Physical Layer Security Over Fluctuating Two-Ray Fading Channels

Wen Zeng, Jiayi Zhang, *Member, IEEE*, Shuaifei Chen, Kostas P. Peppas, *Senior Member, IEEE*, and Bo Ai, *Senior Member, IEEE*

***Abstract*—Ensuring the physical layer security (PHY-security) of millimeter-wave (mmWave) communications is one of the key factors for the success of 5G. Recent field measurements show that conventional fading models cannot accurately model the random fluctuations of mmWave signals. To tackle this challenge, the fluctuating two-ray (FTR) fading model has been proposed. In this correspondence, we comprehensively analyze the PHY-security in mmWave communications over FTR fading channels. More specifically, we derive analytical expressions for significant PHY-security metrics, such as the average secrecy capacity, the secrecy outage probability, and the probability of strictly positive secrecy capacity, with simple functions. The effect of channel parameters on the PHY-security has been validated by numerical results.**

***Index Terms*—Average secrecy capacity, physical layer security, millimeter wave, fluctuating two-ray fading.**

I. Introduction

As a promising technique for supporting skyrocket data rate in fifth-generation (5G), millimeter wave (mmWave) communications have received an increasing attention due to the large available bandwidth at mmWave frequencies [1]. Given the ubiquitousness of wireless channels, mmWave communications are particularly vulnerable to a set of eavesdropping and impersonation attacks. Compared to cryptographic technologies implemented at upper layers, physical layer security (PHY-security) is a low-complexity alternative that exploits the randomness of wireless channels to safeguard the confidential information transmission [2].

An increasing number of literatures show their interests of exploring the PHY-security in mmWave communications [3]–[5]. For example, the effect of peculiar mmWave channel characteristics on the PHY-security performance in mmWave Ad hoc networks has been studied in [3]. In [4], PHY-security transmissions under slow fading channels with multipath propagation in mmWave communications were studied. However, both [3] and [4] neglected the small-scale fading of mmWave channel. Leveraging on a stochastic geometry framework, the authors of [5] investigated the downlink PHY-security performance in an mmWave cellular network assuming Nakagami-m fading. Moreover, the PHY-security performance of hybrid mmWave networks has been investigated in [6], [7].

Most of works only pay attention to the PHY-security in mmWave communications over slow fading channels. The small-scale channel model is also important for taking a deeper look into signal processing for mmWave communications, such as beamforming and precoding. Very recently, a 28 GHz outdoor measurement campaign showed that conventional small-scale fading models [8] (e.g., Rayleigh, Rician and Nakagami-m) cannot accurately model the random fluctuations suffered by mmWave signals [9]. In order to circumvent this issue, the fluctuating two-ray (FTR) fading model proposed in [10] can capture the bimodality of mmWave channels, which is more accurate than conventional fading models.

Therefore, the PHY-security performance of mmWave communications over FTR fading channels is still a significant and unsolved problem. Motivated by that, we provide a further investigation on the comprehensive analysis of the PHY-security performance of mmWave communications and derive analytical exact expressions for the average secrecy capacity (ASC), the secrecy outage probability (SOP), and the probability of strictly positive secrecy capacity (SPSC). Since the FTR includes Rayleigh, Rician, and Nakagami-m as special cases, the derived results can reduce to many pioneering works. Moreover, our work is beneficial to evaluate the state of the art PHY-security techniques and get better insight into the application of the FTR fading models in practical mmWave communications.

II. System Model

Hereafter, we consider the classic Wyner's wiretap model, which has been widely applied in the PHY-security analysis for mmWave communications [5]–[7], [11]. Suppose that the source S sends a message to the legitimate receiver D over the main channel while the eavesdropper E attempts to decode this message from its received signal through the eavesdropper channel. It is assumed that the main and eavesdropper channels experience independent FTR fading. Furthermore, we assume that the full channel state information (CSI) of both main and eavesdropper channels is available at S.

A. FTR Channel Model

The FTR channel model consists of two fluctuating specular components with random phases plus a diffuse component, and incorporates ground reflections in mmWave channels [10]. The probability distribution function (PDF) and cumulative distribution function (CDF) of the instantaneous signal-to-noise ratio (SNR) over FTR channel are

Manuscript received December 2, 2017; revised March 23, 2018 and May 23, 2018; accepted May 27, 2018. Date of publication May 30, 2018; date of current version September 17, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61601020, in part by the Beijing Natural Science Foundation under Grants 4182049 and L171005, in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2018D04, and in part by KLOCN2018002. The review of this paper was coordinated by Prof. M. C. Gursoy. *(Corresponding author: Jiayi Zhang.)*

W. Zeng, J. Zhang, and S. Chen are with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: 16120162@bjtu.edu.cn; jiayizhang@bjtu.edu.cn; 14221092@bjtu.edu.cn).

K. P. Peppas is with the Department of Informatics and Telecommunications, University of Peloponnese, Tripoli 22100, Greece (e-mail: peppas@uop.gr).

B. Ai is with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China (e-mail: aibo@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2842126

expressed as [12]

$$f_i(\gamma_i) = \frac{m_i^{m_i}}{\Gamma(m_i)} \sum_{j_i=0}^{\infty} \frac{K_i^{j_i} d_{j_i}}{j_i! j_i!} \frac{\gamma_i^{j_i}}{(2\sigma_i^2)^{j_i+1}} \exp\left(-\frac{\gamma_i}{2\sigma_i^2}\right), \quad (1)$$

$$F_i(\gamma_i) = \frac{m_i^{m_i}}{\Gamma(m_i)} \sum_{j_i=0}^{\infty} \frac{K_i^{j_i} d_{j_i}}{j_i! j_i!} \gamma\left(j_i+1, \frac{\gamma_i}{2\sigma_i^2}\right), \quad (2)$$

where $i \in \{D, E\}$ represents the main channel or the eavesdropper channel, d_{j_i} is expressed in terms of the fading parameters m_i, K_i and Δ_i, defined in [12, Eq. (9)], and $\gamma(\cdot,\cdot)$ is the incomplete gamma function [13, Eq. (8.350.1)].

The performance of mmWave links is also affected by large-scale blockages, such as buildings, in urban areas. Several past research works, e.g. [14] and references therein, have pointed out that blockages result in significant differences between the path loss characteristics of the line-of-sight (LOS) and the non-line-of-sight (NLOS) components. In [14], the so-called LoS ball blockage model has been considered which approximates general LOS probability functions as a step function to render mathematical analysis tractable. According to this model, the LOS probability of the link equals to one within a certain sphere of fixed radius R_B and zero elsewhere. Assuming that the propagation distance, r_i, lies within this sphere, the average SNR at D or E is given as

$$\bar{\gamma}_i = (E_b/N_0)\, 2\sigma_i^2 (1+K_i)\, r_i^{-\eta_i}, \quad i \in \{D, E\}, \quad (3)$$

where E_b/N_0 is the energy per bit to the noise power spectral density ratio, η_i is path-loss exponent, and $2\sigma_i^2$ is the average power of the diffuse component over the FTR fading.

B. Truncation Error

By truncating (1) up to the first $N_i + 1$ terms, the truncation error is given as

$$\hat{f}_i(\gamma_i) = \frac{m_i^{m_i}}{\Gamma(m_i)} \sum_{j_i=0}^{N_i} \frac{K_i^{j_i} d_{j_i} \gamma_i^{j_i} \exp\left(-\frac{\gamma_i}{2\sigma_i^2}\right)}{j_i! \Gamma(j_i+1) (2\sigma_i^2)^{j_i+1}}. \quad (4)$$

The truncation error of the area under the $f_i(\gamma_i)$ to the first $N_i + 1$ terms is given by

$$\varepsilon_i(N_i) \triangleq \int_0^{\infty} f_i(\gamma_i)\, d\gamma_i - \int_0^{\infty} \hat{f}_i(\gamma_i)\, d\gamma_i. \quad (5)$$

Substituting (1) and (4) into (5) and with the help of [13, Eq. (8.312.2)], (5) can be expressed in closed-form as

$$\varepsilon_i(N_i) = 1 - \frac{m_i^{m_i}}{\Gamma(m_i)} \sum_{j_i=0}^{N_i} \frac{K_i^{j_i} d_{j_i}}{j_i!}. \quad (6)$$

Table I depicts the statistic truncation parameter N_i for different combinations of channel parameters. Note that the maximum required term for accurate N_i is only 27 in all considered cases. In the realistic propagation environment, the main channel and the eavesdropper channel may have different fading parameters, which results different values of truncation parameters. In this case, we define the truncation parameter N as $N \triangleq \max\{N_D, N_E\}$.

TABLE I
REQUIRED TERMS N_i FOR THE TRUNCATION ERROR ($\varepsilon_i \leq 10^{-5}$) WITH DIFFERENT CHANNEL PARAMETERS m_i, K_i, AND Δ_i

FTR Fading Parameters	N_i	ε_i
m_i=15.5, K_i=5, Δ_i=0.4	24	6.27×10^{-6}
m_i=8.5, K_i=5, Δ_i=0.35	27	6.025×10^{-6}
m_i=25.5, K_i=3, Δ_i=0.48	16	8.447×10^{-6}

III. PHY-Security Performance Analysis Over FTR Fading Channels

A. ASC Analysis

Recall that the full CSI of both the main and eavesdropper channels is available at S, which is called as active eavesdropping [15]. In such a scenario, S can adapt the achievable secrecy rate to R_s such that $R_s \leq C_s$. Thus, according to [16], the instantaneous secrecy capacity is defined as

$$C_s(\gamma_D, \gamma_E) = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\}, \quad (7)$$

where $\ln(1+\gamma_D)$ and $\ln(1+\gamma_E)$ are the capacity of the main and eavesdropper channels, respectively. Since both main and eavesdropper channels experience independent fading, the ASC can be given by

$$\begin{aligned}\bar{C}_s(\gamma_D, \gamma_E) &= \int_0^{\infty}\int_0^{\infty} C_s(\gamma_D, \gamma_E) f(\gamma_D, \gamma_E)\, d\gamma_D\, d\gamma_E \\ &= \underbrace{\int_0^{\infty} \ln(1+\gamma_D) f_D(\gamma_D) F_E(\gamma_D) d\gamma_D}_{I_1} \\ &\quad + \underbrace{\int_0^{\infty} \ln(1+\gamma_E) f_E(\gamma_E) F_D(\gamma_E) d\gamma_E}_{I_2} \\ &\quad - \underbrace{\int_0^{\infty} \ln(1+\gamma_E) f_E(\gamma_E) d\gamma_E}_{I_3}, \end{aligned} \quad (8)$$

where $f(\gamma_D, \gamma_E) = f_D(\gamma_D) f_E(\gamma_E)$ is the joint pdf of γ_D and γ_E. With the help of (1), (2) and (8), we can obtain the ASC over FTR fading channels in the following Lemma.

Lemma 1: The ASC over FTR fading channels can be expressed as (10) at the bottom of the next page, where

$$S(w, \mu) \triangleq (w-1)! e^u \sum_{k=1}^{w} \frac{\Gamma(-w+k, \mu)}{\mu^k}. \quad (10)$$

Proof: Please see Appendix A. ■

Note that (9) is given in terms of only simple functions, which can be efficiently evaluated in common softwares.

B. SOP Analysis

When S has no information about the eavesdroppers channel, S has no choice but to encode the confidential data into codewords of a constant rate R_s. If $R_s \leqslant C_s$, perfect secrecy can be achieved and information theoretic security is compromised. The SOP is defined as the probability that the instantaneous secrecy capacity falls below a target rate, which is an important PHY-security performance metric

and widely used to characterize wireless communications. The SOP can be expressed as [17]

$$\begin{aligned}\text{SOP} &= P\left\{C_s\left(\gamma_D,\gamma_E\right) < R_s\right\}\\ &= P\left\{\gamma_D < \Theta\gamma_E + \Theta - 1\right\}\\ &= \int_0^\infty F_D\left(\Theta\gamma_E + \Theta - 1\right) f_E\left(\gamma_E\right) d\gamma_E, \end{aligned} \tag{11}$$

where $R_s \geqslant 0$ is the target secrecy capacity threshold, and $\Theta \triangleq e^{R_s}$. Substituting (1) and (2) into (11), we can obtain the SOP over FTR fading channels in the following Lemma.

Lemma 2: The SOP over FTR fading channels can be expressed as

$$\begin{aligned}\text{SOP} = &\frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma\left(m_D\right)\Gamma\left(m_E\right)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!}\\ &\times \left(1 - \sum_{n=0}^{j_D}\sum_{q=0}^{n} \binom{n}{q} \frac{1}{n!\, j_E!} \exp\left(-\frac{\Theta-1}{2\sigma_D^2}\right)\right.\\ &\left.\times \frac{\Theta^q(\Theta-1)^{n-q}\Gamma\left(j_E+1+q\right)\left(2\sigma_E^2\right)^q}{\left(1+\frac{\sigma_E^2\,\Theta}{\sigma_D^2}\right)^{j_E+q+1}\left(2\sigma_D^2\right)^n}\right). \end{aligned} \tag{12}$$

Proof: Please see Appendix B. ■

By adopting a similar method in [18], we derive the lower bound of the SOP based on (11) as

$$\text{SOP}^L = P\left\{\gamma_D < \Theta\gamma_E\right\} \leq \text{SOP}. \tag{13}$$

Substituting (1) and (2) into (13), the lower bound of the SOP over FTR fading channels is derived in the following Lemma.

Lemma 3: The lower bound of the SOP over FTR fading channels can be expressed as

$$\begin{aligned}SOP^L = &\frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma\left(m_D\right)\Gamma\left(m_E\right)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!}\\ &\times \frac{(\rho\eta)^{j_E}\,\Theta^{j_D+1}}{(\Theta+\rho\eta)^{j_D+j_E+1}} \sum_{k=0}^{j_E}\left(\frac{\Theta}{\rho\eta}\right)^k \frac{(j_D+j_E+1)!}{(j_D+1+k)!\,(j_E-k)!}, \end{aligned} \tag{14}$$

where $\rho \triangleq \frac{\bar{\gamma}_D}{\bar{\gamma}_E} = \frac{\sigma_D^2\left(K_D+1\right)}{\sigma_E^2\left(K_E+1\right)}$ and $\eta \triangleq \frac{K_E+1}{K_D+1}$.

Proof: Please see Appendix C. ■

C. SPSC Analysis

The probability of SPSC, which is a fundamental benchmark in secure communications, can be obtained by [17]

$$\begin{aligned}SPSC &= P\left\{C_s\left(\gamma_D,\gamma_E\right) > 0\right\} = P\left\{\gamma_D > \gamma_E\right\}\\ &= 1 - \text{SOP}^L_{R_s=0}. \end{aligned} \tag{15}$$

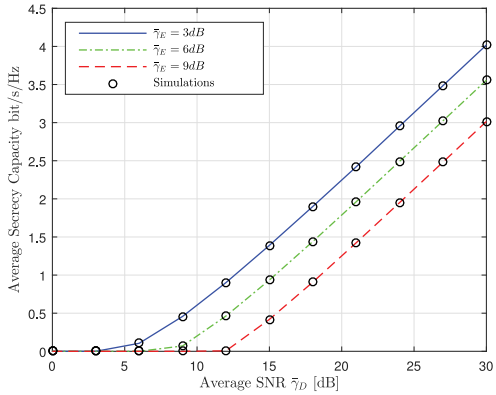

Fig. 1. ASC over FTR fading channels against $\bar{\gamma}_D$ for different values of $\bar{\gamma}_E$ ($K_D = 15, K_E = 5, m_D = 5.5, m_E = 8.5, \Delta_D = 0.4$, and $\Delta_E = 0.35$).

Therefore, we can obtain SPSC by substituting (14) into (15) and setting $\Theta = e^{R_s} = 1$.

IV. Numerical Results

In this section, we present some plots that illustrate the ASC, SOP and SPSC of mmWave communications over FTR fading channels with. For the Monte Carlo simulation, 10^6 realizations of FTR fading channels are generated to validate the analytical expressions derived in previous sections and the propagation distance r_i is normalized to 1 km.

The ASC as a function of $\bar{\gamma}_D$ in dB is depicted in Fig. 1 for $\bar{\gamma}_E = 3, 6, 9$ dB. The outputs of a Monte Carlo simulator are shown to exactly match with the analytical results, which validates our derived results. As expected, the performance of ASC improves with increasing $\bar{\gamma}_D$ or decreasing $\bar{\gamma}_E$. Note that the ASC will fall to zero if the average SNR of the main channel is smaller than the eavesdropper channel ($\bar{\gamma}_D < \bar{\gamma}_E$), which is consistent with (7).

In Fig. 2, we portray the exact and the lower bound of SOP as a function of the average SNR of the eavesdropper channel $\bar{\gamma}_E$. The high-SNRs of $\bar{\gamma}_E$ make the lower bound of the SOP sufficiently tight with the exact SOP. It is clear that the lower bound of SOP becomes accurate as the value of R_s decreases. Moreover, it can be observed that the SOP performance of the considered system is improved by decreasing the values of $\bar{\gamma}_E$, which is consistent with the results presented in Lemma 2 and Lemma 3.

Fig. 3 investigates the impact of the ratios between $\bar{\gamma}_D$ and $\bar{\gamma}_E$, ρ, on the SOP performance. The achievable secrecy rates R_s are considered ($R_s = 1, 2, 3, 4$ bit/s/Hz). Intuitively, as ρ become large, the main channel is much better than the eavesdropper channel and the SOP becomes decreasingly substantial. In addition, smaller R_s can obtain smaller SOP, which is consistent with the results presented in Lemma 2.

$$\begin{aligned}ASC = &\frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma\left(m_D\right)\Gamma\left(m_E\right)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!} \left(\frac{S\left(j_D+1,\left(2\sigma_D^2\right)^{-1}\right)}{j_D!\left(2\sigma_D^2\right)^{j_D+1}} + \frac{S\left(j_E+1,\left(2\sigma_E^2\right)^{-1}\right)}{j_E!\left(2\sigma_E^2\right)^{j_E+1}}\right.\\ &\left. - \sum_{n=0}^{j_E}\frac{S\left(j_D+n+1,\frac{\sigma_D^2+\sigma_E^2}{2\sigma_D^2\,\sigma_E^2}\right)}{n!j_D!\left(2\sigma_E^2\right)^n\left(2\sigma_D^2\right)^{j_D+1}} - \sum_{n=0}^{j_D}\frac{S\left(j_E+n+1,\frac{\sigma_D^2+\sigma_E^2}{2\sigma_D^2\,\sigma_E^2}\right)}{n!j_E!\left(2\sigma_D^2\right)^n\left(2\sigma_E^2\right)^{j_E+1}}\right) - \frac{m_E^{m_E}}{\Gamma\left(m_E\right)}\sum_{j_E=0}^{\infty}\frac{K_E^{j_E}\, d_{j_E}\, S\left(j_E+1,\left(2\sigma_E^2\right)^{-1}\right)}{j_E!j_E!\left(2\sigma_E^2\right)^{j_E+1}}, \end{aligned} \tag{10}$$

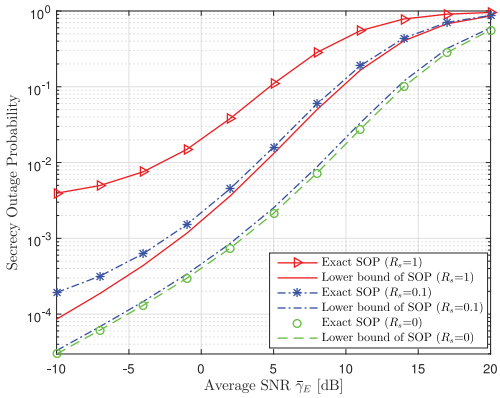

Fig. 2. SOP over FTR fading channels against $\bar{\gamma}_E$ for different values of R_s ($K_D = 15, K_E = 5$, $m_D = 5.5, m_E = 8.5$, $\Delta_D = 0.4$, $\Delta_E = 0.35$, and $\bar{\gamma}_D = 15$ dB).

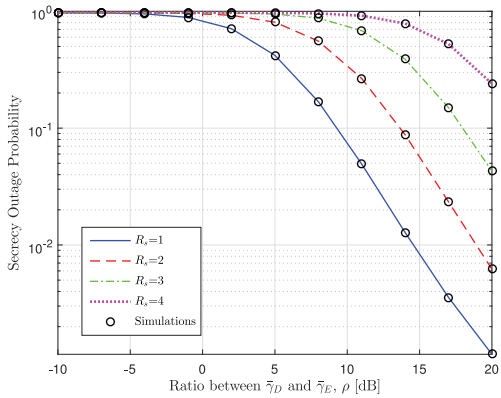

Fig. 3. SOP over FTR fading channels against ρ for different values of R_s ($K_D = K_E = 8, m_D = m_E = 5.5$, and $\Delta_D = \Delta_E = 0.4$).

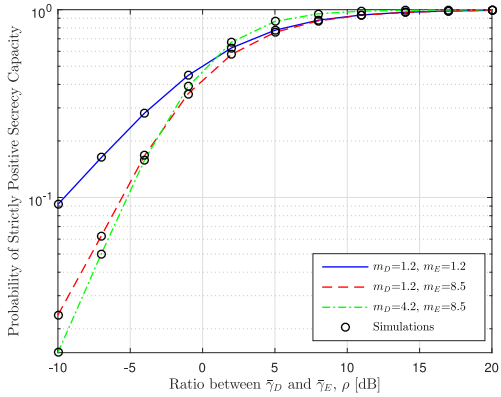

Fig. 4. SPSC over FTR fading channels against ρ for different values of m_D and m_E ($K_D = K_E = 8, \Delta_D = \Delta_E = 0.3$, and $R_s = 0$).

Fig. 4 illustrates the effect of shadowing on the SPSC performance of mmWave communications over FTR fading channels. As can be readily observed, the light shadowing (small values of m) in eavesdropper channel will increase the SPSC. Furthermore, in the moderate- and high-ρ regime, increasing the shadowing effect of the main channel m_D can increase the SPSC performance, which is not observed in the very low-ρ regime.

V. Conclusion

In this correspondence, we investigate the PHY-security performance of mmWave communications over FTR fading channels. We derive analytical expressions for the ASC, SOP and SPSC in terms of simple functions, which can quickly and steadily converge with only a few of N terms to obtain a desired accuracy. Note that derived results can reduce to many pioneering works, since the FTR includes Rayleigh, Rician, and Nakagami-m as special cases. Our analysis validates that the performance of the considered system can be improved with increasing the average SNR of the main channel or decreasing the average SNR of the eavesdropper channel. Moreover, the light shadowing (small values of m) in eavesdropper channel will increase the SPSC. As for current and future directions, it is of interest to investigate the PHY-security performance of mmWave communications by considering more practical channel and system features, such as blockages, interference, and multi-antenna.

Appendix

A. Proof of Lemma 1

For the natural number j_i, the gamma function $\Gamma(\cdot)$ can be expressed as $\Gamma(j_i+1) = j_i!$ [13, Eq. (8.339.1)]. Then, substituting (1) and (2) into (8), I_1 can be expressed as

$$I_1 = \frac{m_D^{m_D}}{\Gamma(m_D)} \frac{m_E^{m_E}}{\Gamma(m_E)} \sum_{j_D=0}^{\infty} \sum_{j_E=0}^{\infty} \frac{K_D^{j_D} d_{j_D} K_E^{j_E} d_{j_E}}{j_D! j_E! j_D! j_E! (2\sigma_D^2)^{j_D+1}} \times \underbrace{\int_0^{\infty} \ln(1+\gamma_D) \gamma_D^{j_D} e^{-\frac{\gamma_D}{2\sigma_D^2}} \gamma\left(j_E+1, \frac{\gamma_D}{2\sigma_E^2}\right) d\gamma_D}_{A_1}, \quad (16)$$

In order to solve the inner integral A_1, with the help of [13, Eq. (8.354.1)], we have

$$\gamma\left(j_E+1, \frac{\gamma_D}{2\sigma_E^2}\right) = j_E! \left(1 - e^{-\frac{\gamma_D}{2\sigma_E^2}} \sum_{n=0}^{j_E} \frac{1}{n!} \left(\frac{\gamma_D}{2\sigma_E^2}\right)^n\right). \quad (17)$$

Substituting (17) into A_1 and formulating the integral as $S(w,\mu) \triangleq \int_0^{\infty} \ln(1+t) t^{w-1} e^{-\mu t} dt$, we can obtain

$$A_1 = j_E! S\left(j_D+1, \frac{1}{2\sigma_D^2}\right) - j_E! \sum_{n=0}^{j_E} \frac{1}{n!} \left(\frac{1}{2\sigma_E^2}\right)^n S\left(j_D+n+1, \frac{\sigma_D^2+\sigma_E^2}{2\sigma_D^2\sigma_E^2}\right). \quad (18)$$

Since w is a natural number in the integral $S(w,\mu)$, we can have (10) as in [19]. Substituting (18) and (10) into (16), and after a simple transformation of the variables, I_1 is given as

$$I_1 = \frac{m_D^{m_D} m_E^{m_E}}{\Gamma(m_D)\Gamma(m_E)} \sum_{j_D=0}^{\infty} \sum_{j_E=0}^{\infty} \frac{K_D^{j_D} d_{j_D} K_E^{j_E} d_{j_E}}{j_D! j_E! j_D! (2\sigma_D^2)^{j_D+1}} \times \left(S\left(j_D+1, \frac{1}{2\sigma_D^2}\right) - \sum_{n=0}^{j_E} \frac{S\left(j_D+n+1, \frac{\sigma_D^2+\sigma_E^2}{2\sigma_D^2\sigma_E^2}\right)}{n!(2\sigma_E^2)^n} \right). \quad (19)$$

Following similar steps, we can obtain I_2 and I_3 as

$$I_2 = \frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma(m_D)\,\Gamma(m_E)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!\, j_E!\, (2\sigma_E^2)^{j_E+1}} \times \left(S\left(j_E+1, \frac{1}{2\sigma_E^2}\right) - \sum_{n=0}^{j_D} \frac{S\left(j_E+n+1, \frac{\sigma_D^2+\sigma_E^2}{2\sigma_D^2\sigma_E^2}\right)}{n!(2\sigma_D^2)^n} \right). \quad (20)$$

$$I_3 = \frac{m_E^{m_E}}{\Gamma(m_E)} \sum_{j_E=0}^{\infty} \frac{K_E^{j_E}\, d_{j_E}\, S\left(j_E+1, (2\sigma_E^2)^{-1}\right)}{j_E!\, j_E!\, (2\sigma_E^2)^{j_E+1}}. \quad (21)$$

Then, we can obtain (10) by combining (19), (20) and (21).

B. Proof of Lemma 2

Substituting (1) and (2) into (11), we can obtain

$$\mathrm{SOP} = \frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma(m_D)\,\Gamma(m_E)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!\, j_D!\, j_E!\, (2\sigma_E^2)^{j_E+1}} \times \underbrace{\int_0^{\infty} \gamma_E^{j_E}\, e^{-\frac{\gamma_E}{2\sigma_E^2}}\, \gamma\left(j_D+1, \frac{\Theta\gamma_E+\Theta-1}{2\sigma_D^2}\right) d\gamma_E}_{I_4}. \quad (22)$$

With the help of [13, Eq. (8.354.1)], I_4 can be expressed as

$$I_4 = j_D! \underbrace{\int_0^{\infty} \gamma_E^{j_E}\, e^{-\frac{\gamma_E}{2\sigma_E^2}}\, d\gamma_E}_{I_5} - j_D! \sum_{n=0}^{j_D} \frac{1}{n!} \left(\frac{1}{2\sigma_D^2}\right)^n e^{\frac{1-\Theta}{2\sigma_D^2}} \times \underbrace{\int_0^{\infty} \gamma_E^{j_E}\, e^{-\frac{\gamma_E}{2\sigma_E^2}-\frac{\Theta\gamma_E}{2\sigma_D^2}} (\Theta\gamma_E+\Theta-1)^n\, d\gamma_E}_{I_6}. \quad (23)$$

Using [13, Eq. (3.326)] and [13, Eq. (1.111)], we have

$$I_5 = \Gamma(j_E+1)\left(2\sigma_E^2\right)^{j_E+1}, \quad (24)$$

$$I_6 = \sum_{q=0}^{n} \binom{n}{q} \frac{\Theta^q (\Theta-1)^{n-q}\, \Gamma(j_E+1+q)}{\left(\frac{1}{2\sigma_E^2}+\frac{\Theta}{2\sigma_D^2}\right)^{j_E+q+1}}. \quad (25)$$

The proof concludes by combining (22)–(25).

C. Proof of Lemma 3

Substituting (1) and (2) into (13), we can obtain

$$SOP^L = \frac{m_D^{m_D}\, m_E^{m_E}}{\Gamma(m_D)\,\Gamma(m_E)} \sum_{j_D=0}^{\infty}\sum_{j_E=0}^{\infty} \frac{K_D^{j_D}\, d_{j_D}\, K_E^{j_E}\, d_{j_E}}{j_D!\, j_E!\, j_D!\, j_E!\, (2\sigma_E^2)^{j_E+1}} \times \underbrace{\int_0^{\infty} \gamma_E^{j_E}\, \exp\left(-\frac{\gamma_E}{2\sigma_E^2}\right) \gamma\left(j_D+1, \frac{\Theta\gamma_E}{2\sigma_D^2}\right) d\gamma_E}_{I_7}. \quad (26)$$

With the help of [13, Eq. (6.455.2)], I_7 can be expressed as

$$I_7 = \frac{\Gamma(j_D+j_E+2)}{(j_D+1)} \left(\frac{\Theta}{2\sigma_D^2}\right)^{j_D+1} \left(\frac{\Theta}{2\sigma_D^2}+\frac{1}{2\sigma_E^2}\right)^{-(j_D+j_E+2)} \times {}_2F_1\left(1, j_D+j_E+2; j_D+2; \frac{\sigma_E^2\Theta}{\sigma_E^2\Theta+\sigma_D^2}\right), \quad (27)$$

where ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the Gauss hypergeometric function [13, Eq. (9.14)]. Using [20, Eq. (7.3.1.129)], the proof concludes by combining (27) and (26) with some simplifications.

REFERENCES

[1] J. Zhang, L. Dai, X. Li, Y. Liu, and L. Hanzo, "On low-resolution ADCs in practical 5G millimeter-wave massive MIMO systems," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 205–211, Jul. 2018.

[2] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Jan. 2017.

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

[4] 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.

[5] 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.

[6] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[7] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[8] J. Zhang, L. Dai, Z. He, S. Jin, and X. Li, "Performance analysis of mixed-ADC massive MIMO systems over Rician fading channels," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1327–1338, Jun. 2017.

[9] S. Sun, H. Yan, G. R. MacCartney, and T. S. Rappaport, "Millimeter wave small-scale spatial statistics in an urban microcell scenario," in *Proc. IEEE Int. Conf. Commun.*, May 2017, pp. 1–7.

[10] J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith, "The fluctuating two-ray fading model: Statistical characterization and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4420–4432, Jul. 2017.

[11] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[12] J. Zhang, W. Zeng, X. Li, Q. Sun, and K. P. Peppas, "New results on the fluctuating two-ray model with arbitrary fading parameters and its applications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2766–2700, Mar. 2018.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 1980.

[14] 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.

[15] L. Wang, M. Elkashlan, J. Huang, and R. Schober, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[16] I. Csiszar and J. Korner, *Broadcast Channels with Confidential Messages*. Piscataway, NJ, USA: IEEE Press, 1978.

[17] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. Mclaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[18] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized Gamma fading channels," *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1257–1260, Jul. 2015.

[19] M. S. Alouini and A. J. Goldsmith, "Capacity of rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1165–1181, Apr. 1999.

[20] A. P. Prudnikov, I. U. A. Brychkov, and O. I. Marichev, *Integrals and Series. Volume 3: More Special Functions.* New York, NY, USA: Gordon & Breach, 1986.