IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 17, 2019, accepted February 28, 2019, date of publication March 4, 2019, date of current version March 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2902716

Physical Layer Security for Land Mobile Satellite Communication Networks With User Cooperation

RUGANG WANG[1,2,3], (Member, IEEE), AND FENG ZHOU[3,4,5], (Member, IEEE)

[1]School of Information Technology, Yancheng Institute of Technology, Yancheng 224051, China
[2]Research Center of Yancheng City Optical Fiber Sensing and Applied Engineering Technology, Yancheng 224051, China
[3]Collaborative Innovation Center of Jiangsu Provincial Ecological Building Materials and Environmental Protection Equipment, Research Center of Yancheng City Optical Fiber Sensing and Applied Engineering Technology, School of Information Technology, Yancheng Institute of Technology, Yancheng 224051, China
[4]School of Information Technology, Yancheng Institute of Technology, Yancheng 224051, China
[5]Joint Open Fund of Jiangsu Collaborative Innovation Center for Ecological Building Material, Nanjing 210096, China

Corresponding author: Feng Zhou (zfycit@ycit.edu.cn)

This work was supported in part by the Natural Science Foundation of China under Grant 61673108, in part by the Colleges and Universities Natural Science Foundation in Jiangsu Province under Contract 18KJB510010, in part by the Open Project Program of the Key Laboratory of Underwater Acoustic Signal Processing, Ministry of Education, China, under Contract UASP1801, in part by the Fundamental Research Funds for the Central Universities under Contract 2242016K30013, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20181050, and in part of the Industry-University-Research Cooperation Project of Jiangsu province under grant No. BY2018282.

ABSTRACT In this paper, we investigate the physical layer security of land mobile satellite (LMS) communication networks, where the multiple legitimate users and eavesdroppers are considered in the system. In order to obtain the best system performance, we propose the cooperating scheme for legitimate users to receive the main signal. Besides, we design two representative eavesdropping scenes for the eavesdroppers, namely, Scene I, colluding scene: the eavesdroppers cooperate with each other and wiretap the information of the main channel together, and the Scene II, non-colluding scene which is the best eavesdropping scene, namely, the most harmful eavesdropper will be selected to overhear the information channel. Furthermore, we obtain the closed-form expressions for the non-zero probability of secrecy capacity, the secrecy outage probability (SOP), and average secrecy capacity (ASC) based on the proposed user cooperation scheme in the presence of two eavesdropping scenes. In order to obtain more insights at the high signal-to-noise-ratios, the asymptotic expressions for the SOP and ASC are also derived under two scenes, from which we can derive the effect of different parameters on the system performance conveniently. Finally, some representative Monte Carlo simulation results are provided to verify the correctness of the obtained analytical results.

INDEX TERMS Land mobile satellite (LMS) communication networks, multiple legitimate users and eavesdroppers, non-zero probability of secrecy capacity (NZPSC), secrecy outage probability (SOP), average secrecy capacity (ASC), user cooperation.

I. INTRODUCTION

Land mobile satellite (LMS) communication networks have attracted much attention due to its wide coverage and high reality, especially for the condition, such as earthquake, deep sea navigation and some disasters. In these conditions, traditional terrestrial communication cannot provide a reliable communication [1]–[4].

The inherent broadcast nature and immense coverage area of LMS communication networks make them vulnerable to potential eavesdropping by illegitimate users [5]. For these reasons, security and privacy in LMS communication has become a critical topic in recent years. In traditional methods, this kind of problem can be solved by the upper layer with the use of cryptographic protocols, i.e., the advanced encryption standard [6]. However, the performance of current cryptographic schemes is on the foundation that the eavesdroppers' computer power is limited. In recent years, the computer power of eavesdropper is becoming more and more powerful [7], so this problem has been mostly solved. Apart from the cryptographic protocol, physical layer security (PLS) has been introduced to strengthen the

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

secure transmission of wireless communications using an information-theoretic point [8]. PLS has initially been proposed by Wyner [9], which exploits the characteristics of fading channels between the user and eavesdropper to improve the secrecy performance. Tolossa *et al.* [10] investigated the secrecy-rate characteristics of multitier downlink heterogeneous networks under generalized fading model for two types scenarios.

As mentioned before, due to the natural characters of the LMS communication networks, secrecy problem is an important issue in the LMS communication networks. An *et al.* [11] studied the secrecy outage probability (SOP) of the LMS communications, especially the asymptotic expressions of the SOP at the high signal-to-noise-ratios (SNRs) were derived. An *et al.* [12] obtained the closed-form expression for the average secrecy capacity (ASC) of the LMS communication networks. An *et al.* [13] summarized the former papers and analyzed the secrecy performance for the LMS communication networks with one user and one eavesdropper, particularly, the authors derived the closed-form expressions for the SOP and ASC, respectively.

To its regret, the former authors just considered one legitimate user and one eavesdropper scene for LMS communication networks. The ability of satellite is becoming more and more powerful, so there are often multiple users or eavesdroppers existing in one satellite beam. In [14] and [15], the authors have announced that multiple users scene is a popular case in the LMS communication networks. Guo *et al.* [16] derived the closed-form and asymptotic expressions for the SOP of LMS communication networks with one legitimate user and multiple eavesdroppers. Especially, the colluding scheme is used among the eavesdroppers, which leads to better secrecy performance. Besides, Guo *et al.* [17] obtained the closed-form expressions of the SOP and ASC for the LMS communication networks with multiple legitimate users and one eavesdropper for LMS communication networks, particularly, maximum user scheduling scheme is used in the legitimate users. Through this scheme, the secrecy performance is enhanced. Guo *et al.* [18] proposed a new joint relay and user scheduling scheme in the hybrid satellite terrestrial network and obtained the closed-form and asymptotic expressions for ASC of the considered network. Kolawole *et al.* [19] and Vuppala *et al.* [20] analyzed the performance and optimization problems for the cognitive satellite-terrestrial networks. Bankey *et al.* [21], [22] investigated the physical layer security for the multiuser hybrid satellite-terrestrial relay networks. Particularly, the authors derived the closed-form and asymptotic expressions for SOP of the considered networks. In the system, the satellite transmits the signal with the help of a terrestrial relay, however the authors did not consider multiple legitimate users and eavesdroppers in LMS communication networks without a terrestrial relay.

Until now, as the authors know that there are few published papers analyzing the secrecy performance for the case that multiple users and multiple eavesdroppers both existed in LMS communication networks. Especially both colluding scheme and non-colluding scheme are considered for the considered scene, which is the motivation of our paper. The contributions of our paper are summarized as follows:

TABLE 1. **Abbreviations and acronyms.**

Acronym	Definition
ASC	average secrecy capacity
AWGN	additive white Gaussian noise
CDF	cumulative distribution function
FSL	free space loss
LMS	land mobile satellite
MC	monte carlo
NZPSC	non-zero probability of secrecy capacity
PDF	probability density function
PLS	physical layer security
SNR	signal-to-noise-ratio
SNRs	signal-to-noise-ratios
SOP	secrecy outage probability
SR	shadowed-Rician

- Firstly, we designed a practical secrecy model for the LMS communication networks with multiple legitimate users and multiple eavesdroppers, which is the extension of the previous papers [16] and [17].
- Secondly, two eavesdropping schemes are considered in the system, namely, colluding scheme and non-colluding scheme.
- Thirdly, the closed-form expressions for the NZPSC, SOP and ASC of the considered system are both derived, which provide efficient ways to evaluate the key parameters on the secrecy system performance.
- Finally, in order to obtain more insights of the system parameters on the secrecy performance at high SNRs, the asymptotic analysis is also given.

The rest of this paper is organized as follows. The system illustration is given in Section II. In Section III, the secrecy system performance is provided, which presents the exact closed-form expressions for the NZPSC, SOP and ASC of the considered LMS communication networks. In section IV, the asymptotic expressions for the SOP and ASC are obtained. Section V shows the Monte Carlo (MC) simulation results, which validate the theoretical analysis. Finally, in Section VI, an elaborate summary of the paper is given.

Notations: **Bold** uppercase letters denote matrices and bold lowercase letters denote vectors, $|\cdot|$ the absolute value of a complex scalar; $\exp(\cdot)$ is the exponential function, $E[\cdot]$ the expectation operator, $\mathcal{CN}(a, b)$ the complex Gaussian distribution of a random coefficient a and covariance b.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As illustrated in Figure 1, in this paper, we consider a general secrecy LMS communication network, which consists of

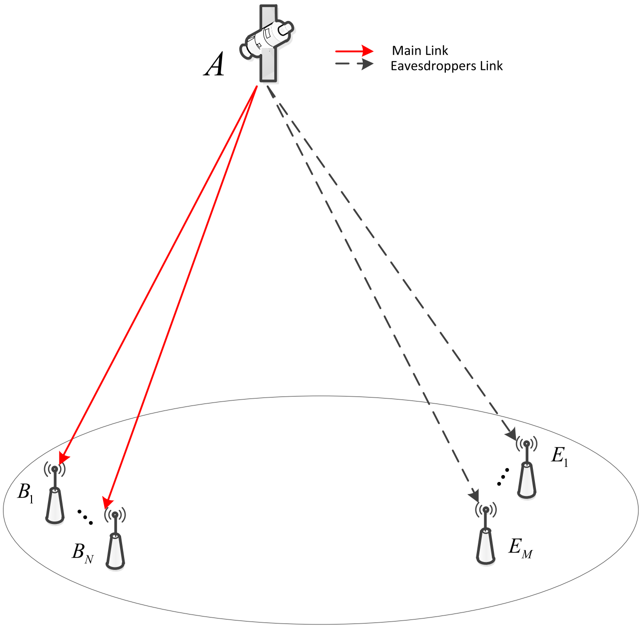


FIGURE 1. The illustration of the system model.

multiple legitimate users and multiple eavesdroppers. In the secrecy LMS system model, the satellite (Alice), i.e, S communicates with the N legitimate users (Bobs) in the presence of multiple eavesdroppers (Eves). As presented before, there are M eavesdroppers around the legitimate users as a result of the wide satellite beam coverage. In the system, we assume that each node is equipped with a single antenna, respectively.[1]

Alice sends its signal $s(t)$ satisfying $E\left[|s(t)|^2\right] = 1$ to the i-th Bob, the signal received at the i-th Bob is given by

$$y_{SB_i}(t) = \sqrt{P_S} h_{SB_i} s(t) + n_{SB_i}(t), \tag{1}$$

where P_S is the transmitted power of the Alice, h_{SB_i} is the channel coefficient between the Alice and the i-th Bob which obeys the shadowed-Rician (SR) fading channel [14]. $n_{SB_i}(t)$ denotes the additive white Gaussian noise (AWGN) at the i-th Bob with $n_{SB_i}(t) \sim \mathcal{CN}\left(0, \delta^2_{SB_i}\right)$.

From (1), we can easily derive the signal-to-noise-ratio (SNR) between the Alice and the i-th Bob as

$$\gamma_{SB_i} = \frac{P_S \left|h_{SB_i}\right|^2}{\delta^2_{SB_i}}. \tag{2}$$

As colluding scheme[2] is used by Bobs, hence the final SNR at Bobs is obtained as

$$\gamma_{SB} = \sum_{i=1}^{N} \gamma_{SB_i}. \tag{3}$$

As mentioned before, due to the wide coverage of the satellite beam, the Eve could wiretap the information from the satellite, hence the received signal at the j-Eve is given by

$$y_{SE_j}(t) = \sqrt{P_S} h_{SE_j} s(t) + n_{SE_j}(t), \tag{4}$$

where h_{SE_j} is the channel coefficient between the Alice and the j-th Eve which obeys the SR fading channel. $n_{SE_j}(t)$ denotes the AWGN at the j-th Eve with $n_{SE_j}(t) \sim \mathcal{CN}\left(0, \delta^2_{SE_j}\right)$.

From (4), the SNR of the j-th Eve is obtained as

$$\gamma_{SE_j} = \frac{P_S \left|h_{SE_j}\right|^2}{\delta^2_{SE_j}}. \tag{5}$$

In this paper, two eavesdropping scene, i.e, the colluding Scene I and the non-colluding Scene II, are, respectively, considered. In Scene I, all eavesdroppers cooperate with each other and overhear the information, hence the SNR of the Eve's link is derived as

$$\gamma_{SE} = \sum_{j=1}^{M} \gamma_{SE_j}. \tag{6}$$

In Scene II, the eavesdroppers with the largest SNR is selected, so the SNR of the Eve's link is given by

$$\gamma_{SE} = \max_{j \in \{1,\ldots,M\}} \left(\gamma_{SE_j}\right). \tag{7}$$

According to the definition of secrecy capacity, it is given by the difference between the capacity of the main channel and the wiretap channel. With the help of (3), (6) and (7), the secrecy capacity for the system can be obtained as

$$C_S = \left[C_{SB} - C_{SE}\right]^+, \tag{8}$$

where the notation $[x]^+$ represents $\max\{0, x\}$, and C_{SB} and C_{SE} are the channel capacities of the main and the wiretap link, which are defined as $C_{SB} = \log_2(1 + \gamma_{SB})$ and $C_{SE} = \log_2(1 + \gamma_{SE})$, respectively.[3]

III. PERFORMANCE ANALYSIS

A. PRIMARY RESULTS

Before deriving the closed-form expression of the secrecy performance, the probability density function (PDF) and the cumulative distribution function (CDF) of γ_{SB} and γ_{SE} should be given first.

[1] We should note that, in order to simplify the analysis, we assume that all nodes are equipped with a single antenna in this paper. However, the following analysis is still fit for the case that all nodes are equipped with multiple antennas. It is very interesting for us to investigate the case that the satellite is equipped with multiple antennas in our future work. Nevertheless, our presented results will serve as a benchmark of the secrecy system performance and provide useful guidelines for the secrecy LMS communication systems.

[2] In order to obtain the best secrecy system performance, hence the Bobs cooperate with each other to receive the legitimate signals, namely, colluding scheme is used.

[3] The main channel condition here is that $C_B > C_E$, which emphasizes the fact the main channel must be better that the wiretap channel, irrespective of the eavesdropper's computational power, which is another motivation to exploit cooperative communications to provided this much-desired advantages.

The channel coefficient $f_{SL_\xi}, L \in \{B, E\}, \xi \in \{i, j\}$ between the terrestrial user (TU, Legitimate users and eavesdroppers are both considered.) and the on-board beam for downlink is given by

$$f_{SL_\xi} = C_{SL_\xi} h_{SL_\xi}, \tag{9}$$

where h_{SL_ξ} represents the random SR coefficient of satellite channel, and C_{SL_ξ} denotes the radio propagation loss including the effects of free space loss (FSL) and the antenna pattern, which is described as

$$C_{SL_\xi} = \frac{\lambda}{4\pi}\frac{\sqrt{G_{SL_\xi} G_{TU}}}{\sqrt{d^2 + d_0^2}}, \tag{10}$$

where λ denotes the carrier wavelength, d is the distance between the terrestrial users and the center of the satellite beam, and $d_0 \approx 35786$km is the height of a GEO satellite. Besides, G_{TU} is the antenna gain of the TU and G_{SL_ξ} is the satellite on-board beam gain.

According to [23], the antenna gain for the TU with parabolic antenna can be approximately expressed as

$$G_{TU}\,(dB) \simeq \begin{cases} \overline{G}_{\max}, & \textit{for } 0^\circ < \beta < 1^\circ \\ 32 - 25\log\beta, & \textit{for } 1^\circ < \beta < 48^\circ \\ -10, & \textit{for } 48^\circ < \beta \le 180^\circ, \end{cases} \tag{11}$$

where $\overline{G}_{\max}$ is the maximum beam gain at the boresight, and β denotes the off-boresight angle. As for G_{SL_ξ}, by defining θ_k as the angle between the TU position and the beam center with respect to the satellite, and $\bar{\theta}_k$ as the 3dB angle of the on-board beam, the antenna gain from the satellite beam to the TU is approximated by [24]

$$G_{SL_\xi} \simeq G_{\max}\left(\frac{J_1(u_k)}{2u_k} + 36\frac{J_3(u_k)}{u_k^3}\right)^2, \tag{12}$$

where G_{max} denotes the maximal beam gain, $u_k = 2.07123\sin\theta_k/\sin\bar{\theta}_k$, J_1 and J_3 denote the first-kind bessel function of order 1 and 3, respectively. In order to obtain the best system performance, hence $\theta_k \to 0$, as a result of $G_{SL_\xi} \approx G_{\max}$. On this foundation, we can have $f_{SL_\xi} = C_{SL_\xi}^{\max} h_{SL_\xi}$ with $C_{\max} = \lambda\sqrt{G_{\max} G_{TU}}/\left(4\pi\sqrt{d^2 + d_0^2}\right)$.

Remark 1: In this paper, we have considered a more general case of LMS communication networks with multiple users and multiple eavesdroppers, where many practical effects, such as satellite beam pattern and path loss, are taken into account. Thus, our work includes the system model in [16] and [17] as a special case, where only one Bob and one eavesdropper is assumed, respectively.

Furthermore, the PDF of $\gamma_{SL_\xi} = \bar{\gamma}_{SL_\xi}\left|C_{SL_\xi}^{\max} h_{SL_\xi}\right|^2$ is given by

$$f_{\gamma_{SL_\xi}}(x) = \frac{\alpha}{\bar{\gamma}_{SL_\xi}} e^{-\frac{\beta}{\bar{\gamma}_{SL_\xi}}} {}_1F_1\left(m; 1; \frac{\delta}{\bar{\gamma}_{SL_\xi}}x\right), \quad x > 0, \tag{13}$$

where ${}_1F_1(a; b; x)$ denotes the confluent hypergeometric function defined in [26]. $\bar{\gamma}_{SL_\xi}$ is the average SNR between the Alice and the ξ-th user, $\alpha = \left(\frac{2bm}{2bm+\Omega}\right)^m/2b$, $\beta = \frac{1}{2b}$, $\delta = \frac{\Omega}{2b(2bm+\Omega)}$ with Ω, $2b$ and $m \ge 0$ being the average power of the LOS component, the average power of the multipath component, and the fading severity parameter ranging from 0 to ∞, respectively. By considering m being integer, the PDF of γ_{SL_ξ} is given by

$$f_{\gamma_{SL_\xi}}(x) = \alpha\sum_{k=0}^{m-1}\frac{(1-m)_k(-\delta)^k}{(k!)^2\left(\bar{\gamma}_{SL_\xi}\right)^{k+1}}x^k\exp(-\Delta x), \tag{14}$$

where $\Delta = \frac{\beta-\delta}{\bar{\gamma}_{SL_\xi}}$ and $(\cdot)_k$ is the Pochhammer symbol [26].

Hence, with the help of [25], the CDF of γ_{SL_ξ} is given by

$$F_{\gamma_{SL_\xi}}(x) = 1 - \alpha\sum_{k=0}^{m-1}\sum_{t=0}^{k}\frac{(1-m)_k(-\delta)^k}{k!\left(\bar{\gamma}_{SL_\xi}\right)^{k+1}t!\Delta^{k-t+1}}x^t e^{-\Delta x}. \tag{15}$$

From [25] and with the help of (3) and (6), the PDF and CDF for γ_{SL} of Scene I can be, respectively, derived as

$$f_{\gamma_{SL}}(x) = \sum_{\xi_1=0}^{m_{SL}-1}\cdots\sum_{\xi_K=0}^{m_{SL}-1}\Xi(K)\,x^{\Lambda_{SL}-1}e^{-\Delta_{SL}x}, K \in \{N, M\}, \tag{16a}$$

$$F_{\gamma_{SL}}(x) = 1 - \sum_{\xi_1=0}^{m_{SL}-1}\cdots\sum_{\xi_K=0}^{m_{SL}-1}\sum_{t=0}^{\Lambda_{SL}-1}\frac{\Xi(K)(\Lambda_{SL}-1)!}{t!\Delta_{SL}^{\Lambda_{SL}-t}}x^t e^{-\Delta_{SL}x}, \tag{16b}$$

where

$$\Xi(K) \triangleq \prod_{\tau=1}^{K}\zeta(\xi_\tau)\,\alpha_{SL}^K\prod_{\upsilon=1}^{K-1}B\left(\sum_{l=1}^{\upsilon}\xi_l + \upsilon, \xi_{\upsilon+1} + 1\right),$$

$$\Lambda_{SL} \triangleq \sum_{\tau=1}^{K}\xi_\tau + K.$$

From [17] and with the help of (7), the PDF and CDF for γ_{SE} of Scene II can be, respectively, obtained as

$$f_{\gamma_{SE}}(x) = \sum_{r=0}^{M}\binom{M}{r}(-1)^r\exp(-\Delta_{SE}rx)\,\Lambda_{SE} \times\left(\Xi_{SE}x^{\Xi_{SE}-1} - \Delta_{SE}rx^{\Xi_{SE}+1}\right), \tag{17a}$$

$$F_{\gamma_{SE}}(x) = \sum_{r=0}^{M}\binom{M}{r}(-1)^r\exp(-\Delta_{SE}rx)\,\Lambda_{SE}x^{\Xi_{SE}}, \tag{17b}$$

where

$$\Xi_{SE} = (m_{SE}-1)\left(r - \sum_{\zeta=1}^{m_{SE}-1}n_\zeta\right) + \sum_{\xi=1}^{m_{SE}-2}\xi n_{\xi+1}, \tag{18}$$

and Ξ_{SE} is given as (19), which is shown at the top of next page. In (19), a_i is given by

$$a_i = \sum_{k_{SE}=i-1}^{m_{SE}-1}\frac{\alpha_{SE}(1-m_{SE})_{k_{SE}}(-\delta_{SE})^{-k_{SE}}}{(k_{SE}!)\,\bar{\gamma}_{SE}^{-k_{SE}+1}\Delta_{SE}^{k_{SE}-i+2}(i-1)!}. \tag{20}$$

$$\Lambda_{SE} = \sum_{n_1=0}^{r} \sum_{n_2=0}^{r-n_1} \cdots \sum_{n_{m_{SE}-1}}^{r-\sum_{l=1}^{n_{m_{SE}-2}} n_l} \frac{r! a_{m_{SE}}^{r-\sum_{j=1}^{n_{m_{SE}-1}} n_j} \prod_{i=1}^{m_{SE}-1} a_i^{n_i}}{n_1! \left(r - \sum_{p=1}^{n_{m_{SE}-1}} n_p\right)!}, \tag{19}$$

B. THE NON-ZERO PROBABILITY OF SECRECY CAPACITY

The non-zero probability of secrecy capacity is the probability that the secrecy capacity C_S remains higher than 0, which is defined as

$$P_{NZPSC} = \Pr\left(C_S > 0\right). \tag{21}$$

Lemma 1: The NZPSC of the considered system for Scene I is given by

$$\begin{aligned}\Pr\left(C_S > 0\right) &= 1 - \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{t=0}^{\Lambda_{SE}-1} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \frac{\Xi\left(N\right)}{t! \Delta_{SE}^{\Lambda_{SE}-t}} \\ &\quad \times \frac{\Xi\left(M\right)\left(\Lambda_{SE}-1\right)!\left(t+\Lambda_{SB}-1\right)!}{\left(\Delta_{SB}+\Delta_{SE}\right)^{t+\Lambda_{SB}}}. \end{aligned} \tag{22}$$

The NZPSC of the considered system for Scene II is derived as

$$\begin{aligned}\Pr\left(C_S > 0\right) = \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{r=0}^{M} \binom{M}{r} \\ \times \frac{\Xi\left(N\right)\left(-1\right)^r \Lambda_{SE}\left(\Xi_{SE}+\Lambda_{SB}-1\right)!}{\left(\Delta_{SE} r + \Delta_{SB}\right)^{\Xi_{SE}+\Lambda_{SB}}}. \end{aligned} \tag{23}$$

Proof: See Appendix A. □

C. SECRECY OUTAGE PROBABILITY

SOP is the likelihood of achieving a non-negative target secrecy rate C_0. It is declared when the instantaneous capacity C_S drops below a target rate, which is defined as

$$P_{sout} = \Pr\left(C_S < C_0\right), \tag{24}$$

where $C_0 = \log_2\left(1+\gamma_0\right)$, γ_0 is the predefined threshold of the secrecy system.

Lemma 2: The SOP of the considered system for Scene I is given by (25)*, which is given at the top of next page.*

The SOP of the considered system for Scene II is derived as (26)*, which is shown at the top of next page.*

Proof: See Appendix B. □

D. AVERAGE SECRECY CAPACITY

By recalling the definition of the achieved secrecy rate given in (8), we can obtain

$$\begin{aligned}C_S = \int_0^\infty \int_z^\infty \left[\log_2\left(1+x\right) - \log_2\left(1+z\right)\right] \\ \times f_{\gamma_{SE}}\left(z\right) f_{\gamma_{SB}}\left(x\right) dz dx. \end{aligned} \tag{27}$$

From [27], in order to evaluate the above integrals, we first evaluate the inner integral by applying integration by parts, and after applying some algebraic manipulations, the ASC can be represented as follows:

$$\begin{aligned}C_S &= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_{SE}}\left(z\right)}{1+z} \left[\int_z^\infty F_{\gamma_{SB}}\left(x\right) dx\right] dz \\ &= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_{SE}}\left(z\right)}{1+z} \left[1 - F_{\gamma_{SB}}\left(z\right)\right] dz. \end{aligned} \tag{28}$$

Now, the closed-form expression for (28) can be derived in Lemma 3.

Lemma 3: The ASC of the considered system for Scene I is given as (29)*, which is shown at the top of next page.*

In (29),

$$\begin{aligned}H\left(n, \mu, \beta\right) &= \left(-1\right)^{n-1} \beta^n e^{\beta\mu} Ei\left(-\beta\mu\right) \\ &\quad + \sum_{s=1}^{n} \frac{\left(s-1\right)!\left(-\beta\right)^{n-s}}{\mu^s}, \mu > 0, \end{aligned}$$

The ASC of the considered system for Scene II is derived as

$$\begin{aligned}\overline{C}_S \\ = \frac{1}{\ln 2} \sum_{r=0}^{M} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{t=0}^{\Lambda_{SB}-1} \binom{M}{r} \frac{\left(-1\right)^r \Lambda_{SE} \Xi\left(N\right)}{t!} \\ \times \frac{\left(\Lambda_{SB}-1\right)!}{\Delta_{SB}^{\Lambda_{SB}-t}} H\left(\Xi_{SE}+t, \left(\Delta_{SE} r + \Delta_{SB}\right), 1\right). \end{aligned} \tag{30}$$

Proof: See Appendix C. □

IV. THE ASYMPTOTIC ANALYSIS

In what follows, to evaluate the impacts of key system parameters on the SOP and ASC in depth, we also look into the SOP and average secrecy capacity at high SNRs. The detailed analysis for the asymptotic SOP and ASC are obtained in the following, respectively.

A. ASYMPTOTIC SECRECY OUTAGE PROBABILITY

We now derive the asymptotic SOP expression when $\overline{\gamma}_{SB} \rightarrow \infty$. This expression allows us to examine the secrecy performance conveniently in the high SNRs regime via two parameters, namely the secrecy diversity order and the secrecy array gain. When $\overline{\gamma}_{SB} \rightarrow \infty$, the expression for (16b) with $SL = SB$ is given by

$$F_{\gamma_{SB}}\left(x\right) \approx \frac{1}{N!} \left(\frac{\alpha_{SB}}{\overline{\gamma}_{SB}} x\right)^N. \tag{31}$$

Lemma 4: Then utilizing (31), (16a) *with* $SL = SE$ *and* (24)*, for Scene I, it can be rewritten as*

$$P_{sout}^{\infty} = \frac{1}{N!} \left(\frac{\alpha_{SB}}{\overline{\gamma}_{SB}}\right)^N \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{q_1=0}^{N} \Xi\left(M\right) \binom{N}{q_1}$$

$$P_{sout} = 1 - \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{t=0}^{\Lambda_{SB}-1} \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \frac{\Xi(N)\,\Xi(M)\,(\Lambda_{SB}-1)!}{t!\Delta_{SB}^{\Lambda_{SB}-t}} \times \sum_{q=0}^{t} \binom{t}{q} \frac{\gamma_0^{t-q}(1+\gamma_0)^q e^{-\Delta_{SB}\gamma_0}(\Lambda_{SE}-1+q)!}{[\Delta_{SB}(1+\gamma_0)+\Delta_{SE}]^{\Lambda_{SE}+q}}. \tag{25}$$

$$P_{sout} = 1 - \sum_{r=0}^{M} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{t=0}^{\Lambda_{SB}-1} \sum_{p=0}^{t} \binom{M}{r}\binom{t}{p} \frac{(-1)^r \Lambda_{SE}\,\Xi(N)\,(\Lambda_{SB}-1)!}{t!\Delta_{SB}^{\Lambda_{SB}-t}} \times \gamma_0^{t-p}(1+\gamma_0)^p e^{-\Delta_{SB}\gamma_0} \left\{ \frac{\Xi_{SE}(\Xi_{SE}-1+p)!}{[\Delta_{SB}(1+\gamma_0)+\Delta_{SE}r]^{\Xi_{SE}+p}} - \frac{\Delta_{SE}r(\Xi_{SE}+1+p)!}{[\Delta_{SB}(1+\gamma_0)+\Delta_{SE}r]^{\Xi_{SE}+p+2}} \right\}. \tag{26}$$

$$\overline{C}_S = \frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{t=0}^{\Lambda_{SB}-1} \frac{\Xi(N)(\Lambda_{SB}-1)!H(t,\Delta_{SB},1)}{t!\Delta_{SB}^{\Lambda_{SB}-t}} + \frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \sum_{t=0}^{\Lambda_{SB}-1} \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{t_1=0}^{\Lambda_{SE}-1} \frac{\Xi(M)}{t_1!} \times \frac{(\Lambda_{SE}-1)!\Xi(N)(\Lambda_{SB}-1)!}{t!\Delta_{SE}^{\Lambda_{SE}-t_1}\Delta_{SB}^{\Lambda_{SB}-t}} H(t+t_1,(\Delta_{SB}+\Delta_{SE}),1). \tag{29}$$

$$\times \frac{\gamma_0^{N-q_1}(1+\gamma_0)^{q_1}(\Lambda_{SE}-1+q_1)!}{\Delta_{SE}^{\Lambda_{SE}+q_1}}. \tag{32}$$

Then utilizing (31), (17a) *and* (24), *for Scene II, it can be given by*

$$P_{sout}^{\infty} = \frac{1}{N!}\left(\frac{\alpha_{SB}}{\overline{\gamma}_{SB}}\right)^N \sum_{q_2=0}^{N} \sum_{r=0}^{M} \binom{N}{q_2}\binom{M}{r} \frac{(-1)^r \Lambda_{SE}}{\gamma_0^{q_2-N}(1+\gamma_0)^{-q_2}} \times \left[\frac{\Xi_{SE}(\Xi_{SE}-1+q_2)!}{(\Delta_{SE}r)^{\Xi_{SE}+q_2}} - \frac{\Delta_{SE}r(\Xi_{SE}+1+q_2)!}{(\Delta_{SE}r)^{\Xi_{SE}+2+q_2}} \right]. \tag{33}$$

Proof: The desired result can be obtained by replacing (16a) *(SL = SE) with* (17a), *and following the similar procedure in Appendix C.* □

From (32) and (33), we extract the secrecy diversity order and secrecy array gain. In doing so, (32) can be rewritten as

$$P_{sout}^{\infty} = G_1^{G_{d_1}}, \tag{34}$$

where $G_{d_1} = N$ is the secrecy diversity order and the secrecy array gain is given by

$$G_1 = \frac{\alpha_{SB}}{\bar{\gamma}_{SB}} \left[\sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{q_1=0}^{N} \frac{\Xi(M)}{N!}\binom{N}{q_1} \times \frac{\gamma_0^{N-q_1}(1+\gamma_0)^{q_1}(\Lambda_{SE}-1+q_1)!}{\Delta_{SE}^{\Lambda_{SE}+q_1}} \right]^{1/N}. \tag{35}$$

With the similar method, (33) can also be re-expressed as

$$P_{sout}^{\infty} = G_2^{G_{d_2}}, \tag{36}$$

where $G_{d_2} = N$ is the secrecy diversity order and the array gain is derived as

$$G_2 = \frac{\alpha_{SB}}{\bar{\gamma}_{SB}} \left\{ \sum_{q_2=0}^{N} \sum_{r=0}^{M} \binom{N}{q_2}\binom{M}{r} \frac{(-1)^r \Lambda_{SE}}{N!\gamma_0^{q_2-N}(1+\gamma_0)^{-q_2}} \times \left[\frac{\Xi_{SE}(\Xi_{SE}-1+q_2)!}{(\Delta_{SE}r)^{\Xi_{SE}+q_2}} - \frac{\Delta_{SE}r(\Xi_{SE}+1+q_2)!}{(\Delta_{SE}r)^{\Xi_{SE}+2+q_2}} \right] \right\}^{1/N}. \tag{37}$$

Remark 2: From G_{d_1} and G_{d_2}, we know that the secrecy diversity order is N, which is the only function of the legitimate users' number. Although the number of eavesdroppers does not affect the secrecy diversity order, it will degrade the secrecy array gain.

B. ASYMPTOTIC AVERAGE SECRECY CAPACITY

We proceed to obtain the asymptotic ASC to examine the maximum average achievable secrecy rate in the high SNR regime. To do this, we assume that the average SNR of the main channel is sufficiently high, i.e., $\overline{\gamma}_{SB} \to \infty$.[4] We maintain the consideration of arbitrary values of the average SNR of the eavesdropping's channel. In order to gain deep insights,

[4] It should be noted that when $\overline{\gamma}_{SE} \to \infty$, the probability of successful eavesdropping approaches 1, so here we do not consider this case.

we provide two novel metrics to characterize the asymptotic ASC, namely, the high SNR slope and the high SNR power offset. To get into the detail analysis of the asymptotic ASC, we should rewrite the CDF of γ_{SE} for Scene I and Scene II, respectively, as

$$\begin{aligned} F_{\gamma_{SE}}(x) &= 1 - \lambda_{SE1}(x), \quad \mathit{SceneI} \\ &= 1 - \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{t=0}^{\Lambda_{SE}-1} \frac{\Xi(M)(\Lambda_{SE}-1)!}{t!\Delta_{SE}^{\Lambda_{SE}-t}} x^t e^{-\Delta_{SE}x}, \end{aligned} \tag{38a}$$

$$\begin{aligned} F_{\gamma_{SE}}(x) &= 1 - \lambda_{SE2}(x), \quad \mathit{SceneII} \\ &= 1 - \sum_{r=1}^{M} \binom{M}{r} (-1)^{r-1} \exp(-\Delta_{SE} r x) \Lambda_{SE} x^{\Xi_{SE}}, \end{aligned} \tag{38b}$$

where

$$\begin{aligned} \lambda_{SE1}(x) &= \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{t=0}^{\Lambda_{SE}-1} \frac{\Xi(M)(\Lambda_{SE}-1)!}{t!\Delta_{SE}^{\Lambda_{SE}-t}} x^t e^{-\Delta_{SE}x}, \end{aligned} \tag{39a}$$

$$\begin{aligned} \lambda_{SE2}(x) &= \sum_{r=1}^{M} \binom{M}{r} (-1)^{r-1} \exp(-\Delta_{SE} r x) \Lambda_{SE} x^{\Xi_{SE}}. \end{aligned} \tag{39b}$$

Lemma 5: The ASC of the considered system in the high SNR regime for Scene I is derived as

$$\overline{C}_S^{\infty} = \omega_1 - \omega_2, \tag{40}$$

where

$$\begin{aligned} \omega_1 &= \frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \frac{\Xi(N)\Gamma(\Lambda_{SB})}{\Delta_{SB}^{\Lambda_{SB}}}, \\ &\quad \times [\psi(\Lambda_{SB}) - \ln(\Delta_{SB})] \end{aligned} \tag{41a}$$

$$\begin{aligned} \omega_2 &= \frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SE}-1} \cdots \sum_{\xi_M=0}^{m_{SE}-1} \sum_{t=0}^{\Lambda_{SE}-1} \frac{\Xi(M)(\Lambda_{SE}-1)!}{t!\Delta_{SE}^{\Lambda_{SE}-t}} \\ &\quad \times H(t, \Delta_{SE}, 1). \end{aligned} \tag{41b}$$

The ASC of the considered system in the high SNR regime for Scene II is obtained as

$$\overline{C}_S^{\infty} = \omega_3 - \omega_4, \tag{42}$$

where

$$\begin{aligned} \omega_3 &= \frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \frac{\Xi(N)\Gamma(\Lambda_{SB})}{\Delta_{SB}^{\Lambda_{SB}}}, \\ &\quad \times [\psi(\Lambda_{SB}) - \ln(\Delta_{SB})] \end{aligned} \tag{43a}$$

$$\omega_4 = \sum_{r=1}^{M} \binom{M}{r} (-1)^{r-1} \Lambda_{SE} H(\Xi_{SE}, \Delta_{SE} r, 1), \tag{43b}$$

where $\psi(\cdot)$ is the digamma function [26, eq. 8.36].

Proof: Please see Appendix D. □

To gain further insights, we evaluate the high SNR slope and the high SNR power offset, as two important system parameters determining the ASC in the high SNR regime. To facilitate the asymptotic analysis, we use the following general form to express the average secrecy capacity as

$$\overline{C}_S^{\infty} = S_{\infty}\left(\log_2 \overline{\gamma}_{SB} - L_{\infty}\right), \tag{44}$$

where S_{∞} is the high SNR slope in *bit/s/Hz* and L_{∞} is the high SNR power offset in 3dB units.

Firstly, we obtain

$$S_{\infty} = \lim_{\overline{\gamma}_{SB} \to \infty} \frac{\overline{C}_S^{\infty}}{\log_2 \overline{\gamma}_{SB}}. \tag{45}$$

By substituting (40) for two scenes into (45), we can easily obtain

$$S_{\infty} = 1. \tag{46}$$

From (46), we conclude that the number of legitimate users and Eavesdroppers have no impacts on the high SNR slope.

Secondly, we can rewrite the high SNR power offset L_{∞} as

$$L_{\infty} = \lim_{\overline{\gamma}_{SB} \to \infty} \left(\log_2 \overline{\gamma}_{SB} - \overline{C}_S^{\infty}\right). \tag{47}$$

It should be noted that (47) definitely characterizes the effect of the main channel and the eavesdropper's channel on the ASC. Hence, by substituting (40) into (47), we can obtain

$$L_{\infty} = L_{\infty}^{SB} + L_{\infty}^{SE}, \tag{48}$$

where

$$\begin{aligned} L_{\infty}^{SB} &= -\frac{1}{\ln 2} \sum_{\xi_1=0}^{m_{SB}-1} \cdots \sum_{\xi_N=0}^{m_{SB}-1} \frac{\Xi(N)\Gamma(\Lambda_{SB})}{\Delta_{SB}^{\Lambda_{SB}}} \\ &\quad \times [\psi(\Lambda_{SB}) - \ln(\beta_{SB} - \delta_{SB})], \end{aligned} \tag{49a}$$

$$L_{\infty}^{SE} = \omega_2, \quad \mathit{for\ SceneI}, \tag{49b}$$

$$L_{\infty}^{SE} = \omega_4, \quad \mathit{for\ SceneII}. \tag{49c}$$

Remark 3: Based on the former analysis, we find that the high SNR power offset is independent of $\overline{\gamma}_{SB}$. It can be found that the contributions of the main channel and eavesdropper channel to L_{∞} are characterized by L_{∞}^{SB} and L_{∞}^{SE}, respectively. We highlight that L_{∞}^{SB} exploits the benefits of N on the ASC. Specially, L_{∞}^{SB} decreases with the increase of N, and as such an enhanced ASC can be obtained. On the other hand, L_{∞}^{SE} quantifies the loss of ASC due to eavesdropping. Specially, L_{∞}^{SE} increases with M, and as such the ASC decreases.

V. NUMERICAL RESULTS

In this section, we provide numerical Monte Carlo (MC) simulation results to verify the correctness of our theoretical results. Without loss of generality, we assume $\delta_{SB_i}^2 = \delta_{SE_j}^2 = 1$ and $\bar{\gamma}_{SB_i} = \bar{\gamma}$ through the figures. The system and channel fading parameters are presented in Table 2 [17] and Table 3 [25], respectively. Scene I: colluding scene; Scene II: non-colluding scene.[5]

TABLE 2. System parameters.

Parameters	Value
Satellite Orbit	GEO
Frequency band	$f = 2\text{GHz}$
3dB angle	$\overline{\theta}_k = 0.8°$
Maximal Beam Gain	$G_{max} = 48\text{dB}$
The Antenna Gain	$G_{ES} = 4\text{dB}$

TABLE 3. Channel parameters.

Shadowing	m	b	Ω
Frequent heavy shadowing (FHS)	1	0.063	0.0007
Average shadowing (AS)	5	0.251	0.279

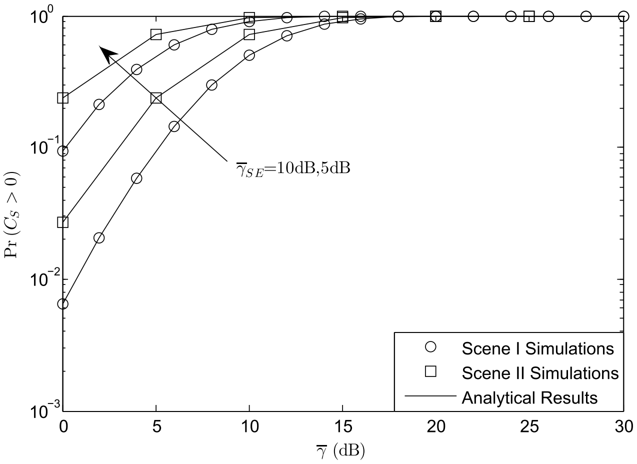
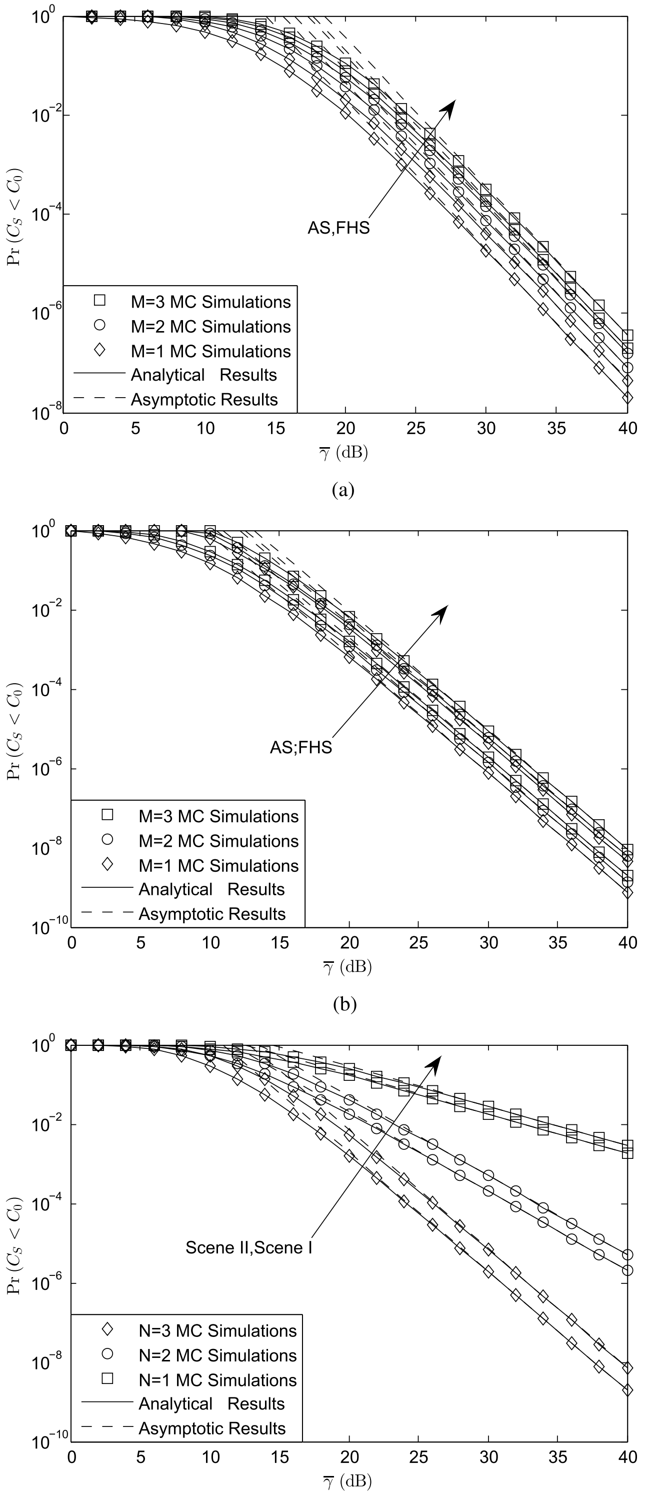


FIGURE 2. The non-zero probability of secrecy capacity of the system versus different $\overline{\gamma}$ with $N = M = 3$ for FHS scenario.

Figure 2 shows the NZPSC of the system versus different $\bar{\gamma}$ with $N = M = 3$ for FHS scenario. In this simulation, we set $\bar{\gamma}_{SE} = 5\text{dB}, 10\text{dB}$, respectively. It is obviously that the obtained analytical results are tight across with the MC simulation ones versus the whole SNR, which verifies the correctness of the analytical results. It can also be found that the NZPSC with $\bar{\gamma}_{SE} = 5\text{dB}$ is larger than that with $\bar{\gamma}_{SE} = 10\text{dB}$ for the reason of more eavesdropping power is used. Besides, the performance of Scene I is worse than that of Scene II which shows the disadvantage of Scene I for the considered system.



(a)

(b)

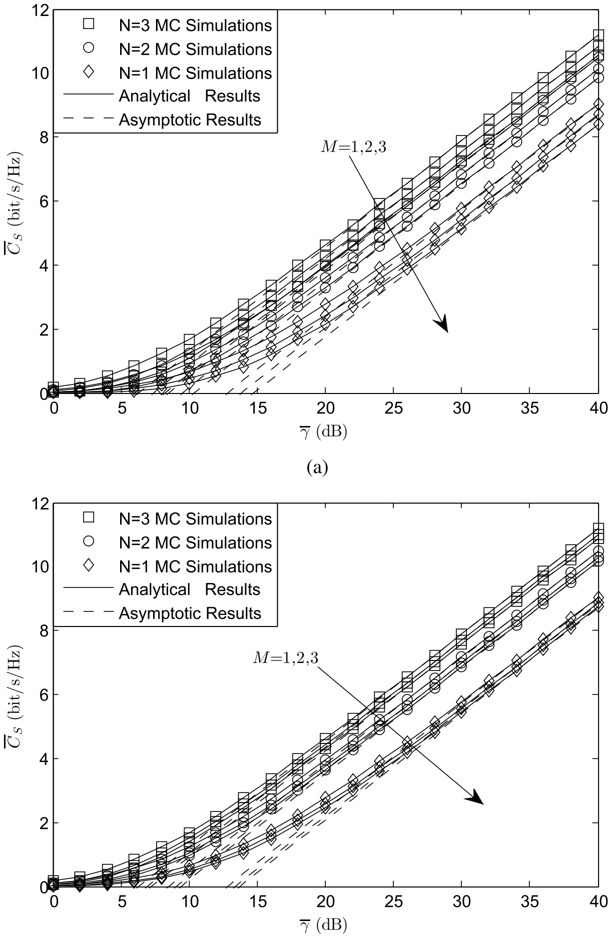
(c)

FIGURE 3. The secrecy outage probability of the system versus different channel shadowing with $\overline{\gamma}_{SE}$=5dB. (a) Scene I for different M. (b) Scene II for different M. (c) Different N for Scene I and Scene II with M=3.

Figure 3 illustrates the SOP of the system versus different channel fading with $\bar{\gamma}_{SE} = 5\text{dB}$. It can be seen that the derived analytical results also match well with the MC simulation ones, while the asymptotic curves are in good agreement with the exact plots in high SNR regime, implying that the obtained theoretical results can accurately evaluate the SOP performance. Compared Figure 3(a) with Figure 3(b), it is obviously that the number of eavesdroppers does not affect the secrecy diversity order, it just influence the secrecy array gain. From the Figure 3(c), the secrecy diversity is only

[5] In the simulation results, we assume that all the legitimate users are located in the same satellite beam.

judged by the number of legitimate users. When N is larger, the diversity is larger, which has been proved in (34) and (36). Finally, the SOP will be larger when the channel is suffering heavy fading.



(a)

(b)

FIGURE 4. The average secrecy capacity of the system versus different N and M with $\overline{\gamma}_{SE}$=5dB for FHS scenario. (a) Scene I. (b) Scene II.

Figure 4 depicts the ASC of the system versus different N and M with $\overline{\gamma}_{SE} = 5$dB for FHS scenario. We find that the ASC for Scene I is smaller than that of Scene II, which can be explained by the fact that Scene I is the worst condition for the system, i.e, all the eavesdroppers cooperate with each other to overhear the confidential information, so the ASC is larger. From Figure 4, we can also find that when N is larger, the ASC is larger. When M is larger, the ASC is smaller, for the reason that in (8), when N is larger or M is smaller, C_S will be larger. Finally, we can find that the high SNR slope of the system is the same, no matter how N and M changes.

VI. CONCLUSIONS

In this paper, we investigated the secrecy performance of land mobile satellite communication networks, where multiple legitimate users and eavesdroppers are considered in the system. Particularly, we analyzed two eavesdroppers cooperation scenes. On the foundation of these scenes, we obtained the closed-form expressions of the non-zero probability of secrecy capacity, the secrecy outage probability and average secrecy capacity. In order to gain more insights at high SNRs, the asymptotic expressions are also derived, which implied the performance of Scene I is worse than that of Scene II. Moreover, we found that the secrecy diversity order is just decided by the number of the legitimate users. The high SNR slope of the average secrecy capacity is fixed. We found that the improvement in channel fading and the number of legitimate users would enhance the system performance, while the increase of the eavesdroppers' number and SNR would degrade the system performance.

APPENDIX A
PROOF OF LEMMA 1

Again from (21), (21) can be rewritten as

$$\begin{aligned}\Pr\left(C_S > 0\right) &= \Pr\left(\gamma_{SB} > \gamma_{SE}\right)\\ &= \int_0^\infty \int_0^y f_{\gamma_{SE}}\left(x\right) f_{\gamma_{SB}}\left(y\right) dxdy\\ &= \int_0^\infty F_{\gamma_{SE}}\left(y\right) f_{\gamma_{SB}}\left(y\right) dy. \qquad (50)\end{aligned}$$

Then for Scene I, by using (16b) with $SL = SE$ and (16a) with $SL = SB$ into (50), after some calculating steps, the final expression can be derived as (22).

Next, for Scene II, with the help of [26], and inserting (17b) and (16a) with $SL = SB$ into (50), after some simplifications, the expression for $\Pr\left(C_S > 0\right)$ can be obtained as (23).

The proof is completed.

APPENDIX B
PROOF OF LEMMA 2

(24) can be re-expressed as

$$\begin{aligned}\Pr\left(C_S < C_0\right) &= \Pr\left[1+\gamma_{SB} < \left(1+\gamma_{SE}\right)\left(1+\gamma_0\right)\right]\\ &= \int_0^\infty \int_0^{y(1+\gamma_0)+\gamma_0} f_{\gamma_{SB}}\left(x\right) f_{\gamma_{SE}}\left(y\right) dxdy\\ &= \int_0^\infty F_{\gamma_{SB}}\left(y\left(1+\gamma_0\right)+\gamma_0\right) f_{\gamma_{SE}}(y) dy. \qquad (51)\end{aligned}$$

Then for Scene I, by substituting (16b) with $SL = SB$ and (16a) with $SL = SE$ into (51), after some calculating steps and utilizing [26, eq. 3.351.3], the final expression for SOP can be derived as (25).

Next, for Scene II, also with the help of [26, eq. 3.351.3], and inserting (17b) and (16a) with $SL = SE$ into (51), after some simplifications, the expression for SOP can be obtained as (26).

The proof is completed.

APPENDIX C
PROOF OF LEMMA 3

For Scene I, by inserting (16b) with $SL = SB, SE$, respectively into (28), (28) can be derived as

$$\begin{aligned}\overline{C}_S &= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_{SE}}\left(z\right)}{1+z}\left[1 - F_{\gamma_{SB}}\left(z\right)\right] dz\\ &= C_1 + C_2, \qquad (52)\end{aligned}$$

where

$$C_1 = \frac{1}{\ln 2}\sum_{\xi_1=0}^{m_{SB}-1}\cdots\sum_{\xi_N=0}^{m_{SB}-1}\sum_{t=0}^{\Lambda_{SB}-1}\frac{\Xi\left(N\right)\left(\Lambda_{SB}-1\right)!}{t!\Delta_{SB}^{\Lambda_{SB}-t}} \times \underbrace{\int_0^\infty \frac{x^t e^{-\Delta_{SB}x}}{1+z}dz}_{J_1}, \tag{53}$$

where J_1 is derived by using [26, eq. 3.353.5] as

$$J_1 = H\left(t, \Delta_{SB}, 1\right). \tag{54}$$

and C_2 is given by

$$C_2 = \frac{1}{\ln 2}\sum_{\xi_1=0}^{m_{SE}-1}\cdots\sum_{\xi_M=0}^{m_{SE}-1}\sum_{t_1=0}^{\Lambda_{SE}-1}\sum_{\xi_1=0}^{m_{SB}-1}\cdots\sum_{\xi_N=0}^{m_{SB}-1}\sum_{t=0}^{\Lambda_{SB}-1}\frac{\Xi\left(M\right)}{t_1!} \times \frac{\left(\Lambda_{SE}-1\right)!\Xi\left(N\right)\left(\Lambda_{SB}-1\right)!}{t!\Delta_{SB}^{\Lambda_{SB}-t}\Delta_{SE}^{\Lambda_{SE}-t}}\underbrace{\int_0^\infty \frac{x^{t+t_1}e^{-\left(\Delta_{SB}+\Delta_{SE}\right)x}}{1+z}dz}_{J_2}. \tag{55}$$

With the help of [26, eq. 3.353.5], J_2 is obtained as

$$J_2 = H\left(t+t_1, \Delta_{SB}+\Delta_{SE}, 1\right). \tag{56}$$

Finally, by inserting (53) and (55) into (52), the final expression for Scene I of the ASC will be derived as (29).

For Scene II, by substituting (17b) and (16b) with $SL = SB$ into (28), (28) can be

$$\overline{C}_S = \frac{1}{\ln 2}\sum_{\xi_1=0}^{m_{SB}-1}\cdots\sum_{\xi_N=0}^{m_{SB}-1}\sum_{t=0}^{\Lambda_{SB}-1}\frac{\Xi\left(N\right)\left(\Lambda_{SB}-1\right)!}{t!\Delta_{SB}^{\Lambda_{SB}-t}} \times \sum_{r=0}^{M}\binom{M}{r}(-1)^r\Lambda_{SE}\underbrace{\int_0^\infty \frac{x^{t+\Xi_{SE}}e^{-\left(\Delta_{SB}+\Delta_{SE}r\right)x}}{1+z}dz}_{J_3}. \tag{57}$$

From [26, eq. 3.353.5], J_3 is given by

$$J_3 = H\left(t+\Xi_{SE}, \Delta_{SB}+\Delta_{SE}r, 1\right). \tag{58}$$

Then, by substituting (57) into (28), the final expression for Scene II of ASC is shown as (30).

The proof is done.

APPENDIX D
PROOF OF LEMMA 4

Again considering (40), for Scene I, (40) can be re-expressed as

$$\overline{C}_S^\infty = \frac{1}{\ln 2}\int_0^\infty\left(\int_0^x \frac{1-\lambda_{SE1}\left(y\right)}{1+y}dy\right)f_{\gamma_{SB}}\left(x\right)dx = \omega_1-\omega_2, \tag{59}$$

where

$$\omega_1 = \frac{1}{\ln 2}\int_0^\infty \ln\left(1+x\right)f_{\gamma_{SB}}\left(x\right)dx, \tag{60}$$

and

$$\omega_2 = \frac{1}{\ln 2}\int_0^\infty\left(\int_0^x \frac{\lambda_{SE1}\left(y\right)}{1+y}dy\right)f_{\gamma_{SB}}\left(x\right)dx. \tag{61}$$

Then, we obtain the asymptotic expressions for ω_1 and ω_2. When $\overline{\gamma}_{SB} \to \infty$, $\ln\left(1+x\right) \approx \ln\left(x\right)$. As such, by utilizing [26, eq. 4.352.1] and performing some algebraic manipulations to derive the asymptotic expression for ω_1 as (41a).

In order to obtain the asymptotic expression for ω_2, we change the order of integration in (61) as

$$\omega_2 = \frac{1}{\ln 2}\int_0^\infty \frac{\lambda_{SE1}\left(y\right)}{1+y}\left[1-F_{\gamma_{SB}}\left(y\right)\right]dy. \tag{62}$$

When $\overline{\gamma}_{SB} \to \infty$, $F_{\gamma_{SB}}\left(y\right) \to 0$. After applying some algebraic manipulations, the asymptotic expression for ω_2 is given by

$$\omega_2 = \frac{1}{\ln 2}\int_0^\infty \frac{\lambda_{SE1}\left(y\right)}{1+y}dy. \tag{63}$$

By substituting (39a) into (63), ω_2 is finally derived as (41b). For Scene II, by replacing (39a) with (39b), the closed-form expressions for ω_3 and ω_4 will be, respectively, obtained. Taking ω_1 and ω_2, ω_3 and ω_4 into (40) and (42), respectively, the asymptotic analysis for ASC will be derived.

The proof is completed.

REFERENCES

[1] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[2] K. Guo, M. Lin, B. Zhang, W.-P. Zhu, J.-B. Wang, and T. A. Tsiftsis, "On the performance of LMS communication with hardware impairments and interference," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1490–1505, Feb. 2019.

[3] K. An, T. Liang, X. Yan, Y. Li, and X. Qiao, "Power allocation in land mobile satellite systems: An energy-efficient perspective," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1374–1377, Jul. 2018.

[4] K. An, T. Liang, G. Zheng, X. Yan, Y. Li, and S. Chatzinotas, "Performance limits of cognitive uplink FSS and terrestrial FS for Ka-band," *IEEE Trans. Aerosp. Electron. Syst.*, to be published.

[5] 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.

[6] 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.

[7] 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, 3rd Quart., 2014.

[8] 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.

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

[10] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-rate analysis in multitier heterogeneous networks under generalized fading model," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 101–110, Feb. 2017.

[11] K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan, and W. Lu, "Secrecy performance analysis of land mobile satellite communication systems over Shadowed–Rician fading channels," in *Proc. 25th Wireless Opt. Commun. Conf. (WOCC)*, Chengdu, China, May 2016, pp. 1–4.

[12] K. An, M. Lin, T. Liang, J. Ouyang, and W.-P. Zhu, "On the ergodic capacity of multiple antenna cognitive satellite terrestrial networks," in *Proc. ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[13] K. An, T. Liang, X. Yan, and G. Zheng, "On the secrecy performance of land mobile satellite communication systems," *IEEE Access*, vol. 6, pp. 39606–39620, 2018.

[14] P. K. Upadhyay and P. K. Sharma, "Max-max user-relay selection scheme in multiuser and multirelay hybrid satellite-terrestrial relay systems," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 268–271, Feb. 2016.

[15] P. K. Sharma, P. K. Upadhyay, D. B. da Costa, P. S. Bithas, and A. G. Kanatas, "Performance analysis of overlay spectrum sharing in hybrid satellite-terrestrial systems with secondary network selection," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6586–6601, Oct. 2017.

[16] K. Guo, B. Zhang, and D. Guo, "Secure performance analysis of a satellite-terrestrial network with multi-eavesdroppers," in *Proc. ICCSNT*, Dalian, China, Oct. 2017, pp. 395–399.

[17] K. Guo, M. Lin, B. Zhang, J. Ouyang, and W.-P. Zhu, "Secrecy performance of satellite wiretap channels with multi-user opportunistic scheduling," *IEEE Wireless Commun. Lett.*, vol. 6, no. 7, pp. 1054–1057, Dec. 2018.

[18] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, "Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling," *IEEE Access*, vol. 6, pp. 55815–55827, 2018.

[19] O. Y. Kolawole, S. Vuppala, M. Sellathurai, and T. Ratnarajah, "On the performance of cognitive satellite-terrestrial networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 668–683, Dec. 2017.

[20] S. Vuppala, M. Sellathurai, and S. Chatzinotas, "Optimal deployment of base stations in cognitive satellite-terrestrial networks," in *Proc. WSA*, Bochum, Germany, Mar. 2018, pp. 1–8.

[21] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, to be published.

[22] V. Bankey and P. K. Upadhyay, "Physical layer secrecy performance analysis of multi-user hybrid satellite-terrestrial relay networks," *CSI Trans. ICT*, vol. 6, no. 2, pp. 187–193, Jun. 2018.

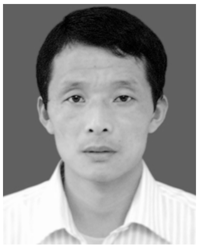
[23] *Prediction Procedure for the Evaluation of Interference Between Stations on the Surface of the Earth at Frequencies Above About 0.1 GHz*, document P.452, ITU-R, Sep. 2013.

[24] 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.

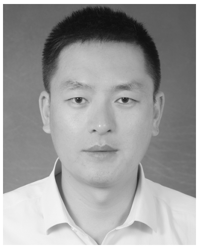
[25] N. I. Miridakis, D. D. Vergados, and A. Michalas, "Dual-hop communication over a satellite relay and shadowed Rician channels," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4031–4040, Sep. 2015.

[26] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of Integrals, Series, and Products*, 7th ed. Boston, MA, USA: Elsevier, 2007.

[27] 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.



RUGANG WANG received the B.S. degrees from the Wuhan University of Technology, Wuhan, China, in 1999, the M.S. degrees from Jinan University, Guangzhou, China, in 2007, and the Ph.D. degrees from Nanjing University, Nanjing, China, in 2012. Since 2012, he has been an Associate Professor with the College of Information Engineering, Yancheng Institute of Technology, Yancheng, China. His research topics include the optical communication networks, novel and key devices for optical communication systems, satellite communication, and physical layer security.



FENG ZHOU received the B.S. and M.S. degrees from Southeast University, Nanjing, China, in 2004 and 2012, respectively. He is currently pursuing the Ph.D. degree with the Army Engineering University of PLA. Since 2017, he has been an Associate Professor with the College of Information Engineering, Yancheng Institute of Technology, Yancheng, China. His research interests include cooperative communication, satellite communication, cognitive radio, and physical layer security.