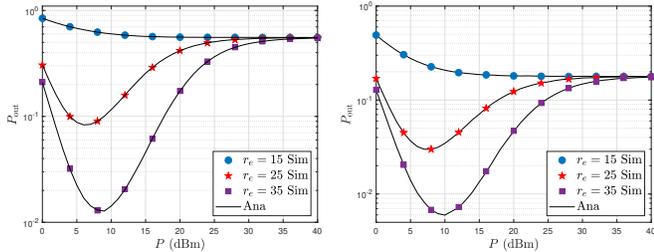
Fig. 4: SOP versus the P with $N_s = 50$, $\tau_c = \tau_1 = \tau_2 = \frac{1}{3}$, $r_1 = 15$, $r_e = 25$, $L = 9$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.

Fig. 3 demonstrates the impact of P for varying r_1 on SOP. In Fig. 3(a), one can easily observe that the secrecy outage performance of the mmWave RSMA systems is enhanced while increasing P . There is a floor for the SOP, which is independent of P , which has been testified in [40] and stated in *Remark 1*. Furthermore, the SOP with lower r_1 outperforms that with larger r_1 since lower r_1 denotes weak path loss on U_1 . One interesting result is found from Figs. 3(b) - 3(d) that the secrecy outage performance of U_1 initially decreases as P increases and then increases to a constant. The reason is given as follows. In Fig. 3(b), part of the common stream and all the private streams are wiretapped, and decoding the common stream is the bottleneck in the scenarios with lower r_1 and decoding the private stream is the bottleneck in the scenarios with larger r_1 . However, in Fig. 3(c), all of the common stream and the private stream are wiretapped, and decoding the private stream is the bottleneck in all the scenarios. In Fig. 3(d), only part of the common stream is wiretapped. Moreover, it can be found that the SOP floor is independent of r_1 in the scenarios where the bottleneck is decoding the common stream. Based on all the subfigures in Fig. 3, we also find that the effect from the location of E on the difference between the SOP of U_1 with different r_1 is weakening.

Fig. 4 presents the impact of P for varying L_c on the SOP of U_1 . In Fig. 4(a), one can observe the SOP increases as L_c increases, which is easy to follow since more significant L_c leads to less L_p , thus, $\gamma_{1,p}$ become smaller and transmissions become more vulnerable to intercept. In Figs. 4(b) and 4(c), one can observe that SOP initially decreases and then increases in the lower- P region as L_c increases, indicating an optimal L_c in the lower- P region to minimize the SOP of U_1 . This is because, in the scenarios with the lower L_c , the SOP



(a) $P_{\text{sop},1}^I$ for varying P with $L_{e1} = 2$. (b) $P_{\text{sop},1}^{II}$ for varying P with $L_{ec} = 2$, $L_{e1} = L_p$.



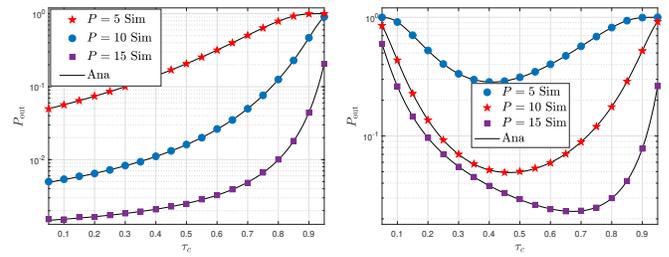
(c) $P_{\text{sop},1}^{III}$ for varying P with $L_{e1} = 1$, $L_{ec} = L_c$, $L_{e2} = L - L_{ec} - L_{e1}$. (d) $P_{\text{sop},1}^{IV}$ for varying P with $L_{ec} = 2$, $L_{e2} = L - L_{ec}$.

Fig. 5: SOP versus the τ_1 and τ_2 ($\tau_c = 1 - \tau_1 - \tau_2$) with $N_s = 50$, $r_1 = 15$, $L = 8$, $L_c = 4$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.

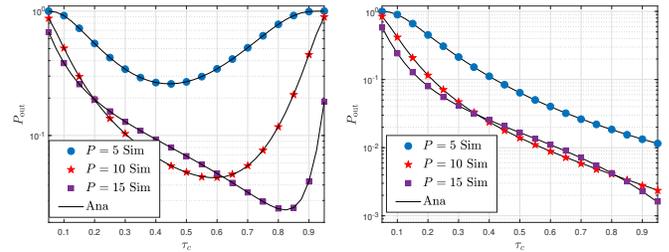
of U_1 depends on both the SINR/SNR of the common and private signals and decoding the common stream is the RSMA system's bottleneck; thus, the larger the L_c , the larger the $\gamma_{1,c}$, and the smaller SOP. In the scenarios with the larger L_c , decoding the private signals is the RSMA system's bottleneck, and the more significant L_c leads to the smaller $\gamma_{1,p}$ and the larger SOP. In Fig. 4(d), it can be observed that the secrecy performance of U_1 is improved as L_c increases since larger L_c leads to $\gamma_{1,c}$.

Fig. 5 demonstrates the impact of P with varying r_e on the SOP of U_1 . We observe that SOP decreases as r_e increases; this is because the path loss of U_1 is the main factor affecting SOP. In the larger- r_e region, SOP initially decreases and then increases as P increases Figs. 5(b) - 5(d) with the same reason as in Figs. 3(a) - 3(d). In the low- r_e region, we observe that SOP decreases as P increases in all the cases, which denotes that more power can improve security performance.

Fig. 6 plots the impact of τ_c with varying P on the SOP of U_1 . We observe that SOP increases as τ_c in Fig. 6(a), which is easy to follow since less power is allocated to private streams as increasing τ_c . In Figs. 6(b) and 6(c), one can observe SOP initially decreases and then increases as τ_c increases, which denotes that there is an optimal τ_c to minimize the SOP. This is because in the lower- τ_c region, decoding the common streams is the bottleneck. Thus, increasing τ_c will enhance the secrecy outage performance. In the larger- τ_c region, decoding the private streams will be the bottleneck. However, the power allocated to the private stream decreases, so the SOP deteriorates. Moreover, the optimal τ_c is relative to P and L_c . Based on Fig. 6(d), the secrecy performance of U_1 improves with the increasing τ_c since the SINR of common streams at U_1 increases as τ_c .

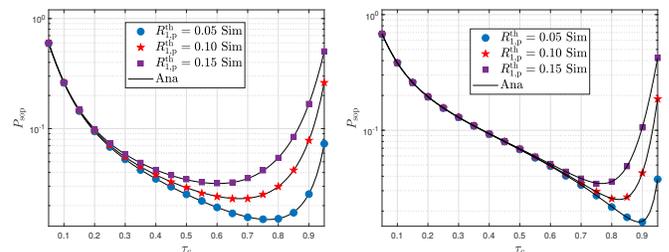


(a) $P_{\text{sop},1}^I$ for varying P with $L_{e1} = 2$. (b) $P_{\text{sop},1}^{II}$ for varying P with $L_{ec} = 2$, $L_{e1} = L_n$.

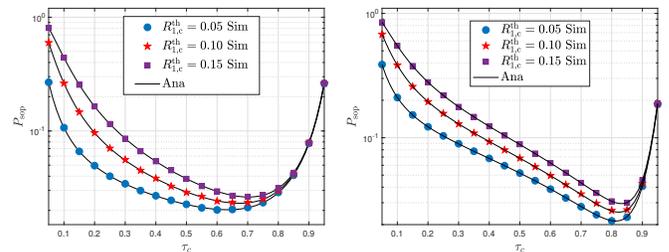


(c) $P_{\text{sop},1}^{III}$ for varying P with $L_{e1} = 1$, $L_{ec} = L_c$, $L_{e2} = L - L_{ec} - L_{e1}$. (d) $P_{\text{sop},1}^{IV}$ for varying P with $L_{ec} = 2$, $L_{e2} = L - L_{ec}$.

Fig. 6: SOP versus the τ_c with $N_s = 50$, $\tau_1 = \tau_2$, $r_1 = 15$, $r_e = 25$, $L = 8$, $L_c = 4$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.



(a) $P_{\text{sop},1}^{II}$ for varying $R_{1,p}^{\text{th}}$ with $L_{ec} = 2$, $L_{e1} = L_p$. (b) $P_{\text{sop},1}^{III}$ for varying $R_{1,p}^{\text{th}}$ with $L_{e1} = 1$, $L_{ec} = L_c$, $L_{e2} = L - L_{ec} - L_{e1}$.



(c) $P_{\text{sop},1}^{II}$ for varying $R_{1,c}^{\text{th}}$ with $L_{ec} = 1$, $L_{e1} = L_p$. (d) $P_{\text{sop},1}^{III}$ for varying $R_{1,c}^{\text{th}}$ with $L_{e1} = 1$, $L_{ec} = L_c$, $L_{e2} = L - L_{ec} - L_{e1}$.

Fig. 7: SOP versus the τ_c with $N_s = 50$, $\tau_1 = \tau_2$, $r_1 = 15$, $r_e = 25$, $L = 8$, $L_c = 4$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.

Fig. 7 presents the impact of τ_c with varying $R_{1,p}^{\text{th}}/R_{1,c}^{\text{th}}$ on the SOP of U_1 . We observe that SOP decreases as $R_{1,p}^{\text{th}}/R_{1,c}^{\text{th}}$ decreases, which is easy to follow since a more significant targeted secrecy rate denotes higher security requirements. Moreover, the optimal τ_c depends on $R_{1,p}^{\text{th}}/R_{1,c}^{\text{th}}$. The smaller $R_{1,p}^{\text{th}}/R_{1,c}^{\text{th}}$, the larger optimal τ_c , which is due to the low requirements and more power can be allocated to the stream to be the system's bottleneck. In Figs. 7(a) and 7(b), in the large-

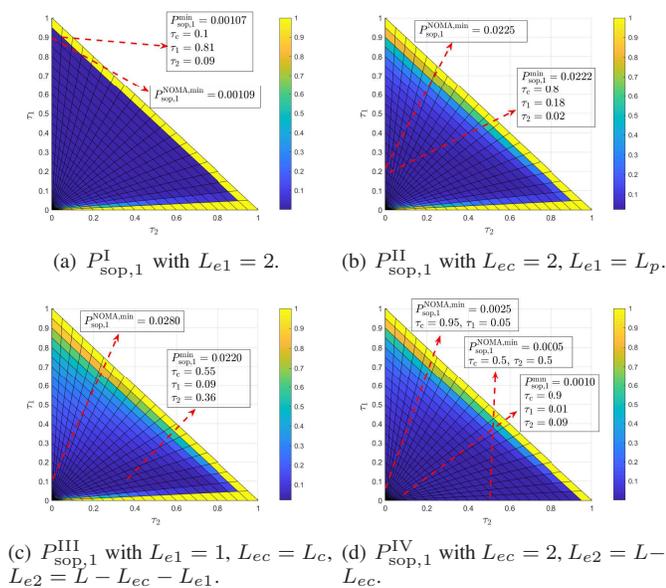


Fig. 8: SOP versus the τ_1 and τ_2 with $N_s = 50$, $P = 10\text{thdB}$, $r_1 = 15$, $r_e = 25$, $L = 8$, $L_c = 4$, and $R_{1,c}^{\text{th}} = R_{1,p}^{\text{th}} = 0.1$.

τ_c region private signals is the bottleneck, so $R_{1,p}^{\text{th}}$ has a more pronounced impact on the SOP. However, in Figs. 7(c) and 7(d), in the lower- τ_c region common signals is the bottleneck, so $R_{1,c}^{\text{th}}$ has a more pronounced impact on SOP.

To evaluate the performance of the RSMA-based mmWave systems, NOMA-based mmWave systems is utilized as the benchmark in this work, which can be found in Fig. 8, wherein the SOP of U_1 for varying τ_c , τ_1 , and τ_2 is presented. Like [28], $P_{sop,1}^{\text{min}}$ and $P_{sop,1}^{\text{NOMA,min}}$ represent the least achievable SOP of RSMA and NOMA systems, respectively. We observe that $P_{sop,1}^{\text{min}}$ successively increases and then decreases from Figs. 8(a) - Fig. 8(d). The underlying reason is that the overlapped resolvable paths between U_1 and E become larger initially, and then eavesdroppers can wiretap more confidential messages. Then, the overlapped resolvable paths between U_1 and E become smaller and also interfered with by messages of U_2 ; thus, the secrecy performance of the mmWave RSMA system is improved. Fig. 8(a) indicated that in the case of significant differences of L_c and L_{e1} , more power should be allocated to s_1 to improve secrecy performance. In Figs. 8(b) - 8(d), one can observe that the secrecy performance of common streams is easier to become a bottleneck; thus, larger τ_c and more minor τ_1 can achieve better secrecy performance. In Figs. 8(c) and 8(d), a more significant fraction of power should be allocated to s_2 relative to s_1 to confuse the eavesdropper. If τ_c or τ_1 in Figs. 8(a) - 8(c) is close to zero, the SOP would be close to 1 since with a low value of the users' SINRs are not sufficient for decoding the common stream or private stream; When τ_2 equals zero, the RSMA system will degenerate as a NOMA system. We observe that the $P_{sop,1}^{\text{min}}$ is less than or equal to $P_{sop,1}^{\text{NOMA,min}}$, the underlying reason in Figs. 8(b) - 8(c) is that common streams are easier to become a bottleneck. More power is allocated to s_1 in NOMA systems than RSMA systems, and the secrecy performance of common streams

worsens as τ_1 increases. In Fig. 8(d), when τ_1 or τ_2 is equal to zero, the RSMA system would degenerate as a NOMA system, one can observe that $P_{sop,1}^{\text{min}}$ at $\tau_2 = 0$ is less than $P_{sop,1}^{\text{NOMA,min}}$. In comparison, $P_{sop,1}^{\text{min}}$ at $\tau_1 = 0$ is larger than $P_{sop,1}^{\text{NOMA,min}}$, the reason is that as $\tau_1 = 0$ and $\tau_2 \neq 0$ directly makes $\gamma_{1,c}$ increase and $\gamma_{e,c}^{\text{IV}}$ decrease.

Based on the results, some new insights are obtained as follows.

- 1) In RSMA mmWave systems, both common and private streams can be the bottleneck of the security.
- 2) There is an optimal transmit power to minimize the SOP of RSMA-based mmWave systems and the optimal transmit power depends on the overlapped paths and distances in the considered systems.
- 3) There is an power allocation coefficient to minimize the SOP of RSMA-based mmWave systems and the optimal power allocation coefficient depends on many parameters, such as, the transmit power, target secrecy rates of common streams and private streams, relative location of all the receivers.
- 4) Relative to Scenario I and Scenario II, allocating more power to s_2 than s_1 in Scenario III and Scenario IV can enhance U_1 's security.

V. CONCLUSION

In this paper, the secure transmissions considering multi-path propagation for mmWave RSMA MISO systems were analyzed. Based on the spatial correlation of the users and the eavesdropper, different eavesdropping scenarios were considered to investigate the secrecy performance, and then the analytical expressions of the SOP for four scenarios were derived. Our results illustrated the effects of overlapped paths between receivers, the power allocation coefficient of RSMA users, and channel parameters on the SOP of RSMA-based mmWave systems. This work considered that the illegitimate user has the same decode order according to the framework of the RSMA system. Other potential threats or more diverse eavesdropping strategies will be interesting work and part of the future work. Moreover, the results of this work demonstrate an optimal power allocation coefficient to minimize the SOP of RSMA systems. Thus, allocating power reasonably to the common and private streams is vital for the secure transmissions of RSMA mmWave systems. It is challenging to obtain the analytical expression for the optimal power allocation coefficient to maximize the secrecy performance of RSMA systems. Optimizing the secrecy performance of RSMA mmWave systems will be conducted in our future work.

REFERENCES

- [1] A. Ghosh, T. A. Thomas, M. C. Cudak, R. Ratasuk, P. Moorut, F. W. Vook, T. S. Rappaport, G. R. MacCartney, S. Sun, and S. Nie, "Millimeter-wave enhanced local area systems: A high-data-rate approach for future wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1152-1163, Jun. 2014.
- [2] M. Xiao, S. Mumtaz, Y. Huang, L. Dai, Y. Li, M. Matthaiou, G. K. Karagiannidis, E. Björnson, K. Yang, I. C. -L, and A. Ghosh, "Millimeter wave communications for future mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 1909-1935, Sep. 2017.

- [3] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1616-1653, 2018.
- [4] S. He, Y. Zhang, J. Wang, J. Zhang, J. Ren, Y. Zhang, W. Zhuang, and X. Shen, "A survey of millimeter-wave communication: Physical-layer technology specifications and enabling transmission technologies," *Proc. IEEE*, vol. 109, no. 10, pp. 1666-1705, Oct. 2021.
- [5] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, R. W. Heath, and Jr., "Modeling and analyzing millimeter wave cellular systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 403-430, Jan 2017.
- [6] A. Alkhateeb, O. E. Ayach, Geert Leus, R. W. Heath, and Jr., "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831-846, Oct. 2014.
- [7] Z. Luo, L. Zhao, L. Tonghui, H. Liu, and R. Zhang, "Robust hybrid precoding/combining designs for full-duplex millimeter wave relay systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9577-9582, Sep. 2021.
- [8] Y. Zhou and S. Sun, "Performance analysis of opportunistic beam splitting NOMA in millimeter wave networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 3030-3043, Mar 2022.
- [9] B. Clerckx, Y. Mao, E. A. Jorswieck, J. Yuan, D. J. Love, E. Erkip, and D. Niyato, "A primer on rate-splitting multiple access: Tutorial, myths, and frequently asked questions," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 5, pp. 1265-1308, May 2023.
- [10] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-splitting multiple access for downlink communication systems: Bridging, generalizing, and outperforming SDMA and NOMA," *EURASIP J Wirel Commun Netw.*, vol. 2018, no. 1, pp. 1-54, Apr. 2018.
- [11] Y. Mao, O. Dizdar, B. Clerckx, R. Schober, P. Popovski, and H. V. Poor, "Rate-splitting multiple access: Fundamentals, survey, and future research trends," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2073-2126, 4th Quart. 2022.
- [12] B. Clerckx, Y. Mao, R. Schober, and H. V. Poor, "Rate-splitting unifying SDMA, OMA, NOMA, and multicasting in MISO broadcast channel: A simple two-user rate analysis," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 349-353, Mar. 2020.
- [13] B. Clerckx, H. Jouddeh, C. Hao, M. Dai, and B. Rassouli, "Rate splitting for MIMO wireless networks: A promising PHY-layer strategy for LTE evolution," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 98-105, May 2016.
- [14] B. Clerckx, Y. Mao, R. Schober, E. A. Jorswieck, D. J. Love, J. Yuan, L. Hanzo, G. Y. Li, E. G. Larsson, and G. Caire, "Is NOMA efficient in multi-antenna networks? A critical look at next generation multiple access techniques," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1310-1343, Jun. 2021.
- [15] J. Zhang, B. Clerckx, J. Ge, and Y. Mao, "Cooperative rate splitting for MISO broadcast channel with user relaying, and performance benefits over cooperative NOMA," *IEEE Signal Process. Lett.*, vol. 26, no. 11, pp. 1678-1682, Nov. 2019.
- [16] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-splitting for multi-antenna non-orthogonal unicast and multicast transmission: Spectral and energy efficiency analysis," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8754-8770, Dec. 2019.
- [17] S. K. Singh, K. Agrawal, K. Singh, and C.-P. Li, "Outage probability and throughput analysis of UAV-assisted rate-splitting multiple access," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2528-2532, Nov. 2021.
- [18] Q. Zhu, Z. Qian, B. Clerckx, and X. Wang, "Rate-splitting multiple access in multi-cell dense networks: A stochastic geometry approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 15844-15857, Dec. 2023.
- [19] A. Bansal, K. Singh, B. Clerckx, C.-P. Li, and M.-S. Alouini, "Rate-splitting multiple access for intelligent reflecting surface aided multi-user communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9217-9229, Sep. 2021.
- [20] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169-8181, Oct. 2019.
- [21] 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.
- [22] S. Mohammad Raghheb, M. S. Hemami, A. Kuesthani, D. W. K. Ng, and L. Hanzo, "On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 53-68, Nov. 2021.
- [23] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114-2127, May 2017.
- [24] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2675-2689, Apr. 2018.
- [25] Y. Ju, H. Wang, Q. Pei, and H.-M. Wang, "Physical layer security in millimeter wave DF relay systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5719-5733, Dec. 2019.
- [26] S. Huang, M. Xiao, and H. V. Poor, "On the physical layer security of millimeter wave NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11697-11711, Oct. 2020.
- [27] P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2658-2693, Nov. 2020.
- [28] M. Abolpour, S. Aissa, L. Musavian, and A. Bhowal, "Rate splitting in the presence of untrusted users: Outage and secrecy outage performances," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 921-935, Jun. 2022.
- [29] Y. Tong, D. Li, Z. Yang, Z. Xiong, N. Zhao, and Y. Li, "Outage analysis of rate splitting networks with an untrusted user," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2626-2631, Feb. 2023.
- [30] A. Salem, C. Masouros, and B. Clerckx, "Secure rate splitting multiple access: How much of the split signal to reveal?," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 4173-4187, Jun. 2023.
- [31] H. Lei, D. Sang, I. S. Ansari, N. Saeed, G. Pan, and M.-S. Alouini, "Trusted transmission: Strengthening security in CR-inspired RSMA systems amidst untrusted users," in *Proc. 2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, Apr. 2024.
- [32] H. Lei, S. Zhou, K.-H. Park, I. S. Ansari, H. Tang, and M.-S. Alouini, "Outage analysis of millimeter wave RSMA systems," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1504-1520, Mar. 2023.
- [33] H. Lei, R. Gao, K.-H. Park, I. S. Ansari, K. J. Kim, and M.-S. Alouini, "On secure downlink NOMA systems with outage constraint," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7824-7836, Dec. 2020.
- [34] H. Lei, F. Yang, H. Liu, I. S. Ansari, K. J. Kim, and T. A. Tsiftsis, "On secure NOMA-aided semi-grant-free systems," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 74-90, Jan. 2024.
- [35] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, and J. Zhang, "Overview of millimeter wave communications for fifth-generation (5G) wireless networks—with a focus on propagation models," *IEEE T. Antenn. Propag.*, vol. 65, no. 12, pp. 6213-6230, Dec. 2017.
- [36] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th edition. Academic Press, 2007.
- [37] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th. New York, NY, USA: Dover Press, 1972.
- [38] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. the international symposium on Symbolic and algebraic computation (ISSAC '90)*, Tokyo, Japan, Aug. 1990, pp. 212-224.
- [39] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. Berlin, Germany: Springer, 2010.
- [40] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over α - μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445-1448, Jun. 2017.