IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 2, 2018, accepted July 3, 2018, date of publication July 9, 2018, date of current version August 7, 2018.

*Digital Object Identifier 10.1109/ACCESS.2018.2854233*

# On the Secrecy Performance of Land Mobile Satellite Communication Systems

**KANG AN[1], TAO LIANG[1], XIAOJUAN YAN[2,3], (Student Member, IEEE), AND GAN ZHENG[4], (Senior Member, IEEE)**

[1] Sixty-third/63$^{rd}$ Research Institute, National University of Defense Technology, Nanjing 210007, China
[2] School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China
[3] Engineering Training Center, Qinzhou University, Qinzhou 535011, China
[4] Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough LE11 3TU, U.K.

Corresponding author: Tao Liang (liangtao63@sina.com)

The work of K. An and T. Liang was supported by the National Natural Science Foundation of China under Grant 61471392. The work of X. Yan was supported in part by the Innovation Project of Guangxi Graduate Education and in part by the Innovation Project of GUET Graduate Education under Grant 2016YJCXB05. The work of G. Zheng was supported in part by the U.K. EPSRC under Grant EP/N007840/1 and in part by the Leverhulme Trust under Grant RPG-2017-129.

**ABSTRACT** In this paper, we investigate the secrecy performance against eavesdropping of a land mobile satellite (LMS) system, where the satellite employs the spot beam technique, and both the terrestrial user and eavesdropper are equipped with multiple antennas and utilize maximal ratio combining to receive the confidential message. Specifically, in terms of the availability of the eavesdropper's CSI at the satellite, we consider both passive (Scenario I) and active (Scenario II) eavesdropping. For Scenario I where the eavesdropper's channel state information (CSI) is unknown to the satellite, closed-form expressions for the probability of non-zero secrecy capacity and secrecy outage probability are derived. Furthermore, expressions for the asymptotic secrecy outage probability are also presented to reveal the secrecy diversity order and array gain of the considered system. For Scenario II where the eavesdropper's CSI is available at the satellite, novel expressions for the exact and asymptotic average secrecy capacity are obtained. Based on a simple asymptotic formula, we can characterize the high signal-to-noise ratio (SNR) slope and high SNR power offset of the LMS systems. Finally, simulations are provided to validate our theoretical analysis and show the effect of different parameters on the system performance.

**INDEX TERMS** Secrecy performance analysis, satellite communication, multi-antenna, shadowed-Rican fading.

## I. INTRODUCTION

Land mobile satellite (LMS) systems have been widely applied in broadcasting, navigation, and disaster relief, due to their potential for providing wide-area coverage and high data transmission rate, especially in situations where the deployment of wired and wireless terrestrial networks is not economically viable [1]. Due to the economical or implemental advantages, LMS systems can provide various telecommunications and multimedia mobile satellite service (MSS). Over the recent years, substantial effort has been done on the optimization design and performance analysis of LMS systems. Specifically, a generic optimization problem for LMS systems was proposed in [2] to handle the data rate with general linear and nonlinear power constraints. Christopoulos *et al.* [3] addressed the frame-based precoding problem within multibeam satellite networks. In addition, various performance metrics, including outage probability [4] and average symbol error rate [5] have been investigated for LMS systems with a single antenna. However, since multi-antenna technology has been widely recognized as an effective means of providing increased diversity and high system capacity [6], the incorporation of multi-antenna techniques into satellite communication systems have recently received much attention [7]–[9].

Despite the benefits of immense coverage area, the inherent broadcast nature of LMS systems make themselves prone to be eavesdropped by illegitimate users [10]. In this regard, privacy and security problem in satellite communications has received significant attentions. Traditionally, this kind of problem can be solved by the upper layers with the use of cryptographic protocols, i.e., the advanced encryption standard [11]. Nevertheless, the performance of current cryptographic schemes, which rely on the limited computational power of the eavesdropper, have become increasingly uncertain, since the computational ability of potential eavesdroppers is becoming more powerful [12]. Besides the cryptographic protocol in the upper layers, physical layer security (PLS) has been introduced to strengthen the secure transmission of wireless communications using an information-theoretic perspective [13], [14]. The key philosophy of physical layer security is to exploit the different characteristics of the channels to the desired user and eavesdropper. Specifically, Wyner [15] have done the foundation work for modern physical layer security. One seminal conclusion can be made from [15] was that a perfect secure transmission can be achieved if the quality of the legitimate user was superior to that of the eavesdropper.

Moreover, an eavesdropping environment can be classified in a passive or active eavesdropping scenario according to the transmitter knows the CSI of the eavesdropper or not. Until now, several works have been devoted to study the security performance in diverse scenarios, such as the work in [16] and [17]. Yang *et al.* [18] investigated the probability for non-zero capacity and secrecy outage probability of the multiple antenna wiretap channel with passive eavesdroppers and assuming maximal ratio combining (MRC) and selection combining (SC) in the presence of Nakagami-*m* fading. In [19], the secrecy outage probability of multiple antenna wiretap channels using transmit antenna selection and generalized selection combining (TAS/GSC) at the receiver was first studied for passive eavesdropping, and an extension to active eavesdropping scenarios was also presented, in which both the exact and asymptotic average secrecy capacity were analyzed.

The above works mainly investigated the secure performance in terrestrial scenarios. However, in satellite communications, where a legitimate user also suffers from wiretapping, limited work has been focused on physical layer security [20]–[22]. In a multibeam environment, an optimization power allocation problem was investigated in [20] by satisfying individual secrecy rate requirements, while the precoding problem was investigated in [21] under the constraint of minimizing the total onboard power and meeting individual secrecy rate demands. Moreover, the authors in [22] studied the secure satellite communications with network coding. In [23], a general construction of the wiretap coding and its applicability for a typical satellite channel were analyzed. Li *et al.* [24], [25] have proposed the joint secure design in cognitive satellite terrestrial networks by minimizing the transmit power with the leakage outage limit for the eavesdropper.

The information-theoretic basics, such as probability of non-zero secrecy capacity, secrecy outage probability, secrecy capacity and etc, are the fundamentals for the application of physical layer security in wireless communication networks [26]. Thus far, existing work on physical layer security in satellite systems has not focused on these related key performance metrics. Due to the particular propagation environments, LMS systems commonly suffer from multiple levels of obstructions (e.g., urban, suburb, and rural scenarios), thus the accuracy of both small- and largescale fading statistics depending upon several factors should be carefully considered. Because of the random channel fluctuations in time varying LMS fading channels, an enhanced secrecy performance can be opportunistically exploited depending on the channel conditions.

In this paper, we consider that a LMS system communicates with its legitimate user, while an unauthorized eavesdropper is present and tries to overhear. Then, we provide a comprehensive secrecy performance analysis of the considered network over the Shadowed-Rician fading channel, a model which was first proposed in [27] and has been widely exploited in satellite communications. Specifically, we assume that multiple antennas are equipped at the legitimate user and the eavesdropper, while the satellite employs spot beam transmission, and we consider two scenarios for detailed analysis, namely, Scenario I: passive eavesdropping, where the satellite has no knowledge of the eavesdropper's CSI, and Scenario II: active eavesdropping, where the CSI of the eavesdropper is available at the satellite.[1] We analyze the secrecy performance of the satellite systems by deriving new theoretical formulas. To the best of our knowledge, this is the first time such expressions are obtained.[2] Our detailed contributions can be outlined as follows:

- For Scenario I, since the transmitter has no information about the eavesdropper's channel, perfect secrecy cannot be guaranteed, so exact closed-form expressions for the probability of non-zero secrecy capacity and average secrecy outage probability are derived to evaluate the secrecy performance [16].
- To gain further insights, simple asymptotic expressions for the secrecy outage probability at the high SNR are obtained to reveal the secrecy diversity order and secrecy array gain. In particular, two representative cases are employed, namely, *Outside Beam Coverage (OBC)*: the eavesdropper is outside the beam coverage area, and *Inside Beam Coverage (IBC)*: the eavesdropper is within the beam coverage area. For *OBC*, we show that the full secrecy diversity order can be achieved, which is simply determined by the antenna configuration at the legitimate user. On the other hand, for IBC, the secrecy diversity order collapses to zero, indicating that increasing the transmit power at the satellite does not provide additional performance gain.
- For scenario II, the transmitter can adapt the transmission rate according to the CSI of both the main and eavesdropper's channel to achieve perfect secure

[1] Scenario II is particularly applicable in multicast and unicast networks where the users play dual roles as legitimate users for some signals and eavesdroppers for others. This scenario has been studied in existing work such as [26] and [28].

[2] The motivation of this paper is to provide the fundamental framework of information-theoretic based physical layer security for satellite communication systems in terms of different eavesdropping scenarios.

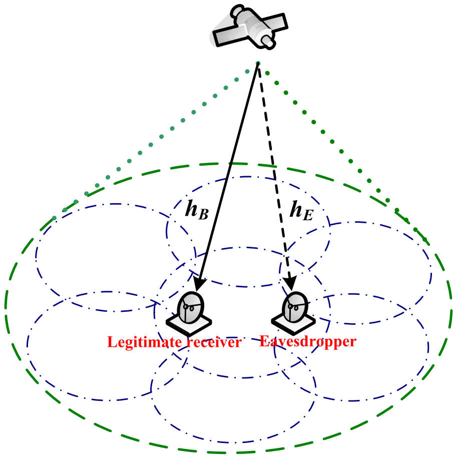

**FIGURE 1.** System model.

transmission. In this case, theoretical expressions for the average secrecy capacity is provided as the as the principle performance metric [19].

- The asymptotic average secrecy capacity is also derived for both the *OBC* and *IBC* cases to show the high SNR power offset and high SNR slope for the LMS systems. For *OBC*, we show that the high SNR slope remains one. For *IBC*, the average secrecy capacity approaches a plateau, which means the high SNR power offset degrades to zero. Moreover, the high SNR power offset is dependent on the beam gain ratio of the legitimate user and eavesdropper.
- Simulation results first show the joint impact of beam radius and locations on the secrecy performance of LMS systems. We observe that for a fixed distance between the legitimate user and eavesdropper, a narrow beam radius leads to enhanced secrecy performance. When the eavesdropper is outside the beam coverage, the secrecy performance of the LMS systems gradually fluctuates with a certain range, and is irrelevant to the beam radius.

The remainder of this paper is organized as follows. In Section II, we describe the system model. In Section III, we provide the statistical property of the satellite links. The secrecy performance of the considered LMS system are analyzed for different scenarios in Sections IV and V, respectively. Section VI shows the numerical results along with discussions. Eventually, useful conclusions are drawn in Section VII.

*Notation*: $E[\cdot]$ denotes the expectation operator, $\mathbb{C}^{M\times N}$ the space of $M \times N$ complex matrices, $|\cdot|$ the absolute value, $\|\cdot\|_F^2$ the Frobenius norm, $\mathcal{N}_C(m,\sigma^2)$ the complex Gaussian distribution with mean $m$ and variance $\sigma^2$.

## II. SYSTEM MODEL

As depicted in Fig. 1, we consider the downlink of a satellite communication network exploiting a geostationary satellite (Sat) with single antenna (a.k.a. feed) sends confidential message to the legitimate user (Bob) with $N_B$ antennas in the presence of an Eve with $N_E$ antennas attempting to overhear the satellite information signal in the same beam.[3,4] We assume that the CSI of satellite links is available at the gateway (GW), which can be realized by feedback/training sent from the terminals via a return channel, which already exists in current systems, such as DVB-S2 [2], [21].

### A. SATELLITE CHANNEL MODEL

To realistically model the feature of satellite networks in achieving physical layer security, the main characteristics of satellite channels should be properly modeled. Specifically, the composite fading distribution and on-board beam factor are taken into consideration [24], [25].

The beam gain is determined by the on-board antenna pattern and the position of a ground user. For the $i$-th receiver within the satellite spot beam coverage area, the beam gain can be approximated as [2]

$$b(\varphi_i) = \left(\frac{J_1(u_i)}{2u_i} + 36\frac{J_3(u_i)}{u_i^3}\right)^2, \tag{1}$$

where $u_i$ is given by

$$u_i = 2.07123\frac{\sin\varphi_i}{\sin\varphi_{3dB}}, \tag{2}$$

with $\varphi_i$ representing the angle between the position of the $i$-th receiver and the beam center, and $\varphi_{3dB}$ the angle corresponding to the 3-dB powerloss, which are, respectively, given by

$$\varphi_i = \arctan\left(\frac{d_i}{D}\right), \tag{3}$$

$$\varphi_{3dB} = \arctan\left(\frac{R}{D}\right), \tag{4}$$

where $R$ is the beam's radius, $D$ the distance between the satellite and $i$-th receiver, and $d_i$ the distance between the beam center and the $i$-th receiver. Since the distance between the user and beam center is much smaller than the satellite altitude, namely, $d_i \ll D$, the relative distance can be transformed into [29]

$$\varphi_i \approx \frac{d_i}{R}, \tag{5}$$

and we have

$$u_i = 2.07123\frac{d_i}{R}. \tag{6}$$

Besides the on-board beam pattern employed at the satellite, our work on physical layer security is distinguished

[3] The motivation of the employed SIMO system is due to the fact that the implementation of multiple antennas on a satellite, to fully exploit its channel capabilities, is not a suitable choice, due to the lack of scatterers in its vicinity, which is a common assumption in many existing works (see [6], [7] and the reference therein).

[4] For scenarios with multiple legitimate users, the user scheduling scheme should be further designed, which is an open topic beyond the interest in this paper. Moreover, if multiple eavesdroppers are considered, the cooperative or non-cooperative eavesdropping scenarios should be further discussed. The study of these issues could be our future works.

by use of the LMS channel model, which is different from that typically assumed for terrestrial wireless systems. Generally, satellite links are modeled by composite fading distributions to describe more accurately the amplitude fluctuation of the signal envelope. While various mathematical models, such as Loo, Barts-Stutzman, and Karasawa *et al.*, have been proposed to describe the satellite channel distributions, the Shadowed-Rician (SR) model presented in [27] has been recognized as the most commonly used one in analytical studies of LMS communication performance [4], [5], [7]–[9]. Particularly, the SR model has found wide applications in different frequency bands such as the UHF-band, L-band, S-band, and Ka-band [27]. In this model, elements of the channel vector are identical independently distributed (i.i.d) random variables described by

$$g_i = \bar{g}_i + \tilde{g}_i \tag{7}$$

where the line-of-sight (LOS) component $\bar{g}_i$ is composed of i.i.d Nakagami-$m$ random variables and the entries of the scattering component $\tilde{g}_i$ follow an i.i.d Rayleigh fading distribution. The SR channel links are denoted as $g_i \sim \mathrm{SR}\left(\Omega_i, b_i, m_i\right)$ with $\Omega_i$ representing the average power of the LoS component, $2b_i$ the average power of the multipath component, and $m_i$ the Nakagami-$m$ parameter corresponding to the severity of the fading. By combining the beam gain coefficient in (1) and the channel fading vector in (7), the overall satellite channel for $i$-th user can be modeled as

$$h_i = \sqrt{b\left(\varphi_i\right)} g_i. \tag{8}$$

### B. OUTPUT SINR

Let $x\left(t\right)$ be the signal transmitted by the satellite to a legitimate user with $N_B$ antennas. An eavesdropper with $N_E$ antennas tries to illegally overhear the transmitted signal from the satellite. Denoting $h_B \in \mathbb{C}^{N_B \times 1}$ and $h_E \in \mathbb{C}^{N_E \times 1}$ as the channel vectors for the Sat-Bob and Alice-Eve links, the received signals at Bob and Eve at time $t$ can be respectively expressed as

$$y_B\left(t\right) = \sqrt{P} w_B^H \left(h_B x\left(t\right) + n_B\left(t\right)\right) \tag{9}$$

$$y_E\left(t\right) = \sqrt{P} w_E^H \left(h_E x\left(t\right) + n_E\left(t\right)\right), \tag{10}$$

where $P$ denotes the transmit power at satellite, the amplitude of $x\left(t\right)$ is normalized to one, namely, $E\left[\left|x\left(t\right)\right|^2\right] = 1$, and $w_B \in \mathbb{C}^{N_B \times 1}$ and $w_E \in \mathbb{C}^{N_E \times 1}$ are the beamforming (BF) weight vectors at Bob and Eve, respectively. Meanwhile, $n_B\left(t\right) \sim \mathcal{N}_C\left(0, {\sigma_B}^2\right)$ and $n_E\left(t\right) \sim \mathcal{N}_C\left(0, {\sigma_E}^2\right)$ represent zero mean additive white Gaussian noise (AWGN) at Bob and Eve, respectively.

Similar to most related work such as [4]–[9], we consider that perfect CSI is available at each of the terminals. Thus, by employing MRC, namely, $w_B = h_B / \left\|h_B\right\|_F$ and $w_E = h_E / \left\|h_E\right\|_F$, the instantaneous received signal-to-noise ratio (SNR) at Bob and Eve can be, respectively, expressed as

$$\gamma_B = \frac{P}{\sigma_B} \left\|h_B\right\|_F^2 = \bar{\gamma}_B \left\|h_B\right\|_F^2, \tag{11}$$

$$\gamma_E = \frac{P}{\sigma_E} \left\|h_E\right\|_F^2 = \bar{\gamma}_E \left\|h_E\right\|_F^2, \tag{12}$$

where $\bar{\gamma}_B = Pb\left(\varphi_B\right) / \sigma_B$ and $\bar{\gamma}_E = Pb\left(\varphi_E\right) / \sigma_E$ denote, respectively, the average SNR of the Sat-Bob and Sat-Eve links.

### C. SECRECY RATE

Secure data transmission between Sat and Bob can be achieved under the condition that the quality of the main channel is better than that of eavesdropper's channel. According to [26] and [28], the achievable secrecy rate for the wiretap channel considered here is

$$C_S = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \le \gamma_E, \end{cases} \tag{13}$$

where $C_B = \log_2\left(1 + \gamma_B\right)$ and $C_E = \log_2\left(1 + \gamma_E\right)$ are the channel capacities of legitimate user and eavesdropper, respectively.

The information-theoretic based analysis are the fundamentals of physical layer security technique in both satellite and terrestrial communications. In what follows, depending on whether Eve's CSI is available at the satellite, we will investigate the secrecy performance of the LMS communication systems for the two different scenarios. In particular, we will analyze the probability of non-zero secrecy capacity, and derive the exact and asymptotic secrecy outage probabilities for Scenario I, and the exact and asymptotic average secrecy capacity for Scenario II, respectively.

## III. STATISTICAL PROPERTIES OF SATELLITE LINKS

In this section, we study the statistical properties of satellite links, which are useful for the subsequent derivations of our analytical expressions. According to [30], an exact analytical expression for the probability density function (PDF) of $\gamma_i = \bar{\gamma}_i \left\|h_i\right\|_F^2, i \in \{B, E\}$, is given by

$$\begin{aligned} f_{\gamma_i}\left(x\right) &= \alpha_i^{N_i} \sum_{l_i=0}^{c_i} \binom{c_i}{l_i} \beta_i^{c_i - l_i} \left[\left(\frac{x^{d_i - l_i - 1}}{\bar{\gamma}_i^{d_i - l_i} \Gamma\left(d_i - l_i\right)}\right)\right. \\ &\quad \times {}_1F_1\left(d_i; d_i - l_i; -\frac{\left(\beta_i - \delta_i\right)}{\bar{\gamma}_i} x\right) + \frac{\varepsilon_i \delta_i x^{d_i - l_i}}{\bar{\gamma}_i^{d_i - l_i + 1} \Gamma\left(d_i - l_i + 1\right)} \\ &\quad \left. \times {}_1F_1\left(d_i + 1; d_i - l_i + 1; -\frac{\left(\beta_i - \delta_i\right)}{\bar{\gamma}_i} x\right)\right] \end{aligned} \tag{14}$$

where ${}_1F_1\left(a; b; c\right)$ represents the confluent hypergeometric function [31, eq. (9.210.1)], $\alpha_i$, $\beta_i$ and $\delta_i$ are given by

$$\alpha_i = 2b_i m_i / \left(2b_i m_i + \Omega_i\right)^{m_i} / 2b_i \tag{15a}$$

$$\beta_i = 1 / 2b_i \tag{15b}$$

$$\delta_i = \Omega_i / 2b_i \left(2b_i m_i + \Omega_i\right), \tag{15c}$$

with $c_i = \left(d_i - N_i\right)^+$, $\varepsilon_i = m_i N_i - d_i$, $d_i = \max\left\{N_i, \lfloor m_i N_i \rfloor\right\}$, where $\lfloor z \rfloor$ is the largest integer not greater than $z$, and $(z)^+$ indicates that if $z < 0$, then let $(z)^+ = 0$.

For simplicity, we suppose that the Nakagami channel parameter $m$ takes on integer values, i.e. $m_i \in \mathbb{N}$ [7]. Under this assumption, we adopt the following identity [32]

$$ {}_1F_1\left(a; a-n; z\right) = \frac{(-1)^n n!}{(1-a)_n} \exp(z) L_n^{a-n-1}(-z), \quad (16)$$

with $(x)_n = x(x+1)(x+n-1)$ representing the Pochhammer symbol and $L_n^{\alpha}(\cdot)$ the Laguerre polynomial, which can be represented as [31, eq. (8.970.1)]

$$L_n^{\alpha}(z) = \sum_{m=0}^{n} (-1)^m \binom{n+\alpha}{n-m} \frac{z^m}{m!}. \quad (17)$$

As such we can obtain the following expressions

$$\begin{aligned} {}_1F_1\left(d_i; d_i - l_i; -\frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}x\right) &= \frac{(-1)^{l_i} l_i!}{(1-d_i)_{l_i}} \sum_{k_i=0}^{l_i} \frac{(-1)^{k_i}}{k_i!} \\ &\times \binom{d_i-1}{l_i-k_i} \left(\frac{(\beta_i-\delta_i)x}{\bar{\gamma}_i}\right)^{k_i} e^{-\frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}x}, \end{aligned} \quad (18)$$

$$\begin{aligned} {}_1F_1\left(d_i+1; d_i - l_i+1; -\frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}x\right) &= \frac{(-1)^{l_i} l_i!}{(-d_i)_{l_i}} \sum_{k_i=0}^{l_i} \frac{(-1)^{k_i}}{k_i!} \\ &\times \binom{d_i}{l_i-k_i} \left(\frac{(\beta_i-\delta_i)x}{\bar{\gamma}_i}\right)^{k_i} e^{-\frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}x}. \end{aligned} \quad (19)$$

Hence, substituting (18) and (19) into (14), we have

$$\begin{aligned} f_{\gamma_i}(x) = \alpha_i^{N_i} \sum_{l_i=0}^{c_i} \binom{c_i}{l_i} \beta_i^{c_i-l_i} \left[\mathcal{P}_i\left(x, l_i, d_i, \bar{\gamma}_i\right)\right. \\ \left. +\varepsilon_i \delta_i \mathcal{P}\left(x, l_i, d_i+1, \bar{\gamma}_i\right)\right], \end{aligned} \quad (20)$$

where $\mathcal{P}_i\left(x, l_i, d_i, \bar{\gamma}_i\right)$ can be written as

$$\begin{aligned} \mathcal{P}_i\left(x, l_i, d_i, \bar{\gamma}_i\right) &= \frac{(-1)}{\Gamma\left(d_i-l_i\right)\left(1-d_i\right)_{l_i}} \sum_{k_i=0}^{l_i} \frac{(-1)^{l_i+k_i}}{k_i!} \\ &\times \binom{d_i-1}{l_i-k_i} \frac{\left(\beta_i-\delta_i\right)^{k_i}}{\bar{\gamma}_i^{k_i+d_i-l_i}} x^{k_i+d_i-l_i-1} e^{-\frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}x}. \end{aligned} \quad (21)$$

In addition, by using (20) along with [31, eq. (3.351.1)], the cumulative distribution function (CDF) of $\gamma_i = \bar{\gamma}_i \left\|h_i\right\|_F^2$ can be expressed as

$$\begin{aligned} F_{\gamma_i}(x) = \alpha_i^{N_i} \sum_{l_i=0}^{c_i} \binom{c_i}{l_i} \beta_i^{c_i-l_i} \left[\mathcal{Q}_i\left(x, l_i, d_i, \bar{\gamma}_i\right)\right. \\ \left. +\varepsilon_i \delta_i \mathcal{Q}_i\left(x, l_i, d_i+1, \bar{\gamma}_i\right)\right], \end{aligned} \quad (22)$$

where $\mathcal{Q}_i\left(x, l_i, d_i, \bar{\gamma}_i\right)$ is given by

$$\begin{aligned} \mathcal{Q}_i\left(x, l_i, d_i, \bar{\gamma}_i\right) &= \frac{l_i!\left(\beta_i-\delta_i\right)^{l_i-d_i}}{\Gamma\left(d_i-l_i\right)\left(1-d_i\right)_{l_i}} \sum_{k_i=0}^{l_i} \frac{(-1)^{l_i+k_i}}{k_i!} \\ &\times \binom{d_i-1}{l_i-k_i} \gamma\left(k_i+d_i-l_i, \frac{(\beta_i-\delta_i)}{\bar{\gamma}_i}\right), \end{aligned} \quad (23)$$

and where $\gamma(\cdot, \cdot)$ is the lower incomplete Gamma function [31, eq. (8.350.1)].

## IV. SECRECY PERFORMANCE ANALYSIS OF SCENARIO I

For Scenario I, since the CSI of the eavesdropper's channel is unavailable at Alice, and similar to [18] and [19], we adopt the probability of non-zero secrecy capacity, and the exact and asymptotic secrecy outage probability to evaluate the secrecy performance of the network.

$$\begin{aligned} \Pr\left(C_s>0\right) = \alpha_E^{N_E} \sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E-l_E} \alpha_B^{N_B} \sum_{l_B=0}^{c_B} \binom{c_B}{l_B} \beta_B^{c_B-l_B} \left[\mathcal{U}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)\right. \\ +\varepsilon_B \delta_B \mathcal{U}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) + \varepsilon_E \delta_E \mathcal{U}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right) \\ \left. +\varepsilon_B \delta_B \varepsilon_E \delta_E \mathcal{U}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right)\right]. \end{aligned} \quad (25)$$

$$\begin{aligned} \mathcal{U}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = \frac{\left(\beta_E-\delta_E\right)^{l_E-d_E} l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}} \sum_{k_E=0}^{l_E} \frac{(-1)^{l_E+k_E}}{k_E!} \binom{d_E-1}{l_E-k_E} \\ \times \frac{l_B!}{\Gamma\left(d_B-l_B\right)\left(1-d_B\right)_{l_B}} \sum_{k_B=0}^{l_B} \frac{(-1)^{l_B+k_B}}{k_B!} \binom{d_B-1}{l_B-k_B} \frac{\left(\beta_B-\delta_B\right)^{k_B}}{\bar{\gamma}_B^{k_B+d_B-l_B}} \\ \times \underbrace{\int_0^{\infty} x^{k_B+d_B-l_B-1} \gamma\left(k_E+d_E-l_E, \frac{\left(\beta_E-\delta_E\right)}{\bar{\gamma}_E} x\right) e^{-\frac{(\beta_B-\delta_B)}{\bar{\gamma}_B}x} dx}_{I_1}. \end{aligned} \quad (27)$$

### A. PROBABILITY OF NON-ZERO SECRECY CAPACITY

In wireless networks, channel quality may vary over time and frequency, a property that can be opportunistically exploited for improved transmission [18]. Therefore, we consider the probability of non-zero secrecy capacity, which can be given by

$$\begin{aligned}\Pr\left(C_s > 0\right) &= \Pr\left(\gamma_B > \gamma_E\right)\\ &= \int_0^\infty \int_0^x f_{\gamma_B}(x) f_{\gamma_E}(y)\, dydx\\ &= \int_0^\infty F_{\gamma_E}(x) f_{\gamma_B}(x)\, dx. \end{aligned} \tag{24}$$

By substituting (20) and (22) into (24), $\Pr\left(C_s > 0\right)$ can be computed as in (25), as shown at the bottom of the previous page, where $U\left(l_B, d_B, l_E, d_E\right)$ is given by

$$\begin{aligned}\mathcal{U}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = \int_0^\infty &\mathcal{Q}_E\left(x, l_E, d_E, \bar{\gamma}_E\right)\\ &\times \mathcal{P}_B\left(x, l_B, d_B, \bar{\gamma}_B\right) dx. \end{aligned} \tag{26}$$

Substituting (21) and (23) into (26), $\mathcal{U}\left(l_B, d_B, l_E, d_E\right)$ can be calculated as (27). To solve the integral $I_1$ as (27), as shown at the bottom of the previous page, we first employ [33, eq. (8.4.16.1)] to express the incomplete gamma function $\gamma\left(k_E + d_E - l_E, \frac{\left(\beta_E - \delta_E\right)}{\bar{\gamma}_E} x\right)$ as

$$\begin{aligned}&\gamma\left(k_E + d_E - l_E, \frac{\left(\beta_E - \delta_E\right)}{\bar{\gamma}_E} x\right)\\ &\quad = G_{1,2}^{1,1}\left[\frac{\left(\beta_E - \delta_E\right)}{\bar{\gamma}_E} x \,\middle|\, \begin{matrix} 1 \\ k_E + d_E - l_E + 1, 0 \end{matrix}\right], \end{aligned} \tag{28}$$

where $G_{p,q}^{m,n}\left[\cdot\,|\cdot\right]$ is the Meijer-G function of a single variable [31, eq. (9.301)]. Furthermore, substituting (28) into (27) and using [31, eq. (7.813.1)], we obtain

$$\begin{aligned}I_1 &= \left(\frac{\bar{\gamma}_B}{\beta_B - \delta_B}\right)^{k_B + d_B - l_B}\\ &\quad \times G_{2,2}^{1,2}\left[\frac{\left(\beta_E - \delta_E\right)\bar{\gamma}_B}{\left(\beta_B - \delta_B\right)\bar{\gamma}_E} \,\middle|\, \begin{matrix} -\left(k_B + d_B - l_B - 1\right), 1 \\ k_E + d_E - l_E + 1, 0 \end{matrix}\right], \end{aligned} \tag{29}$$

and further express (27) as (30), as shown at the bottom of this page. By substituting (30) into (25), the probability of non-zero secrecy capacity $\Pr\left(C_s > 0\right)$ can be directly calculated.

### B. SECRECY OUTAGE PROBABILITY

The secrecy outage probability can be defined as the probability that the secrecy capacity falls below a predefined rate $R_s$. Mathematically, it is given by [18]

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s\right). \tag{31}$$

Based on (13), we can further rewrite (31) as

$$\begin{aligned}P_{out}\left(R_s\right) = &\underbrace{\Pr\left(C_s < R_s \middle| \gamma_B > \gamma_E\right)\Pr\left(\gamma_B > \gamma_E\right)}_{I_3}\\ &+ \underbrace{\Pr\left(\gamma_B < \gamma_E\right)}_{I_4}, \end{aligned} \tag{32}$$

where $I_3$ and $I_4$ in (32) can be calculated as

$$I_3 = \int_0^\infty \int_y^{2^{R_s}(1+y)-1} f_{\gamma_B}(x) f_{\gamma_E}(y)\, dxdy \tag{33}$$

$$I_4 = \int_0^\infty \int_0^y f_{\gamma_B}(x) f_{\gamma_E}(y)\, dxdy. \tag{34}$$

Using (33) and (34) in (32) along with some algebraic manipulations, we have

$$\begin{aligned}P_{out}\left(R_s\right) &= \int_0^\infty \int_0^{2^{R_s}(1+y)-1} f_{\gamma_B}(x) f_{\gamma_E}(y) dxdy\\ &= \int_0^\infty F_{\gamma_B}\left(2^{R_s}(1+y) - 1\right) f_{\gamma_E}(y)\, dy. \end{aligned} \tag{35}$$

By substituting (20) and (22) into (35), $P_{out}\left(R_s\right)$ can be derived as in (36), as shown at the top of the next page, where $V\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)$ is given by (37), as shown at the top of the next page. To solve the integral $I_5$ in (37) which involves an incomplete gamma function with a shift parameter, we first apply [31, eq. (8.352.6)] to express the $\gamma\left(k_B + d_B - l_B, 2^{R_s}(1+y) - 1\right)$ as a finite series representation along with the binominal expression $(a+x)^n = \sum_{k=0}^{n}\binom{n}{k} x^k a^{n-k}$ [27, eq. (1.111)], we may write

$$\begin{aligned}I_5 = &\left(k_B + d_B - l_B - 1\right)!\\ &\times\left[1 - e^{-\frac{\left(\beta_B - \delta_B\right)\left(2^{R_s} - 1\right)}{\bar{\gamma}_B}} \times \sum_{\tau_B=0}^{k_B + d_B - l_B - 1} \frac{1}{\tau_B!}\left(\frac{\beta_B - \delta_B}{\bar{\gamma}_B}\right)^{\tau_B}\right.\\ &\left.\sum_{\zeta_B=0}^{\tau_B}\binom{\tau_B}{\zeta_B}\frac{2^{\zeta_B R_s}\bar{\gamma}_E^{\zeta_B}\left(\zeta_B + k_E + d_E - l_E - 1\right)!}{\left(2^{R_s} - 1\right)^{\zeta_B - \tau_B}\left(\beta_E - \delta_E\right)^{\zeta_B + d_E - l_E}}\right]. \end{aligned} \tag{38}$$

$$\begin{aligned}\mathcal{U}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = &\frac{(-1)^{l_E}\left(\beta_E - \delta_E\right)^{l_E - d_E} l_E!}{\Gamma\left(d_E - l_E\right)\left(1 - d_E\right)_{l_E}} \sum_{k_E=0}^{l_E}\frac{(-1)^{k_E}}{k_E!}\binom{d_E - 1}{l_E - k_E}\frac{(-1)^{l_B} l_B!}{\Gamma\left(d_B - l_B\right)\left(1 - d_B\right)_{l_B}}\\ &\times \sum_{k_B=0}^{l_B}\frac{(-1)^{k_B}}{k_B!\left(\beta_B - \delta_B\right)^{d_B - l_B}}\binom{d_B - 1}{l_B - k_B} G_{2,2}^{1,2}\left[\frac{\left(\beta_E - \delta_E\right)\bar{\gamma}_B}{\left(\beta_B - \delta_B\right)\bar{\gamma}_E} \,\middle|\, \begin{matrix} -\left(k_B + d_B - l_B - 1\right), 1 \\ k_E + d_E - l_E + 1, 0 \end{matrix}\right]. \end{aligned} \tag{30}$$

$$\begin{aligned}P_{out}\left(R_s\right) = \alpha_E^{N_E}\sum_{l_E=0}^{c_E}\binom{c_E}{l_E}\beta_E^{c_E-l_E}\alpha_B^{N_B}\sum_{l_B=0}^{c_B}\binom{c_B}{l_B}\beta_B^{c_B-l_B}\big[&\mathcal{V}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)\\ &+\varepsilon_B\delta_B\mathcal{V}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)+\varepsilon_E\delta_E\mathcal{V}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right)\\ &+\varepsilon_B\delta_B\varepsilon_E\delta_E\mathcal{V}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right)\big]. \end{aligned} \tag{36}$$

$$\begin{aligned}\mathcal{V}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = {}& \frac{l_B!\left(\beta_B-\delta_B\right)^{l_B-d_B}}{\Gamma\left(d_B-l_B\right)\left(1-d_B\right)_{l_B}}\sum_{k_B=0}^{l_B}\frac{(-1)^{l_B+k_B}}{k_B!}\binom{d_B-1}{l_B-k_B}\frac{l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}\\ &\times\sum_{k_E=0}^{l_E}\frac{(-1)^{l_E+k_E}}{k_E!}\binom{d_E-1}{l_E-k_E}\frac{\left(\beta_E-\delta_E\right)^{k_E}}{\bar{\gamma}_E^{k_E+d_E-l_E}}\underbrace{\int_0^\infty y^{k_E+d_E-l_E-1}e^{-\frac{\left(\beta_E-\delta_E\right)}{\bar{\gamma}_E}y}\gamma\left(k_B+d_B-l_B, 2^{R_s}\left(1+y\right)-1\right)dy}_{I_5}, \end{aligned} \tag{37}$$

$$\begin{aligned}\mathcal{V}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = {}& \frac{(-1)\, l_B!\left(\beta_B-\delta_B\right)^{l_B-d_B}}{\Gamma\left(d_B-l_B\right)\left(1-d_B\right)_{l_B}}\sum_{k_B=0}^{l_B}\frac{(-1)^{l_B+k_B}}{k_B!}\binom{d_B-1}{l_B-k_B}\frac{(-1)^{l_i}\, l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}\\ &\times\sum_{k_E=0}^{l_E}\frac{(-1)^{k_E}}{k_E!}\binom{d_E-1}{l_E-k_E}\left(k_B+d_B-l_B-1\right)!\Bigg[1-e^{-\frac{\left(\beta_B-\delta_B\right)\left(2^{R_s}-1\right)}{\bar{\gamma}_B}}\sum_{\tau_B=0}^{k_B+d_B-l_B-1}\frac{1}{\tau_B!}\\ &\times\left(\frac{\beta_B-\delta_B}{\bar{\gamma}_B}\right)^{\tau_B}\sum_{\zeta_B=0}^{\tau_B}\binom{\tau_B}{\zeta_B}\frac{2^{\zeta_B R_s}\bar{\gamma}_E^{\zeta_B}\left(\zeta_B+k_E+d_E-l_E-1\right)!}{\left(2^{R_s}-1\right)^{\zeta_B-\tau_B}\left(\beta_E-\delta_E\right)^{\zeta_B+d_E-l_E}}\Bigg]. \end{aligned} \tag{39}$$

In deriving (38), we have used [31, eq. (3.351.3)]. Then, by inserting (38) into (37), $\mathcal{V}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)$ can be obtained as in (34). Eventually, by substituting (39), as shown at the top of this page into (37) and performing some necessary manipulations, one can directly obtain a closed-form expression for $P_{out}\left(R_s\right)$.

### *C. ASYMPTOTIC SECRECY OUTAGE PROBABILITY*

Although an exact analytical expression for secrecy outage probability has been obtained, it is difficult to gain much insight from (36). Therefore, in what follows, we will derive the asymptotic secrecy outage probability at high SNR, where $P \to \infty$ (approaching Tx saturation). We take into account two realistic cases, i.e., *Outside Beam Coverage (OBC)*: Eve is located outside the beam coverage, which can be mathematically described as $\bar{\gamma}_B \to \infty$ for arbitrary small $\bar{\gamma}_E$ since Eve is relatively far away from the legitimate user [19], and *Inside Beam Coverage (IBC)*: Eve is located within the beam coverage, which can be view as $\bar{\gamma}_B \to \infty$ and $\bar{\gamma}_E \to \infty$ since Eve is close to the legitimate user [19]. For both cases, we can reveal two important performance metrics, namely the secrecy diversity order and the secrecy array gain of the network.

#### 1) OUTSIDE BEAM COVERAGE (OBC): $\bar{\gamma}_B \to \infty$

When the Eve is located far away from the legitimate user, the secrecy outage probability can be obtained in the following theorem.

*Theorem 1: The asymptotic secrecy outage probability for case a) at high SNR can be expressed as*

$$P_{out}^{\infty}\left(R_s\right) = \Xi\bar{\gamma}_B^{-N_B}, \tag{40}$$

*where*

$$\begin{aligned}\Xi = {}& \frac{\alpha_B^{N_B}\left(-1\right)^{c_B}c_B!}{\Gamma\left(N_B+1\right)\left(1-d_B\right)_{c_B}}\binom{d_B-1}{c_B}\\ &\times\alpha_E^{N_E}\sum_{l_E=0}^{c_E}\binom{c_E}{l_E}\beta_E^{c_E-l_E}\left[\mathcal{W}\left(l_B, d_B, l_E, d_E, \bar{\gamma}_E\right)\right.\\ &\left.+\varepsilon_E\delta_E\mathcal{W}\left(l_B, d_B, l_E, d_E+1, \bar{\gamma}_E\right)\right]. \end{aligned} \tag{41}$$

*with*

$$\begin{aligned}&\mathcal{W}\left(l_B, d_B, l_E, d_E, \bar{\gamma}_E\right)\\ &\quad= \frac{l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}\\ &\qquad\times\sum_{k_E=0}^{l_E}\frac{(-1)^{l_E+k_E}}{k_E!}\binom{d_E-1}{l_E-k_E}\sum_{\varphi=0}^{N_B}\binom{N_B}{\varphi}\\ &\qquad\times\frac{2^{\varphi R_s}\bar{\gamma}_E^{\varphi}\left(\varphi+k_E+d_E-l_E-1\right)!}{\left(2^{R_s}-1\right)^{\varphi-N_B}\left(\beta_E-\delta_E\right)^{\varphi+d_E-l_E}}. \end{aligned} \tag{42}$$

*Proof:* See Appendix A. ■

According to [18] and [19], we can express the asymptotic secrecy outage probability in terms of the secrecy diversity order $G_d$ and the secrecy array gain $G_a$, namely

$$P_{out}^{\infty}\left(R_s\right) = \left(G_c\bar{\gamma}_B\right)^{-G_d}. \tag{43}$$

$$\bar{C}_s = \alpha_E^{N_E} \sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E-l_E} \alpha_B^{N_B} \sum_{l_B=0}^{c_B} \binom{c_B}{l_B} \beta_B^{c_B-l_B} \left[\mathcal{X}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)\right.$$
$$+\varepsilon_B\delta_B\mathcal{X}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) + \varepsilon_E\delta_E\mathcal{X}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right)$$
$$\left.+\varepsilon_B\delta_B\varepsilon_E\delta_E\mathcal{X}\left(l_B, d_B+1, \bar{\gamma}_B, l_E, d_E+1, \bar{\gamma}_E\right)\right]. \tag{51}$$

$$\mathcal{X}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right) = \frac{\left(\beta_E-\delta_E\right)^{l_E-d_E} l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}} \sum_{k_E=0}^{l_E} \frac{(-1)^{l_E+k_E}}{k_E!} \binom{d_E-1}{l_E-k_E} \frac{l_B!}{\Gamma\left(d_B-l_B\right)\left(1-d_B\right)_{l_B}} \sum_{k_B=0}^{l_B} \frac{(-1)^{l_B+k_B}}{k_B!}$$
$$\times \binom{d_B-1}{l_B-k_B} \sum_{\tau_B=0}^{k_B+d_B-l_B-1} \frac{\Gamma\left(k_B+d_B-l_B\right)}{\tau_B!(\beta_B-\delta_B)^{d_B-l_B-\tau_B}\bar{\gamma}_B^{\tau_B}} \underbrace{\int_0^\infty \frac{y^{\tau_B}}{1+y}\gamma\left(k_E+d_E-l_E, \frac{\left(\beta_E-\delta_E\right)}{\bar{\gamma}_E}y\right) e^{-\frac{\left(\beta_B-\delta_E\right)}{\bar{\gamma}_E}y} dy}_{I_6}. \tag{52}$$

Based on (43), the achievable secrecy diversity order and secrecy array gain can be directly obtained as

$$G_d = N_B, \quad and \quad G_a = \Xi^{-\frac{1}{N_B}}. \tag{44}$$

*Remark 1: It can be seen that the achievable secrecy diversity order $G_d$ of the considered network is only determined by the number of antennas $N_B$ at Bob. However, while the number of antennas $N_E$ at Eve, and the channel parameters of both Bob and Eve, $\left(\Omega_B, b_B, m_B\right)$ and $\left(\Omega_E, b_E, m_E\right)$ do not affect the secrecy diversity order, they have an impact on the secrecy array gain of the LMS system.*

### 2) IBC: $\bar{\gamma}_B \to \infty$ AND $\bar{\gamma}_E \to \infty$

In this case, the Eve is located close to the legitimate user. Based on (43) and by applying the fact $\bar{\gamma}_B/\bar{\gamma}_E = b\left(\varphi_B\right)/b\left(\varphi_E\right)$, the asymptotic secrecy outage probability for the *IBC* case is derived as

$$P_{out}^{\infty}\left(R_s\right) = \lim_{\bar{\gamma}_E\to\infty} P_{out,a}^{\infty}\left(R_s\right) = \Theta\left(\frac{b\left(\varphi_B\right)}{b\left(\varphi_E\right)}\right)^{-N_B}, \tag{45}$$

where

$$\Theta = \frac{\alpha_B^{N_B}(-1)^{c_B} c_B!}{\Gamma\left(N_B+1\right)\left(1-d_B\right)_{c_B}} \binom{d_B-1}{c_B}$$
$$\times\alpha_E^{N_E} \sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E-l_E} \left[J\left(l_B, d_B, l_E, d_E\right)\right.$$
$$\left.+\varepsilon_E\delta_E J\left(l_B, d_B, l_E, d_E+1\right)\right], \tag{46}$$

with

$$J\left(l_B, d_B, l_E, d_E\right) = \frac{l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}$$
$$\times\sum_{k_E=0}^{l_E} \frac{(-1)^{l_E+k_E}}{k_E!} \binom{d_E-1}{l_E-k_E}$$
$$\times\frac{2^{N_B R_s}\left(N_B+k_E+d_E-l_E-1\right)!}{\left(\beta_E-\delta_E\right)^{N_B+d_E-l_E}}. \tag{47}$$

*Remark 2: As can be observed from (45), the achievable secrecy diversity order $G_d$ for the IBC case approaches a constant in the high SNR regime, implying that the secrecy diversity is zero. The SNR ratio between Bob and Eve is only determined by the beam gains $b\left(\varphi_B\right)$ and $b\left(\varphi_E\right)$, which indicates that increasing the satellite transmit power cannot enhance the secrecy performance.*

## V. SECRECY PERFORMANCE ANALYSIS OF SCENARIO II

This section focuses on the scenario where the CSI of Eve is available at Alice. In this case, we employ the exact and asymptotic average secrecy capacity as the principle secrecy performance metric [16], [19].

### A. AVERAGE SECRECY CAPACITY

Based on the definition of the achievable average secrecy capacity, we have

$$\bar{C}_s = \mathrm{E}\left[C_s\right] = \int_0^\infty \int_0^\infty C_s f_{\gamma_B,\gamma_E}(x, y) dx dy \tag{48}$$

where $f_{\gamma_B,\gamma_E}(x, y)$ is the joint PDF of $\gamma_B$ and $\gamma_E$. Due to the independence of the main and eavesdropper's channels, using (13) in (48) yields

$$\bar{C}_s = \int_0^\infty \int_y^\infty \left[\log_2(1+x) - \log_2(1+y)\right]$$
$$\times f_{\gamma_E}(y) f_{\gamma_B}(x)\, dy dx. \tag{49}$$

Employing integration by parts along with some other algebraic manipulations, (49) can be rewritten as

$$\bar{C}_s = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(y)}{1+y}\left[\int_y^\infty f_{\gamma_B}(x)\, dx\right] dy. \tag{50}$$

Then, by substituting (20) and (22) into (50), $\bar{C}_s$ can be evaluated as in (51), as shown at the top of this page, where $\mathcal{X}\left(l_B, d_B, \bar{\gamma}_B, l_E, d_E, \bar{\gamma}_E\right)$ can be calculated as in (52), as shown at the top of this page. In order to compute the integral $I_6$ in (45), we first exploit (20) and the equality [34, eq.(10)]

$$(1+\alpha x)^{-\beta} = \frac{1}{\Gamma(\beta)} G_{1,1}^{1,1}\left[\alpha x \,\middle|\, \begin{matrix} 1-\beta \\ 0 \end{matrix}\right]. \tag{53}$$

$$\mathcal{X}\left(l_B,d_B,\bar{\gamma}_B,l_E,d_E,\bar{\gamma}_E\right)=\frac{\left(\beta_E-\delta_E\right)^{l_E-d_E}l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}\sum_{k_E=0}^{l_E}\frac{(-1)^{l_E+k_E}}{k_E!}\binom{d_E-1}{l_E-k_E}\frac{l_B!}{\Gamma\left(d_B-l_B\right)\left(1-d_B\right)_{l_B}}\sum_{k_B=0}^{l_B}\frac{(-1)^{l_B+k_B}}{k_B!}$$
$$\times\binom{d_B-1}{l_B-k_B}\sum_{\tau_B=0}^{k_B+d_B-l_B-1}\frac{\Gamma\left(k_B+d_B-l_B\right)\bar{\gamma}_B}{\tau_B!(\beta_B-\delta_B)^{d_B-l_B+1}}G^{1,1,1,1,1}_{1,[1:1],0,[2:1]}\left[\begin{array}{c|c}\frac{(\beta_E-\delta_E)\bar{\gamma}_B}{(\beta_B-\delta_B)\bar{\gamma}_E} & \tau_B+1\\ & 1;0\\ \frac{\bar{\gamma}_B}{\beta_B-\delta_B} & --\\ & k_E+d_E-l_E+1,0;0\end{array}\right]. \quad (55)$$

Then, with the aid of [35, eq. (3.1)], we obtain $I_6$ as

$$I_6=\left(\frac{\bar{\gamma}_B}{\beta_B-\delta_B}\right)^{\tau_B+1}$$
$$\times G^{1,1,1,1,1}_{1,[1:1],0,[2:1]}\left[\begin{array}{c|c}\frac{(\beta_E-\delta_E)\bar{\gamma}_B}{(\beta_B-\delta_B)\bar{\gamma}_E} & \tau_B+1\\ & 1;0\\ \frac{\bar{\gamma}_B}{\beta_B-\delta_B} & --\\ & k_E+d_E-l_E+1,0;0\end{array}\right], \quad (54)$$

where $G^{1,1,1,1,1}_{1,[1:1],0,[2:1]}[\cdot|\cdot]$ denotes the Meijer-G function of two variables [35]. Subsequently, by substituting (54) into (52), $\mathcal{X}\left(l_B,d_B,\bar{\gamma}_B,l_E,d_E,\bar{\gamma}_E\right)$ can be expressed as in (55), as shown at the top of this page. Finally, by substituting (55) into (51) and performing some algebraic manipulations, $C_s$ can be directly evaluated.

### B. ASYMPTOTIC AVERAGE SECRECY CAPACITY AT HIGH SNR

To investigate the impact of key system parameters, such as the number of antennas at Bob and Eve and the channel parameters of $h_B$ and $h_E$ on the average secrecy capacity, we focus on the asymptotic secrecy capacity of the system at high SNR in the following cases.

#### 1) OBC: $\bar{\gamma}_B\rightarrow\infty$

Before delving into the detailed analysis, applying the identity [31, eq. (3.351.2)], we first rewrite the CDF of $\gamma_E$ as

$$F_{\gamma_E}(x)=1-\Phi_{\gamma_E}(x) \quad (56)$$

where

$$\Phi_{\gamma_E}(x)=\alpha_E^{N_E}\sum_{l_E=0}^{c_E}\binom{c_E}{l_E}\beta_E^{c_E-l_E}$$
$$\times\left[\mathcal{R}_E\left(x,l_E,d_E,\bar{\gamma}_E\right)+\varepsilon_E\delta_E\mathcal{R}_E\left(x,l_E,d_E+1,\bar{\gamma}_E\right)\right] \quad (57)$$

and $\left[\mathcal{R}_E\left(x,l_E,d_E,\bar{\gamma}_E\right)\right.$ is given by

$$\mathcal{R}_E\left(x,l_E,d_E,\bar{\gamma}_E\right)$$
$$=\frac{l_E!}{\Gamma\left(d_E-l_E\right)\left(1-d_E\right)_{l_E}}$$
$$\times\sum_{k_E=0}^{l_E}\frac{(-1)^{l_E+k_E}}{k_E!}\binom{d_E-1}{l_E-k_E}$$
$$\times\sum_{\tau_E=0}^{k_E+d_E-l_E-1}\frac{\Gamma\left(k_E+d_E-l_E\right)}{\tau_E!(\beta_E-\delta_E)^{d_E-l_E-\tau_E}\bar{\gamma}_E^{\tau_E}}x^{\tau_E}e^{-\frac{(\beta_E-\delta_E)}{\bar{\gamma}_E}x}. \quad (58)$$

Then, using (56) in (50) and changing the order of integration, we further have

$$\bar{C}_s^{\infty}=\frac{1}{\ln 2}\int_0^{\infty}\left[\int_0^{x}\frac{1-\Phi_{\gamma_E}(y)}{1+y}dy\right]f_{\gamma_B}(x)\,dx=\Lambda_1-\Lambda_2 \quad (59)$$

where $\Lambda_1$ and $\Lambda_2$ can be written as

$$\Lambda_1=\frac{1}{\ln 2}\int_0^{\infty}\ln(1+x)f_{\gamma_B}(x)\,dx \quad (60)$$
$$\Lambda_2=\frac{1}{\ln 2}\int_0^{\infty}\int_0^{x}\frac{\Delta_{\gamma_E}(y)}{1+y}f_{\gamma_B}(x)\,dydx. \quad (61)$$

Next, we will derive $\Lambda_i(i=1,2)$ in the high SNR regime. When $x\rightarrow\infty$, we have $\ln(1+x)\approx\ln x$. By substituting (58) into (60), and applying [31, eq. (4.352.1)], one can obtain

$$\Lambda_1^{\infty}=\alpha_B^{N_B}\sum_{l_B=0}^{c_B}\binom{c_B}{l_B}\beta_B^{c_B-l_B}\left[\mathcal{G}_B\left(l_B,d_B,\bar{\gamma}_B\right)\right.$$
$$\left.+\varepsilon_B\delta_B\mathcal{G}_B\left(l_B,d_B+1,\bar{\gamma}_B\right)\right]+\log_2\bar{\gamma}_B, \quad (62)$$

where $\mathcal{G}_B\left(l_B,d_B,\bar{\gamma}_B\right)$ is given by

$$\mathcal{G}_B\left(l_B,d_B+1,\bar{\gamma}_B\right)$$
$$=\frac{(-1)_B^{l_B}l_B!}{\Gamma\left(d_B-l_B+1\right)\left(-d_B\right)_{l_B}}$$
$$\times\sum_{k_B=0}^{l_B}\frac{(-1)^{k_B}}{k_B!}\binom{d_B}{l_B-k_B}\frac{\Gamma\left(k_B+d_B-l_B+1\right)}{\left(\beta_B-\delta_B\right)^{d_B-l_B+1}}$$
$$\times\left[\psi\left(k_B+d_B-l_B+1\right)-\ln\left(\beta_B-\delta_B\right)\right], \quad (63)$$

and $\psi(\cdot)$ is the digamma function [31]. Resorting to [18], the asymptotic expression for $\Lambda_2^{\infty}$ can be calculated as

$$\Lambda_2^{\infty}=\frac{1}{\ln 2}\int_0^{\infty}\frac{\Phi_{\gamma_E}(x)}{1+x}dx. \quad (64)$$

Hence, combining (57) and (64) along with [36, eq. (2.3.6.9)], we obtain

$$\Lambda_2^{\infty}=\alpha_E^{N_E}\sum_{l_E=0}^{c_E}\binom{c_E}{l_E}\beta_E^{c_E-l_E}\left[\mathcal{T}_E\left(l_E,d_E,\bar{\gamma}_E\right)\right.$$
$$\left.+\varepsilon_E\delta_E\mathcal{T}_E\left(l_E,d_E+1,\bar{\gamma}_E\right)\right], \quad (65)$$

$$C_s^{\infty} = \alpha_B^{N_B} \sum_{l_B=0}^{c_B} \binom{c_B}{l_B} \beta_B^{c_B - l_B} \left[\mathcal{G}_B\left(l_B, d_B, \bar{\gamma}_B\right) + \varepsilon_B \delta_B \mathcal{G}_B\left(l_B, d_B + 1, \bar{\gamma}_B\right)\right] + \log_2 \bar{\gamma}_B - \alpha_E^{N_E} \sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E - l_E} \left[\mathcal{T}_E\left(l_E, d_E, \bar{\gamma}_E\right) + \varepsilon_E \delta_E \mathcal{T}_E\left(x, l_E, d_E + 1, \bar{\gamma}_E\right)\right]. \quad (67)$$

where

$$\begin{aligned}\mathcal{T}_E&\left(l_E, d_E, \bar{\gamma}_E\right) \\ &= \frac{(-1)^{l_E} l_E!}{\Gamma\left(d_E - l_E\right)\left(1 - d_E\right)_{l_E}} \sum_{k_E=0}^{l_E} \frac{(-1)^{k_E}}{k_E!} \\ &\quad \times \binom{d_E - 1}{l_E - k_E} \sum_{\tau_E=0}^{k_E + d_E - l_E - 1} \frac{\Gamma\left(k_E + d_E - l_E\right)}{\tau_E!(\beta_E - \delta_E)^{d_E - l_E - \tau_E} \bar{\gamma}_E^{\tau_E}} \\ &\quad \times \Gamma\left(\tau_E + 1\right) U\left(\tau_E + 1, \tau_E + 1; \frac{\left(\beta_E - \delta_E\right)}{\bar{\gamma}_E}\right). \quad (66)\end{aligned}$$

with $U(\cdot, \cdot; \cdot)$ being the confluent hypergeometric function [31]. Eventually, by using (62) and (65) in (59), the asymptotic average secrecy capacity of the system for the *OBC* case can be evaluated as in (67), as shown at the top of this page.

To gain insight on the average secrecy capacity at high SNR, the slope and power offset at the high SNR are also needed to be analyzed. To facilitate the asymptotic analysis, we adopt the general form in [37] to express $C_s^{\infty}$ as

$$C_s^{\infty} = S_{\infty}\left(\log_2 \bar{\gamma}_B - \mathcal{L}_{\infty}\right), \quad (68)$$

where $S_{\infty}$ denotes the high SNR slope in bit/s/Hz (3dB) and $\mathcal{L}_{\infty}$ the high SNR power offset in 3dB units.

According to [38], by substituting (67) into (68) along with algebraic manipulations, the high SNR slope is given by

$$S_{\infty} = \lim_{\bar{\gamma}_B \to \infty} \frac{C_s^{\infty}}{\log_2 \bar{\gamma}_B} = 1 \quad (69)$$

Furthermore, the high SNR power offset can be expressed as

$$\mathcal{L}_{\infty} = \lim_{\bar{\gamma}_B \to \infty} \left(\log_2 \bar{\gamma}_B - \frac{C_s^{\infty}}{S_{\infty}}\right). \quad (70)$$

Hence, substituting (68) and (69) into (70), we have

$$\mathcal{L}_{\infty} = \mathcal{L}_{\infty}^B + \mathcal{L}_{\infty}^E, \quad (71)$$

where the first term $\mathcal{L}_{\infty}^B$, which shows the effect of the Sat-Bob channel parameters on the average secrecy capacity, is given by

$$\begin{aligned}\mathcal{L}_{\infty}^B = -\alpha_B^{N_B} &\sum_{l_B=0}^{c_B} \binom{c_B}{l_B} \beta_B^{c_B - l_B} \\ &\times \left[\mathcal{G}_B\left(l_B, d_B, \bar{\gamma}_B\right) + \varepsilon_B \delta_B \mathcal{G}_B\left(l_B, d_B + 1, \bar{\gamma}_B\right)\right], \quad (72)\end{aligned}$$

and the second term $\mathcal{L}_{\infty}^E$, which characterizes the impact of the eavesdropping link on the average secrecy capacity, can be expressed as

$$\begin{aligned}\mathcal{L}_{\infty}^E = \alpha_E^{N_E} &\sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E - l_E} \left[\mathcal{T}_E\left(l_E, d_E, \bar{\gamma}_E\right)\right. \\ &\left. + \varepsilon_E \delta_E \mathcal{T}_E\left(l_E, d_E + 1, \bar{\gamma}_E\right)\right]. \quad (73)\end{aligned}$$

*Remark 3: As can be seen from (69) that the slop always equals to one at the high SNR, which means system parameters, such as* $N_B$*,* $N_E$*,* $\left(\Omega_B, b_B, m_B\right)$ *and* $\left(\Omega_E, b_E, m_E\right)$ *have no impact on* $S_{\infty}$*. Morever, the effects of the main channel parameters and eavesdropper link condition on the average secrecy capacity can be characterized with the aid of the high SNR power offset component* $\mathcal{L}_{\infty}^B$ *given in (72) and* $\mathcal{L}_{\infty}^E$ *in (73), respectively.*

### 2) IBC: $\bar{\gamma}_B \to \infty$ AND $\bar{\gamma}_E \to \infty$

In this case, we first need to further provide the asymptotic $\Lambda_2^{\infty}$ with $\bar{\gamma}_E \to \infty$.

$$\begin{aligned}\tilde{\Lambda}_2^{\infty} = \lim_{\bar{\gamma}_E \to \infty} \Lambda_2^{\infty} = \log_2 \bar{\gamma}_E + \alpha_E^{N_E} &\sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \beta_E^{c_E - l_E} \\ &\times \left[\mathcal{I}_E\left(l_E, d_E\right) + \varepsilon_E \delta_E \mathcal{I}_E\left(l_E, d_E + 1\right)\right], \quad (74)\end{aligned}$$

where

$$\begin{aligned}\mathcal{I}_E&\left(l_E, d_E + 1\right) \\ &= \frac{(-1)_E^{l_E} l_E!}{\Gamma\left(d_E - l_E + 1\right)\left(-d_E\right)_{l_E}} \\ &\quad \times \sum_{k_E=0}^{l_E} \frac{(-1)^{k_E}}{k_E!} \binom{d_E}{l_E - k_E} \frac{\Gamma\left(k_E + d_E - l_E + 1\right)}{\left(\beta_E - \delta_E\right)^{d_E - l_E + 1}} \\ &\quad \times \left[\psi\left(k_E + d_E - l_E + 1\right) - \ln\left(\beta_E - \delta_E\right)\right], \quad (75)\end{aligned}$$

Then, by combining (71) and (74), the asymptotic average secrecy capacity for case b) can be computed as

$$\begin{aligned}C_s^{\infty} = \log_2&\left(\frac{b\left(\varphi_B\right)}{b\left(\varphi_E\right)}\right) + \alpha_B^{N_B} \sum_{l_B=0}^{c_B} \binom{c_B}{l_B} \beta_B^{c_B - l_B} \\ &\times \left[\mathcal{G}_B\left(l_B, d_B\right) + \varepsilon_B \delta_B \mathcal{G}_B\left(l_B, d_B + 1\right)\right] - \alpha_E^{N_E} \sum_{l_E=0}^{c_E} \binom{c_E}{l_E} \\ &\times \beta_E^{c_E - l_E} \left[\mathcal{I}_E\left(l_E, d_E\right) + \varepsilon_E \delta_E \mathcal{I}_E\left(l_E, d_E + 1\right)\right]. \quad (76)\end{aligned}$$

*Remark 4: Based on (76), it can be found that the high SNR slope equals zero. This observation is consistent with (45) that the achievable average secrecy capacity cannot be enhanced by increasing the satellite transmit power when Eve is located close to the legitimate user.*

## VI. NUMERICAL RESULTS

In this section, we provide numerical simulations to examine the validity of the performance analysis and the impact of various system parameters on the network. Here, the predefined rate is chosen as $R_s = 1$, the simulation results are obtained by performing $10^6$ channel realizations, and the different shadowing severities of the main and eavesdropper's channels $h_i \sim \text{SR}\left(\Omega_i, b_i, m_i\right)$ $(i \in \{B, E\})$ are given in Table I. Without loss of generality, we assume the legitimate receiver is located at the center of the central beam, namely, $d_B = 0$ (maximum beam gain direction) [2], [21].

**TABLE 1.** LMS channel parameters [27], [30]

| Shadowing | $b_i$ | $m_i$ | $\Omega_i$ |
|---|---|---|---|
| Frequent Heavy Shadowing (FHS) | 0.063 | 2 | $8.97 \times 10^{-4}$ |
| Infrequent Light Shadowing (ILS) | 0.875 | 10 | 1.29 |

### A. IMPACT OF BEAM RADIUS AND EVE'S POSITION

To begin with, we investigate the impact of different beam radii $R$ and eavesdropper positions $d_E$ on the secrecy performance of the LMS network. Fig. 2 and Fig. 3 depict, respectively, the secrecy outage probability and average secrecy capacity of the satellite network for different $R$ and $d_E$. First of all, it is observed that the theoretical results are in excellent agreement with the Monte Carlo simulations, implying the validity of the secrecy performance analysis. Next, as we see from Fig. 2, for fixed $d_E$, the secrecy outage probability is reduced with the decrease of beam radius $R$. Specifically, when Eve's position is outside the beam coverage, the secrecy outage probability of the LMS system gradually fluctuates within a certain range around $10^{-3}$ and $10^{-6}$. This means that the narrower the beam pattern of the satellite antenna feed, the better secrecy performance is obtained. Finally, as shown in Fig. 3, when $R$ is fixed, the average secrecy capacity rapidly improves with the increase of $d_E$, and gradually remains stable between 6 and 7.

### B. IMPACT OF KEY SYSTEM PARAMETERS

In what follows, we focus on the impact of various key system parameters, including the number of antennas at the legitimate user and eavesdropper, and the channel shadowing severities on the secrecy performance of the satellite network.

#### 1) OBC

When Eve is located away from the legitimate user, the received average SNR at Eve is relatively small and can be viewed as a constant for the convenience of analysis. First of all, assuming both the Sat-Bob and Sat-Eve channels are subject to the AS scenario, Fig. 4 depicts the probability of non-zero secrecy capacity versus $\bar{\gamma}_B$ for different values of Eve's average SNR $\bar{\gamma}_E$. As shown in the figure, the theoretical results are in excellent agreement with the Monte Carlo simulations, which validates the accuracy of the derivations. In addition, the probability of non-zero secrecy capacity degrades significantly with an increase in Eve's average SNR $\bar{\gamma}_E$, which indicates the negative effect of the received power at the eavesdropper.

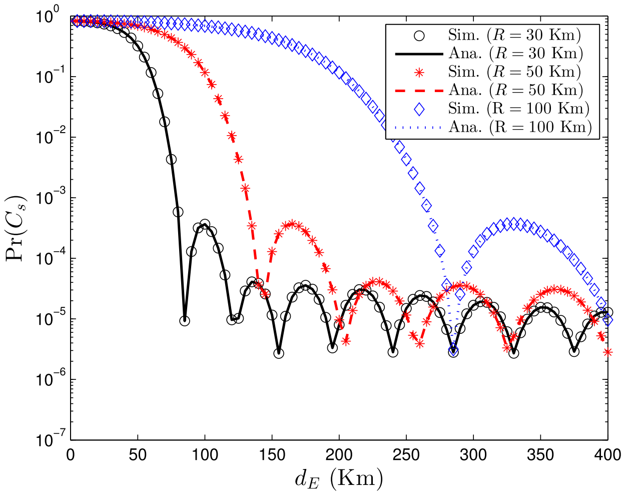

**FIGURE 2.** Secrecy outage probability with respective to different $R$ and $d_E$ ($N_B = N_E = 2$, $h_B$ and $h_E$: ILS scenario, $P/\sigma^2 = 20$ dB).

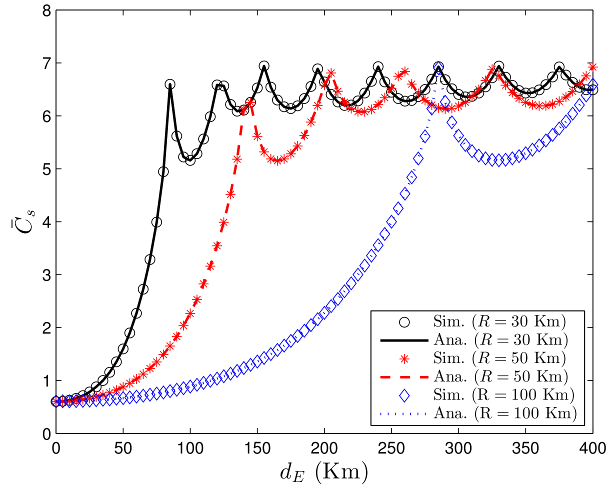

**FIGURE 3.** Average Secrecy Capacity with respective to different $R$ and $d_E$ ($N_B = N_E = 2$, $h_B$ and $h_E$: ILS scenario, $P/\sigma^2 = 20$ dB).

Fig. 5 investigates the effect of the number of antennas at Bob and Eve on the secrecy outage probability of the system, where both the Sat-Bob and Sat-Eve links follow the AS scenario. All of the analytical curves of secrecy outage probability agree well with simulation results, and the asymptotic results are very tight in the high SNR regime, implying the validity of the derived expressions. We also see that $N_B$ has a significant positive impact on the secrecy

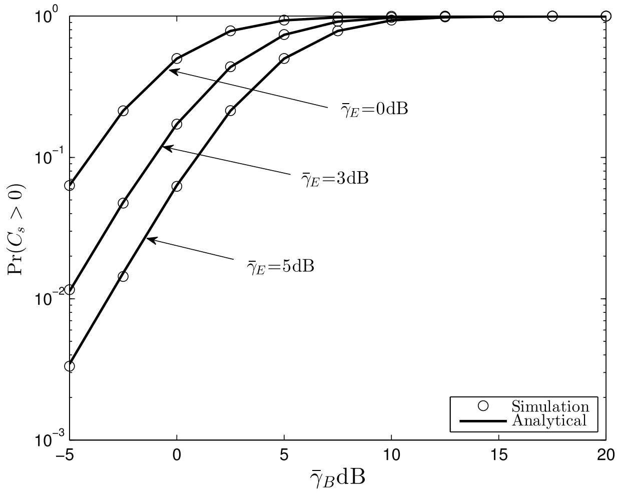

**FIGURE 4.** The probability of the non-zero secrecy capacity versus $\bar{\gamma}_B$ with different $\bar{\gamma}_E$ ($h_B$ and $h_E$: ILS scenario).

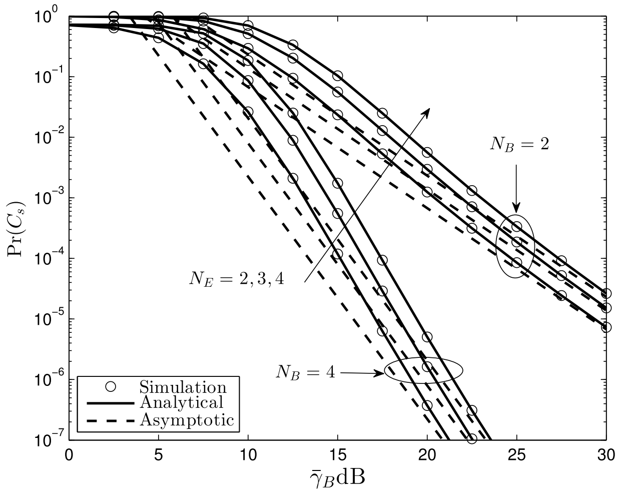

**FIGURE 5.** Secrecy outage probability versus $\bar{\gamma}_B$ for different antenna configurations ($h_B$ and $h_E$: ILS scenario, $\bar{\gamma}_E = 5$dB).

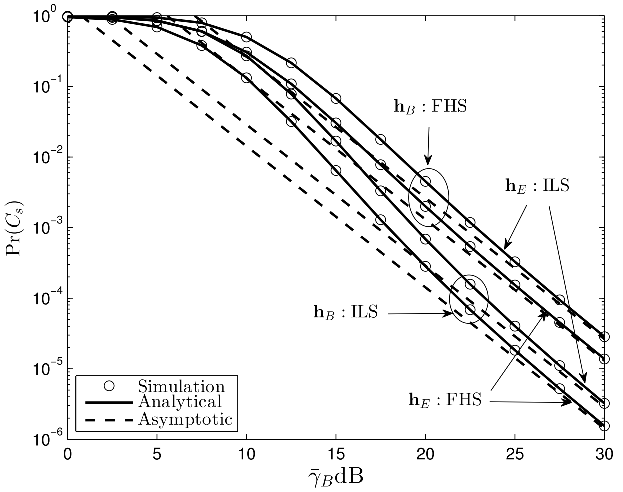

**FIGURE 6.** Secrecy outage probability versus $\bar{\gamma}_B$ for different shadowing severities ($N_B = N_E = 2$, $\bar{\gamma}_E = 5$dB).

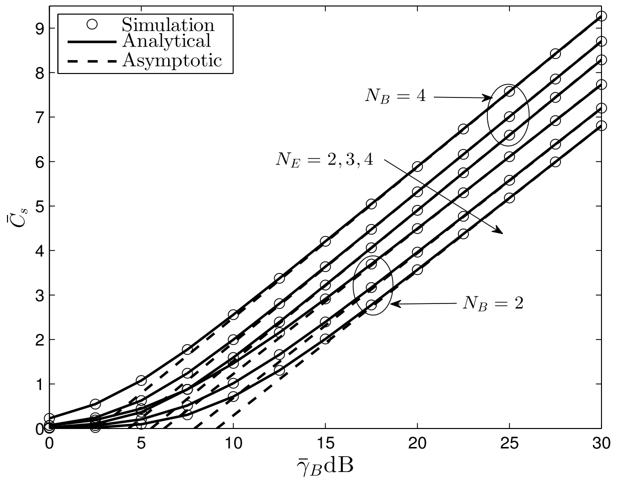

**FIGURE 7.** Average secrecy capacity versus $\bar{\gamma}_B$ for different antenna configurations ($h_B$ and $h_E$: ILS scenario, $\bar{\gamma}_E = 5$dB).

performance, justifying the benefits of employing multiple antennas in enhancing the secrecy of LMS systems. Moreover, it can be observed that the secrecy diversity order of the system only depends on the number of antennas at Bob, which corroborates the observation in Remark I. Meanwhile, although an increase in $N_E$ does not influence the achievable secrecy diversity order, it does degrade the system secrecy performance by reducing the secrecy array gain.

Fig. 6 illustrates the secrecy outage probability versus $\bar{\gamma}_B$ for different levels of shadowing of the Sat-Bob and Sat-Eve channels, respectively. It can be seen that the shadowing severities of both Bob and Eve do not influence the achievable secrecy diversity order of the system. However, weaker shadowing for the main channel results in a reduced secrecy outage probability by improving the secrecy array gain. On the other hand, the secrecy performance will be severely degraded by a weaker shadowing on the eavesdropper channel due to the reduction of secrecy array gain. Note that the secrecy performance of the LMS network improves as the shadowing becomes less severe for both receivers. This occurs due to the fact that, as the LOS component becomes stronger, the random variation in the channel is reduced, and hence the probability that Eve's channel will be better than Bob's will also be correspondingly reduced, especially if Bob's channel is already on average stronger than Eve's.

In Figs. 7 and 8, the average security capacity of the proposed system with various antenna configurations and shadowing severity are illustrated, respectively. As shown in these figures, at the high SNR, the slope of $S_\infty$ is always being one in all cases, which matches well with the formula given in (69). It can be observed from Fig. 7 that the average secrecy capacity improves when either the $N_B$ increases or the $N_E$ decreases. This is because a larger $N_B$ can reduce $\mathcal{L}_\infty^B$ given in (72) and further decrease the high SNR power offset, While a lower $N_B$ can directly lead to a larger SNR power offset $\mathcal{L}_\infty^E$. It can also be seen from Fig. 8 that due to the a

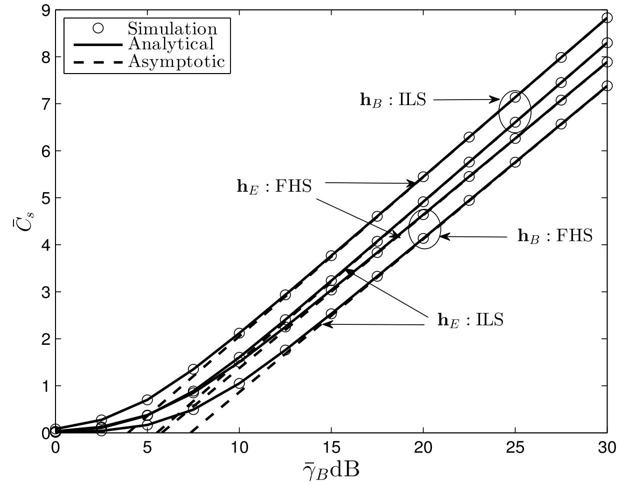

**FIGURE 8.** Average secrecy capacity versus $\bar{\gamma}_B$ for different shadowing severities ($N_B = N_E = 2$ and $\bar{\gamma}_E = 5$dB).

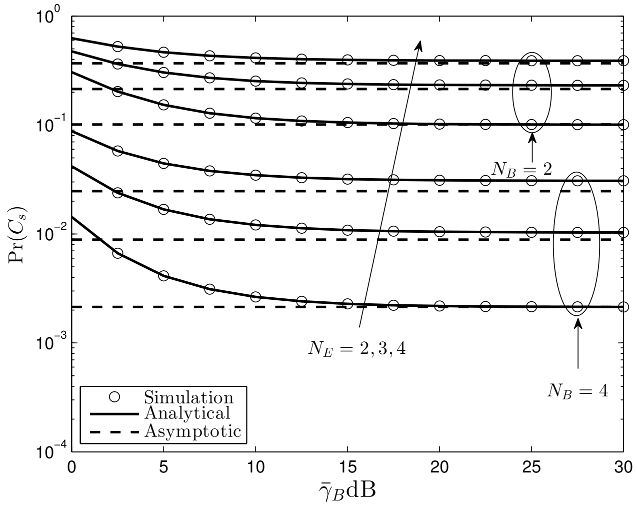

**FIGURE 9.** Secrecy outage probability for different antenna configurations ($h_B$ and $h_E$: ILS scenario, $R = 100$ Km, $d_E = 80$ Km).

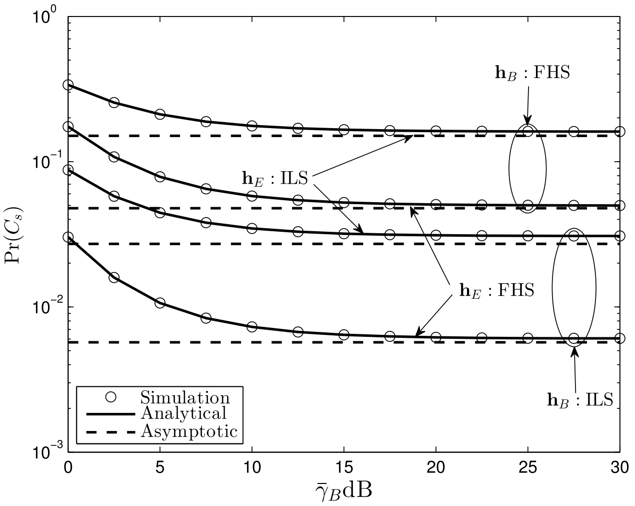

**FIGURE 10.** Secrecy outage probability for different shadowing severities ($N_B = N_E = 4$, $R = 100$ Km and $d_E = 80$ Km).

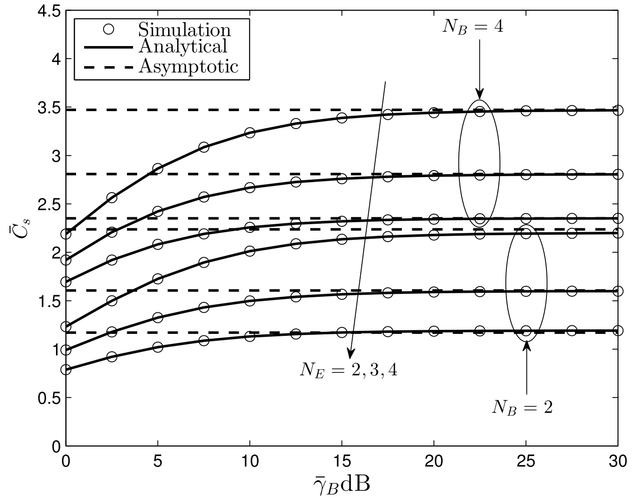

**FIGURE 11.** Average Secrecy Capacity for different antenna configurations ($h_B$ and $h_E$: ILS scenario, $R = 100$ Km, $d_E = 80$ Km).

better channel quality for Bob corresponds to a smaller power offset $\mathcal{L}_\infty^B$, the average secrecy capacity of the considered system increases as the main link quality is getting better. On the other hand, as validated in (73), a better channel quality for the eavesdropper can degrade the average secrecy capacity of the proposed system. Consequently, to improve the secrecy performance of the legitimate user, we should add more artificial noise on the eavesdropper to weaker its link condition.

### 2) IBC

Subsequently, we focus on the cases when Eve is located close to Bob. Firstly, Fig. 9 and Fig. 10 show the secrecy outage probability for different antenna configurations and shadowing severity of the Sat-Bob and Sat-Eve channels, respectively. As predicted in (45), for all the analytical curves, the secrecy outage probability gradually converges to a finite lower bound at high SNR, which proves that the achievable secrecy diversity order collapses to zero when Eve is located close to the legitimate user. In this case, increasing the transmit power does not provide additional secrecy performance enhancement, and the various key channel parameters only affect the secrecy array gain. Another phenomenon that must be noticed is that the channel shadowing severities of the Eve link have a greater impact on the system performance even if Bob's channel is already on average stronger than Eve's. This observation is different from the findings in Fig. 5 and Fig. 6, where the Eve is located far away from Bob.

Then, Fig. 11 and Fig. 12 plot the average secrecy capacity for different antenna configurations and shadowing severity. We can observe that the average secrecy capacity asymptotically approaches an upper bound in the high SNR regime, which confirms the high SNR slope $S_\infty$ equals zero as suggested by (76). Meanwhile, different channel parameters improve or reduce the achievable average secrecy capacity by affecting the high SNR power offset.

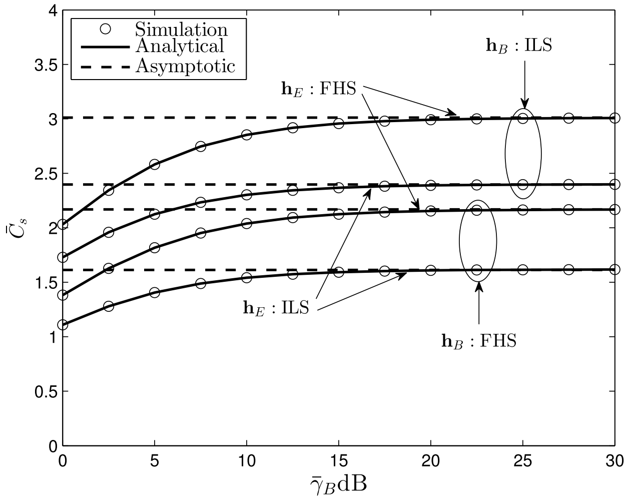

**FIGURE 12. Average Secrecy Capacity for different shadowing severities ($N_B = N_E = 4$, $R = 100$ Km, $d_E = 80$ Km).**

## VII. CONCLUSIONS

In this paper, a security problem for LMS communication systems has been studied, where the confidential messages sent by a single antenna satellite to a multi-antenna legitimate user are overheard by a multi-antenna eavesdropper. Specifically, two representative scenarios have been considered, namely, Scenario I: the satellite has no knowledge of the eavesdropper, and Scenario II: the CSI of the eavesdropper is available at the satellite. For Scenario I, we derived analytical expressions for the probability of non-zero secrecy capacity, and the exact and asymptotic secrecy outage probability of the network. For scenario II, both the exact and asymptotic average secrecy capacity were obtained. Finally, numerical results for both scenarios were provided to validate the theoretical derivations, and show the impact of various key parameters on the secrecy performance of the LMS system. For Scenario I, we demonstrated that the secrecy diversity order of the system only depends on $N_B$, and an increase in $N_E$ only degrades the secrecy array gain. For Scenario II, we found that system parameters can only affect the high SNR power offset, while the slope at the high SNR always remains as one in all cases. Furthermore, for both scenarios, we noted that an improved secrecy performance of the satellite system can be achieved when either the desired user's channel is stronger on average than the eavesdropper's, or the strength of the LOS component increases. The contributions of this work provide an intuitive guidance for the system design, performance evaluation, and implementation of physical layer security in satellite communication systems.

.

## APPENDIX A
## PROOF OF THEOREM 1

Inspired by the series representation of the incomplete gamma function [27, eq. (8.354.1)]

$$\gamma(\alpha, x) = x^{\alpha}\sum_{n=0}^{\infty}\frac{(-1)^n x^n}{n!(\alpha+n)} \overset{x\to 0}{\approx} \frac{x^{\alpha}}{\alpha}, \qquad (A.1)$$

we have the asymptotic CDF of $\gamma_i$ as

$$F^{\infty}_{\gamma_i}(x) = \alpha_i^{N_i}\sum_{l_i=0}^{c_i}\binom{c_i}{l_i}\beta_i^{c_i-l_i}\frac{(-1)^{l_i} l_i!(\beta_i-\delta_i)^{l_i-d_i}}{\Gamma(d_i-l_i)(1-d_i)_{l_i}} \times\binom{d_i-1}{l_i}\left(\frac{\beta_i-\delta_i}{\bar{\gamma}_i}\right)^{d_i-l_i}\frac{x^{d_i-l_i}}{d_i-l_i}. \qquad (A.2)$$

Considering that the asymptotic performance of $F^{\infty}_{\gamma_i}(x)$ is determined by the lowest-order terms of $\bar{\gamma}_1$ at high SNR, we let $l_i = c_i$ in (A.2), and further obtain

$$F^{\infty}_{\gamma_i}(x) = \frac{\alpha_i^{N_i}(-1)^{c_i}c_i!}{\Gamma(N_i+1)(1-d_i)_{c_i}}\binom{d_i-1}{c_i}\frac{x^{N_i}}{\bar{\gamma}_i^{N_i}} + O\left(x^{N_i+1}\right). \qquad (A.3)$$

Based on (35), the asymptotic secrecy outage probability can be expressed as

$$P^{\infty}_{out}(R_s) = \int_0^{\infty} F^{\infty}_{\gamma_B}\left(2^{R_s}(1+y)-1\right) f_{\gamma_E}(y)\,dy \quad (A.4)$$

Hence, by using (A.3) and (20) in (A.4) and applying [27, eq. (7.813.1)], $P^{\infty}_{out}(R_s)$ can be derived as shown in Theorem I.

## REFERENCES

[1] A. Vaneli-Corali *et al.*, "Satellite communications: Research trends and open issues," in *Proc. Int. Workshop Satell. Space Commun. (IWSSC)*, Sep. 2007, pp. 71–75.

[2] G. Zheng, *et al.* "Generic optimization of linear precoding in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2308–2320, Jun. 2012.

[3] D. Christopoulos, S. Chatzinotas, and B. Ottersten, "Multicast multigroup precoding and user scheduling for frame-based satellite communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4695–4707, Sep. 2015.

[4] V. K. Sakarellos, C. Kourogiorgas, and A. D. Panagopoulos, "Cooperative hybrid land mobile satellite–terrestrial broadcasting systems: Outage probability evaluation and accurate simulation," *Wireless Pers. Commun.*, vol. 79, no. 2, pp. 1471–1481, Nov. 2014.

[5] K. An *et al.* "Symbol error analysis of hybrid Satellite-terrestrial cooperative networks with co-channel interference," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1947–1950, Nov. 2014.

[6] K. P. Liolis, A. D. Panagopoulos, and P. G. Cottis, "Multi-satellite MIMO communications at Ku-band and above: Investigations on spatial multiplexing for capacity improvement and selection diversity for interference mitigation," *EURASIP J. Wireless Commun. Netw.*, vol. 2007, Dec. 2007, Art. no. 059608.

[7] N. I. Miridakis, D. D. Vergados, and A. Michalas, "Dual-hop communication over a satellite relay and shadowed rician channels," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4031–4040, Sep. 2015.

[8] K. An, M. Lin, W.-P. Zhu, Y. Huang, and G. Zheng, "Outage performance of cognitive hybrid satellite–terrestrial networks with interference constraint," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9397–9404, Nov. 2016.

[9] K. An *et al.*, "Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4390–4404, Nov. 2015.

[10] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[11] H. Cruickshank, M. P. Howarth, S. Iyengar, Z. Sun, and L. Claverotte, "Securing multicast in DVB-RCS satellite systems," *IEEE Wireless Commun.*, vol. 12, no. 5, pp. 38–45, Oct. 2005.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[13] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[14] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[15] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] 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 Secur.*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[17] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.

[18] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

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

[20] J. Lei, Z. Han, M. Á. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.

[21] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[22] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1862–1874, Sep. 2015.

[23] A. Vazquez-Castro and M. Hayashi, "Information-theoretic physical layer security for satellite channels," in *Proc. IEEE AERO*, Big Sky, MT, USA, Mar. 2017, pp. 1–14.

[24] B. Li, Z. Fei, X. Xu, and Z. Chu, "Resource allocations for secure cognitive satellite-terrestrial networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 78–81, Feb. 2018.

[25] B. Li, Z. Fei, Z. Chu, F. Zhou, K.-K. Wong, and P. Xiao, "Robust chance-constrained secure transmission for cognitive satellite–terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4208–4219, May 2018.

[26] 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.

[27] A. Abdi, W. C. Lau, M. S. Alouini, and M. Kaveh, "A new simple model for land mobile satellite channels: First- and second-order statistics," *IEEE Trans. Wireless Commun.*, vol. 2, no. 3, pp. 519–528, May 2003.

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[29] J. Arnau, D. Christopoulos, S. Chatzinotas, C. Mosquera, and B. Ottersten, "Performance of the multibeam satellite return link with correlated rain attenuation," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6286–6299, Nov. 2014.

[30] M. R. Bhatnagar and M. K. Arti, "On the closed-form performance analysis of maximal ratio combining in Shadowed–Rician fading LMS channels," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 54–57, Jan. 2014.

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

[32] Accessed: 2015. [Online]. Available: http:functions.wolfram.com/07.20.03.0007.01

[33] A. P. Prudnikov *et al.*, *Integrals and Series: More Special Functions*, vol. 3. New York, NY, USA: Gordon & Breach, 1990.

[34] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. Int. Conf. Symp. Algebr. Comput.*, 1990, pp. 212–224.

[35] R. P. Agrawal, "Certain transformation formulae and Meijer's G function of two variables," *Indian J. Pure Appl. Math.*, vol. 1, no. 4, pp. 537–551, 1970.

[36] A. P. Prudnikov, *Integrals and Series: Elementary Functions*, vol. 1. New York, NY, USA: Gordon & Breach, 1990.

[37] A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.

[38] S. Jin, R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

**KANG AN** received the B.E. degree in electronic engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011, the M.E. degree in communication engineering from the PLA University of Science and Technology, Nanjing, China, in 2014, and the Ph.D. degree in communication engineering from Army Engineering University, Nanjing, China, in 2017. Since 2018, he has been with the Sixty-third/63$^{rd}$ Research Institute, National University of Defense Technology, Nanjing, China, where he is currently an Engineer. His research interests include satellite communication, cooperative communication, physical layer security, and cognitive radio.

**TAO LIANG** received the Ph.D. degree in computer science and technology from the Nanjing Institute of Communications Engineering, Nanjing, China, in 1998. Since 2017, he has been with the Sixty-third/63rd Research Institute, National University of Defense Technology, Nanjing, where he is currently a Research Fellow. His research interests include satellite communication, digital signal processing in communications, physical layer security, cooperative communication, and cognitive network.

**XIAOJUAN YAN** (S'18) received the B.S. degree from the Southwest University of Science and Technology in 2007 and the M.S. degree from Guangxi University in 2014. She is currently pursuing the Ph.D. degree with the School of Information and Communications, Guilin University of Electronic Technology, China. From 2016 to 2017, she was a Visiting Ph.D. Student with Heriot-Watt University, Edinburgh, U.K., under the supervision of Prof. C.-X. Wang. Her current research interests are in the fields of satellite-terrestrial networks, cooperative communications, and non-orthogonal multiple access.

**GAN ZHENG** (S'05–M'09–SM'12) received the B.Eng. and M.Eng. degrees in electronic and information engineering from Tianjin University, China, in 2002 and 2004, respectively, and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, Hong Kong, in 2008.

He is currently a Senior Lecturer with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, U.K. His research interests include UAV communications, edge caching, full-duplex radio, wireless power transfer, cooperative communications, cognitive radio, and physical-layer security. He was a Best Recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2015 GLOBECOM Best Paper Award. He currently serves as an Associate Editor for the IEEE Communications Letters.