IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 14, 2019, accepted February 24, 2019, date of publication March 5, 2019, date of current version March 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2903154

Secrecy Performance of Land Mobile Satellite Systems With Imperfect Channel Estimation and Multiple Eavesdroppers

YUSHENG LI[1], KANG AN[1], (Member, IEEE), TAO LIANG[1], AND XIAOJUAN YAN[2,3], (Student Member, IEEE)

[1]Sixty-third 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

Corresponding author: Kang An (ankang89@nudt.edu.cn)

This work was supported in part by the Research Project of NUDT under Grant ZK18-02-11, and in part by the National Natural Science Foundation of China under Grant 61471392.

ABSTRACT The inherent broadcast nature has exposed the land mobile satellite (LMS) communication systems to severe security threats in both the civil and military applications. This paper investigates the secrecy performance of a Shadowed-Rician fading multi-antenna LMS communication system with imperfect channel estimation, which consists of a satellite, a legitimate receiver and a cluster of unauthorized eavesdroppers who want to overhear the confidential message. Specifically, the analytical expressions for the probability of non-zero secrecy capacity are derived in terms of the Meijer-G functions, which provide an efficient means to evaluate the secrecy performance of the system. Then, both the exact and asymptotic secrecy outage probability expressions of the considered system are obtained. Furthermore, based on the simple asymptotic secrecy outage probability, we can reveal two key performance metrics, namely, the secrecy diversity order and secrecy array gain. Finally, simulation results are carried out to validate the theoretical results and show the superiority of employing multiple antennae in enhancing the secrecy performance for LMS communication systems. Our findings suggest that the secrecy diversity order only depends on the number of antennas at the legitimate receiver, and is independent of the imperfect channel estimation and the shadowing severities of both the main and eavesdropper channels.

INDEX TERMS Secrecy performance, physical layer security, satellite communication, imperfect channel estimation.

I. INTRODUCTION

Land mobile satellite (LMS) communication systems have been widely applied in various areas, especially in disaster recovery and rescue missions (see e.g., [1]–[3] and the references therein). The broadcast nature and immense area coverage of LMS communication system makes it inherently vulnerable to potential eavesdropping by illegitimate receivers [4]. As such, the privacy and security issue in satellite communication systems have received enormous attention in both the civil and military areas.

A. BACKGROUND AND MOTIVATION

Typically, the security issues in satellite communications are achieved at upper layers by means of encryption schemes, such as the Advanced Encryption Standard (AES) [5]. Nevertheless, the current cryptographic schemes, which relay on the limited computational power of eavesdropper, have become increasingly unreliable, especially when the computational ability of eavesdropper becomes more powerful [6]. In contrast to the upper layer cryptographic techniques, some efforts have been devoted to the information-theoretic perspective and introduced the physical layer security (PHY) technique to realize the secure transmission of wireless communications by exploiting the different characteristics between the main and eavesdropper's channels. In particular, Wyner [7] first introduced the concept of wiretap channel and laid the foundation for the physical layer security that perfect secure transmission can be achieved when the quality of the eavesdropper's is inferior to that of the main channel, and the result was later extended

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

to the scalar Gaussian wiretap channels [8] and broadcast channels [9].

Early important works focusing on the secrecy performance of terrestrial wireless networks mainly considered the simple scenarios where all the nodes are equipped with a single antenna [10], [11]. However, since multiple antenna technique has exhibited a significant advantage in achieving higher data transmission rates and power efficiency, more and more researchers have paid close attention to the idea of incorporating the multiple antenna technique into wireless communication systems. In [12], the secrecy outage probability for maximal ratio combining (MRC) and selection combining (SC) at the eavesdropper was compared. Moreover, He *et al.* [13] considered MRC at both the legitimate receiver and the eavesdropper, and derived closed-form expressions for the probability of non-zero secrecy rate and the secrecy outage probability. In addition, the secrecy performance for multiple-input multiple-output (MIMO) wiretap channels with orthogonal space-time block codes (OSTBCs) and arbitrary antenna correlation was also analyzed in [14]. In [15] and [16], transmit antenna selection (TAS) was considered to improve the secrecy performance over Rayleigh and Nakagami-m fading channels, respectively. Both MRC and SC at both the legitimate receiver and the eavesdropper were studied in [17], where the asymptotic secrecy outage probability showed that the secrecy diversity order was the same as that without secrecy and independent of the number of the eavesdropper's antennas. More recently, [18] proposed the TAS at the transmitter and the generalized SC (GSC) at the receiver to enhance secure communications.

While theses prior works have significantly improved our understanding on the secrecy performance of multiple antenna wiretap channels, they all suffer the limitation of perfect channel state (CSI) information assumption. Under this situation, the recent work in [19] has investigated the effect of imperfect CSI on the secrecy performance of a multiple antenna wiretap channel over Nakagami-m fading channel. In [20], the secrecy performance for a TAS-MRC system with imperfect feedback was studied over Rayleigh fading channels. Moreover, Huang *et al.* [21] proposed a general-order TAS/MRC scheme with outdated CSI for secure transmission in MIMO wiretap channels over Nakagami-m fading channels.

The physical layer security approach can also be an alternative approach for satellite networks applications. In contrast to the literatures focusing on the terrestrial wireless networks, there are very few works dealing with the physical layer security issues for satellite communication. With perfect CSI, Lei *et al.* [22] first addressed the optimal precoding problem in multibeam satellite systems by proposing a partial zero-forcing (ZF) approach where the useful signal is orthogonal to the eavesdroppers' channels, and then a suboptimal precoding problem based on artificial noise (AN) was provided for scenarios with the perfect or partial CSI. By assuming the availability of the eavesdropper's CSI, the physical layer security issues in satellite communications were investigated in [23] by using the principle of network coding, and the problem of minimizing the transmit power on a multibeam satellite while satisfying individual secrecy rate was studied in [24] for cases of both perfect and imperfect CSI. The expression of the probability of non-zero secrecy capacity for downlink satellite systems under rain fading was analyzed in [25]. Moreover, An *et al.* [26] first investigated the secrecy performance of LMS systems in the presence of both active and passive eavesdroppers. By considering a multiuser multirelay architecture for relay-enabled hybrid satellite-terrestrial networks, the comprehensive secrecy performance of both amplify-and-forward (AF) and decode-and-forward (DF) protocols are presented in [27] with the presence of multiple eavesdroppers. Bankey and Upadhyay [28] analyzed the secrecy performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling scheme. In [29], the achievable secrecy performance merits of LMS systems with co-channel interference were theoretically investigated.

Nevertheless, although these aforementioned works explored the security issues in satellite communication systems from different perspectives, they still suffer from the following disadvantages. Firstly, the perfect CSI of the legitimate user must be available, which is too restrictive in practical scenarios. It should be pointed out that the exact CSI of satellite link is particularly difficult to be obtained due to the high latency affected by the round trip propagation delay [30], [31]. Besides, despite their works for the purpose of system design, various key performance metrics in evaluating the secure transmission, such as the probability of non-zero secrecy capacity and secrecy outage probability have not been studied for satellite communications thus far.

B. CONTRIBUTION AND NOVELTY

In this paper, we investigate the secure performance of LMS communication systems over Shadowed-Rician fading channel, where a satellite communications with a legitimate receiver in the presence of a cluster of unauthorized eavesdropper. Since the multiple antenna technique exhibits a significant advantage in achieving high system capacity and energy efficiency for satellite communication at low cost and complexity [32]–[34], we consider that the legitimate receiver is equipped with multiple antennas to enhance the secrecy performance of the system, while the satellite and eavesdropper have only a single antenna. To make our analysis more comprehensive, we consider only the imperfect CSI is available at the legitimate receiver, and the actual channel gain requires to be estimated by using the training data.

Our detailed contributions can be outlined as follows:

- We first derive the novel analytical expression for the probability of non-zero secrecy capacity in terms of the generalized Meijer-G functions, which provides an efficient approach to evaluate the system performance.
- The exact analytical expressions for the secrecy outage probability are provided, which are general and applicable to the arbitrary number of antennas and training

symbols, and various shadowing severities of the main and eavesdropper channels.

- To gain further insights, the simple asymptotic expressions for secrecy outage probability at high SNR are developed to examine the asymptotic behavior of the considered system, which characterize the impact of key system parameters on the secrecy performance. Based on the derived asymptotic results, we can reveal two important performance metrics, namely the achievable secrecy diversity order and secrecy array gain of the LMS communication system.

Notation: $(\cdot)^H$ denotes the Hermitian transpose, $\|\cdot\|_F$ the Frobenius norm of a matrix, $|\cdot|$ the absolute value, $\mathrm{E}[\cdot]$ is the expectation operator, $\exp(-x)$ is the exponential function, and $\mathcal{N}_C(\boldsymbol{\mu},\boldsymbol{\Sigma})$ represents the circular complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. ${}_1F_1(a;b;c)$ denotes the confluent Hypergeometric function [35, eq. (9.210.1)], $M_{a,b}(\cdot)$ is the Whittaker function [35, eq. (9.221)], $\mathrm{G}_{p,q}^{m,n}[\cdot|\cdot]$ is the Meijer-G functions with a single variable [35, eq. (9.301)].

II. SYSTEM MODEL

As depicted in Fig. 1, we consider a LMS-based wiretap channel which consists of a satellite (Alice), a legitimate receiver (Bob) and a cluster of multiple eavesdropper (Eves).[1] Here, we consider the Alice and Eve have a single antenna while the Bob is equipped with N antennas, which can apply the superiority of multiple antenna technique to improve the secrecy performance of the LMS system.[2] The channel between the Alice and Bob is referred as the main channel and that between the Alice and Eve is referred as the eavesdropper channel. The overall communication can be summarized in the following two phases for training and data transmission.

- **Training Phase:** Since there exists only a single radio frequency (RF) at the Alice, it has to send the training symbols sequence for the channel estimation at Bob.
- **Transmission Phase:** After performing the channel estimation based on the transmitted training symbols, the Bob feedbacks the instantaneous SNR of the main channel to Alice for secure data transmission.

Let $\mathbf{h}_B$ and $h_{E,i}$ denote the channel vector of the main channel, and the channel coefficient of the eavesdropper channel, respectively. The received signal for Bob and Eve at time t are, respectively given by

$$\mathbf{y}_B=\sqrt{P}\mathbf{h}_Bx+\mathbf{n}_B, \tag{1}$$

and

$$y_{E,i}=\sqrt{P}h_{E,i}x+n_E, \tag{2}$$

where P denotes the transmit power at Alice, x the transmitted signal obeying $\mathrm{E}\left[|x|^2\right]=1$, $\mathbf{n}_B\sim\mathcal{N}\left(0,{\sigma_B}^2\boldsymbol{I}_N\right)$

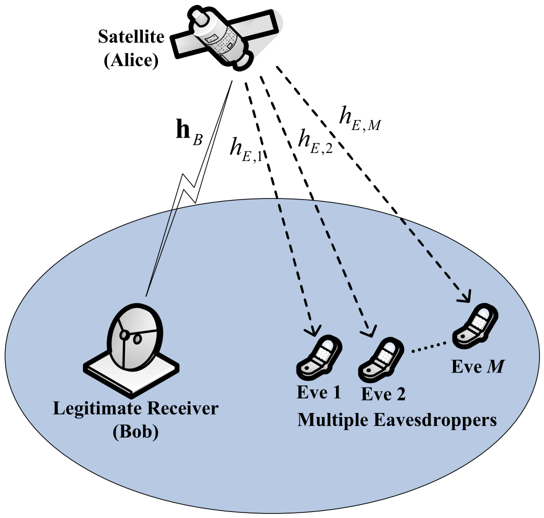


FIGURE 1. System model.

and $n_E\sim\mathcal{N}\left(0,{\sigma_E}^2\right)$ represent the zero mean additive white Gaussian noise (AWGN) at Bob and Eve, respectively. Under the assumption of perfect CSI estimation, the detector of transmitted symbols can be obtained by maximizing the conditional PDF of, which is given by [36]

$$f\left(\mathbf{y}_B\left|x,\mathbf{h}_B\right.\right)=\frac{1}{\sigma^{2N}\pi^N}\exp\left(-\frac{\left\|\mathbf{y}_B-\mathbf{h}_Bx\right\|}{\sigma^2}\right). \tag{3}$$

By maximizing the $f\left(\mathbf{y}_B\left|x,\mathbf{h}_B\right.\right)$, we need to find the required maximum likelihood (ML) detector. From (3), the decision variable for ML detector can be written as [37]

$$\Lambda=\arg\min_x\left\|\mathbf{y}_B-\mathbf{h}_Bx\right\|^2. \tag{4}$$

In practical scenario, the perfect CSI estimation cannot be obtained at the receiver, we replace the exact channel gains by estimated one in the decision variable as

$$\Lambda=\arg\min_x\left\|\mathbf{y}_B-\hat{\mathbf{h}}_Bx\right\|^2, \tag{5}$$

where $\hat{\mathbf{h}}_B$ is the imperfect estimation of $\mathbf{h}_B$. We consider the satellite transmits $L\in\mathbb{Z}^+$ training symbols to the receiver in L time slots during the training phase, therefore the receiver signal at the legitimate receiver can be write as

$$\mathbf{r}_k=\mathbf{h}_Bs+\mathbf{n}_{B,i},\quad k=1,2,\ldots,L, \tag{6}$$

where s is the training symbol with $\mathrm{E}\left[|s|^2\right]=1$, $\mathbf{n}_i$ the AWGN with zero mean and σ^2 variance. Therefore, the ML estimate of can be obtained as [36]

$$\hat{\mathbf{h}}_B=\frac{1}{L}\sum_{k=1}^{L}\mathbf{r}_ks^*=\mathbf{h}_B+\frac{1}{L}\sum_{k=1}^{L}\mathbf{n}_{B,k}s^*=\mathbf{h}_B+\hat{\mathbf{n}}_B, \tag{7}$$

where $\hat{\mathbf{n}}_B$ denotes the estimated noise component with zero mean and σ^2/L variance. By substituting (1) and (7) into (5), we have

$$\Lambda=\arg\min_x\left\|\mathbf{h}_B(x-\tilde{x})-\hat{\mathbf{n}}_Bx+\mathbf{n}_B\right\|^2. \tag{8}$$

[1] Herein, the time division multiplexing (TDM) scheme is employed, and a single legitimate user is served for the considered time slot.

[2] Enabling multiple antennas at a satellite is not a fruitful option due to the lack of scatterers on its vicinity, whereas the multi-antenna terrestrial receiver would be a more suitable solution.

By using the MRC scheme along with (8), the instantaneous received SNR at the Bob can be given by [38]

$$\tilde{\gamma}_B = \frac{\bar{\gamma}_B \left\| \mathbf{h}_B \right\|_F^2}{(1 + 1/L)}, \tag{9}$$

where $\bar{\gamma}_B = P/\sigma_B$ represents the average SNR of the main channel.

As for the multiple Eves, due to the fact that the satellite has no knowledge of the eavesdropping channel, and the Eves does not have to discriminate the pilot and data symbols.[3] Without loss of generality, we consider the worst-case scenario regardless of the estimation error.[4] Please note that the worst-case scenario is the most severe possible outcome that can reasonably be considered to occur in a particularly occasion. Moreover, the adoption of worst-case scenario has been viewed as a common approach in the secrecy performance evaluation, especially to prepare for contingencies that could result in worst issues. After some necessary manipulations, the instantaneous received SNR at i-th $(i = 1, 2, ..., M)$ Eve can be written as

$$\gamma_{E,i} = \frac{P}{\sigma_E} \left| h_{E,i} \right|^2 = \bar{\gamma}_E \left| h_{E,i} \right|^2, \tag{10}$$

where $\bar{\gamma}_E = P/\sigma_E$ is the average SNR of the eavesdropper channels. We consider the cooperative eavesdroppers scenarios, where the illegitimate nodes can cooperative via MRC to form a group of colluding eavesdroppers. Thus, the overall received SNR for of M eavesdroppers can be written as

$$\gamma_E = \sum_{i=1}^{M} \gamma_{E,i} = \bar{\gamma}_E \sum_{i=1}^{M} \left| h_{E,i} \right|^2. \tag{11}$$

The secure data transmission between Alice and Bob can be achieved under the condition that the quality of main channel is superior of eavesdroppers' channel. According to [8], the achievable secrecy capacity of multiple antenna wiretap channels is given by

$$C_S = \begin{cases} C_B - C_E, & \tilde{\gamma}_B > \gamma_E \\ 0, & \gamma_B \le \gamma_E, \end{cases} \tag{12}$$

where $C_B = \log_2(1 + \tilde{\gamma}_B)$ and $C_E = \log_2\left(1 + \gamma_E\right)$ are the main channel capacity of Bob and wiretap channel capacity of Eve, respectively.

III. SECRECY PERFORMANCE

In this section, we present a comprehensive investigation on the secrecy performance of LMS communication systems in terms of the non-zero secrecy capacity, exact as well as asymptotic secrecy outage probability.

A. PRELIMINARY RESULTS

Before delving into the details, we first present the statistical properties of satellite link, which will be frequently used in the subsequent derivations.

Although some mathematical models, such as Loo, Barts-Stutzman, and Karasawa *et al.*, have been presented to describe the satellite channel, the Shadowed-Rician model proposed in [39] is commonly used in existing works, which provides a significantly less computational burden than other channel models, and has been widely used in the related works. In this model, the channel fading coefficient h is described as

$$h = A \exp(j\phi) + Z \exp(j\xi), \tag{13}$$

where ϕ is the stationary random phase vector with its elements uniformly distributed over $[0, 2\pi)$, and ξ the deterministic phase vector of the LOS component. In addition, A and Z are the amplitudes of the scatter and the LOS components, which are the independent stationary random processes following Rayleigh and Nakagami distributions, respectively. The Shadowed-Rician fading distribution can be characterized as $h \sim \mathrm{SR}(\Omega, b, m)$ with Ω being the average power of LoS component, $2b$ the average power of the multipath component, and m the Nakagami-m parameter corresponding to the fading severity.

According to [39], the channel parameters of the satellite links closely depend on the elevation angle θ_i, which can be calculated over the range $20^\circ \le \theta_i \le 80^\circ, i \in \{B, E_j\, (j = 1, 2, ..., M)\}$ by the following expressions

$$\begin{aligned} b_i(\theta_i) &= -4.7943 \times 10^{-8}\theta_i^3 + 5.5784 \times 10^{-6}\theta_i^2 \\ &\quad - 2.1344 \times 10^{-4}\theta_i + 3.2710 \times 10^{-2} \\ m_i(\theta_i) &= 6.3739 \times 10^{-5}\theta_i^3 + 5.8533 \times 10^{-4}\theta_i^2 \\ &\quad - 1.5973 \times 10^{-1}\theta_i + 3.5156 \\ \Omega_i(\theta_i) &= 1.4428 \times 10^{-5}\theta_i^3 - 2.3798 \times 10^{-3}\theta_i^2 \\ &\quad + 1.2702 \times 10^{-1}\theta_i - 1.4864 \end{aligned} \tag{14}$$

For the main link, the channel vector $\mathbf{h}_B$ with identical independent distributed (i.i.d) SR fading distribution is described as $\mathbf{h}_B = \bar{\boldsymbol{h}}_B + j\tilde{\boldsymbol{h}}_B$, where the line-of-sight (LoS) component $\bar{\boldsymbol{h}}_B$ is composed of i.i.d Nakagami-m random variables and the entries of the scattering component $\tilde{\boldsymbol{h}}_B$ follow the i.i.d Rayleigh fading distribution.

Lemma 1: The analytical expression for the PDF of $\tilde{\gamma}_B = \bar{\gamma}_B \left\| \mathbf{h}_B \right\|_F^2 / (1 + 1/L)$ *is given by*

$$f_{\tilde{\gamma}_B} = \alpha_B^N \sum_{l=0}^{c} \binom{c}{l} \beta_B^{c-l} \left[P(x, l, d) + \varepsilon \delta_B P(x, l, d+1) \right], \tag{15}$$

where

$$P(x, l, d) = \frac{x^{d-l-1}}{\bar{\gamma}_B^{d-l}\Gamma(d-l)} \left(1 + \frac{1}{L}\right)^{d-l}$$

[3] This paper focuses on the scenarios that eavesdroppers are passive receivers rather than active jamming threats. If the desired satellite link is completely jammed by eavesdroppers, the possible connection for the legitimate user cannot be guaranteed. We would like to point out the jamming attack is beyond the scope of this work, which could be our future research interest.

[4] Currently, it is difficult to quantitatively determine the estimation error for Eves simultaneously, which will be our future works.

$$\times {}_1F_1\left(d; d-l; -\left(\beta_B - \delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right), \quad (16)$$

with $c = (d-N)^+$, $\varepsilon = m_B N - d$, $d = \max\{N, \lfloor m_B N \rfloor\}$, *where* $\lfloor z \rfloor$ *is the largest integer not greater than z, and* $(z)^+$ *indicates that if* $z < 0$*, then let* $z = 0$. *Proof: The proof can be found in [39].* □

We consider the channel coefficient $h_{E,i}$ from Alice to Eve also follows the Shadowed-Rician fading distribution, which can be similarly modeled as $h_{E,i} = \bar{h}_{E,i} + j\tilde{h}_{E,i}$ with $\bar{h}_{E,i}$ and $\tilde{h}_{E,i}$ being the scattering and LoS components, respectively. As stated above, we consider the multiple eavesdroppers are located in close proximity to each other to employ cooperative eavesdropping. Therefore, as was shown in [25] and [31], the satellite slant path lengths are significantly larger than the terrestrial path between each eavesdropper, which results in almost the equal elevation angles, namely, $\theta_E = \theta_{E,i}\,(i = 1, 2, ..., M)$. Hence, we the PDF of γ_E can be obtained in the following lemma.

Lemma 2: The PDF of $\gamma_E = \bar{\gamma}_E \sum_{i=1}^{M} \left|h_{E,i}\right|^2$ *is given by*

$$f_{\gamma_E}(x) = \frac{\alpha_E^M x^{M-1}}{\Gamma(M)\,\bar{\gamma}_E^N} e^{-\frac{\beta_E x}{\bar{\gamma}_E}}\, {}_1F_1\left(Mm_E; M; \frac{\delta_E x}{\bar{\gamma}_E}\right), \quad (17)$$

where α_E, β_E *and* δ_E *are, respectively, given by*

$$\alpha_E = 2b_E m_E \big/ (2b_E m_E + \Omega_E)^{m_E} \big/ 2b_E, \quad (18a)$$

$$\beta_E = 1\big/2b_E, \quad (18b)$$

$$\delta_E = \Omega_E \big/ 2b_E\,(2b_E m_E + \Omega_E), \quad (18c)$$

where m_E, b_E *and* Ω_E *can be computed form (6).*

Proof: The proof can be found in [39]. □

In the following sections, based on these statistical properties of the fading channels, we will provide a comprehensive performance evaluation of the secrecy performance merits of the considered network.

B. PROBABILITY OF NON-ZERO SECRECY CAPACITY

In wireless networks, channel quality may vary over time and frequency, which can be exploited opportunistically for secrecy transmission as long as the main channel is better than the eavesdropper channel. Therefore, we consider the probability of the non-zero secrecy capacity, which can be expressed as

$$\begin{aligned}\Pr\left(C_s > 0\right) &= \Pr\left(\tilde{\gamma}_B > \gamma_E\right)\\ &= \int_0^\infty F_{\gamma_E}(x) f_{\tilde{\gamma}_B}(x)\,dx. \end{aligned} \quad (19)$$

where $F_{\gamma_E}(x)$ is cumulative distributed function (CDF) of γ_E. Based on the statistical properties of each link, we can derive the probability of non-zero secrecy capacity in the following Theorem.

Theorem 1: The analytical expression of $\Pr\left(C_s > 0\right)$ *for imperfect CSI can be expressed as*

$$\begin{aligned}\Pr\left(C_s > 0\right)\\ &= \alpha_B^N \alpha_E^M \sum_{k=0}^{\infty} \frac{\Gamma(Mm_E + k)}{\Gamma(Mm_E)\,\Gamma(M+k)\,k!} \frac{\delta_E^k}{\beta_E^{k+M}}\\ &\quad \times \sum_{l=0}^{c} \binom{c}{l} \beta_B^{c-l} \left[I(x,l,d) + \varepsilon\delta_B I(x,l,d+1)\right], \end{aligned} \quad (20)$$

where $I(x,l,d)$ *is given by*

$$\begin{aligned} I(x,l,d)\\ &= \left(1+\frac{1}{L}\right)^{d-l} \frac{1}{\beta_B^{d-l}\,\Gamma(d)}\\ &\quad \times G_{3,3}^{2,2}\left[\Theta \middle| \begin{matrix} 1-d, 1-d+l-k-M, 1-d+l \\ 0, -d+l, 1-d+l \end{matrix}\right], \end{aligned} \quad (21)$$

where $\Theta = \left(1+\frac{1}{L}\right)\frac{(\beta_B - \delta_B)\bar{\gamma}_E}{\beta_E \bar{\gamma}_B}$ *and* $G_{p,q}^{m,n}[\cdot|\cdot]$ *is the Meijer-G function of single variable [34]*

Proof: See Appendix B. □

Remark 1: Please note that the Meijer-G function of single variable can be efficiently calculated by Matlab or Mathematic.

C. SECRECY OUTAGE PROBABILITY

The secrecy outage probability is defined as the probability that the secrecy capacity falls below a predefined rate R_s. Mathematically, it is given by

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s\right). \quad (22)$$

Based on (12), we can further rewrite (22) as

$$P_{out}\left(R_s\right) = \underbrace{\Pr\left(C_s < R_s \middle| \tilde{\gamma}_B > \gamma_E\right)\Pr\left(\tilde{\gamma}_B > \gamma_E\right)}_{I_1} + \underbrace{\Pr\left(\tilde{\gamma}_B < \gamma_E\right)}_{I_2}, \quad (23)$$

where the I_1 and I_2 can be calculated as

$$I_1 = \int_0^\infty \int_y^{2^{R_s}(1+y)-1} f_{\tilde{\gamma}_B}(x) f_{\gamma_E}(y)\,dxdy, \quad (24)$$

and

$$I_2 = \int_0^\infty \int_0^y f_{\tilde{\gamma}_B}(x) f_{\gamma_E}(y)\,dxdy. \quad (25)$$

Thus, utilizing (24) and (25) into (23) along with algebraic manipulations, we have

$$\begin{aligned} P_{out}\left(R_s\right) &= \int_0^\infty \int_0^{2^{R_s}(1+y)-1} f_{\tilde{\gamma}_B}(x) f_{\gamma_E}(y) dxdy\\ &= \int_0^\infty F_{\tilde{\gamma}_B}\left(2^{R_s}(1+y)-1\right) f_{\gamma_E}(y)\,dy. \end{aligned} \quad (26)$$

Capitalizing on (15) and utilizing the identity [41, eq. (13.1.32)] along with [42, eq. (2.19.5.3)], we get the CDF of $\tilde{\gamma}_B$ as

$$F_{\tilde{\gamma}_B} = \alpha_B^N \sum_{l=0}^{c} \binom{c}{l} \beta_B^{c-l} \left[Q(x,l,d) + \varepsilon\delta_B Q(x,l,d+1)\right], \quad (27)$$

where

$$Q\left(x,l,d\right)=\left(1+\frac{1}{L}\right)^{\frac{d-l-1}{2}}\frac{\left(\beta_B-\delta_B\right)^{\frac{l-d-1}{2}}}{\bar{\gamma}_B^{\frac{d-l-1}{2}}\Gamma\left(d-l+1\right)}x^{\frac{d-l-1}{2}}$$
$$\times\exp\left(-\left(1+\frac{1}{L}\right)\frac{\left(\beta_B-\delta_B\right)x}{2\bar{\gamma}_B}\right)$$
$$\times M_{\frac{d+l-1}{2},\frac{d-l}{2}}\left(\left(1+\frac{1}{L}\right)\frac{\left(\beta_B-\delta_B\right)x}{\bar{\gamma}_B}\right),\quad(28)$$

with $M_{a,b}\left(\cdot\right)$ being the Whittaker function [35, eq. (9.221)]. However, the exact secrecy outage probability can only be evaluated by using (27) and (17) into (26). Hence, we consider an alternative approach in the following derivation. By applying the identities [43, Appendix A6]

$$x^{\sigma}\exp\left(-\frac{x}{2}\right)M_{k,m}\left(x\right)$$
$$=\frac{\Gamma\left(2m+1\right)}{\Gamma\left(\frac{1}{2}+k+m\right)}$$
$$\times\sqrt{x}\mathrm{H}_{1,2}^{1,1}\left[x\left|\begin{matrix}\left(\frac{1}{2}+\sigma-k,1\right)\\\left(\sigma+m,1\right),\left(\sigma-m,1\right)\end{matrix}\right.\right],\quad(29)$$

and [43, eq. (1.2.4)]

$$x^k\mathrm{H}_{p,q}^{m,n}\left[x\left|\begin{matrix}\left(a_p,A_p\right)\\\left(b_q,B_p\right)\end{matrix}\right.\right]=\mathrm{H}_{p,q}^{m,n}\left[x\left|\begin{matrix}\left(a_p+k,A_p\right)\\\left(b_q+k,B_p\right)\end{matrix}\right.\right],\quad(30)$$

where $\mathrm{H}_{p,q}^{m,n}\left[\cdot\left|\cdot\right.\right]$ is the H-fox function, which can be transformed to the Meijer-G function as [43, eq. (1.7.1)]

$$\mathrm{H}_{p,q}^{m,n}\left[x\left|\begin{matrix}\left(a_p,1\right)\\\left(b_q,1\right)\end{matrix}\right.\right]=\mathrm{G}_{p,q}^{m,n}\left[x\left|\begin{matrix}a_p\\b_q\end{matrix}\right.\right],\quad(31)$$

Thus, combining (29)-(31), we can rewrite the $Q\left(x,l,d\right)$ in (28) into a simple form with respect to the Meijer-G function as

$$Q\left(x,l,d\right)$$
$$=\frac{\left(\beta_B-\delta_B\right)^{l-d}}{\Gamma\left(d\right)}$$
$$\times\mathrm{G}_{1,2}^{1,1}\left[\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\left|\begin{matrix}1-l\\d-l,0\end{matrix}\right.\right].\quad(32)$$

Subsequently, substituting (14), (27) and (32) into (26), we can obtain

$$P_{out}\left(R_s\right)=\alpha_B^N\alpha_E^M\sum_{l=0}^{c}\binom{c}{l}\beta_B^{c-l}$$
$$\times\left[J\left(R_s,l,d\right)+\varepsilon\delta_BJ\left(R_s,l,d+1\right)\right],\quad(33)$$

where

$$J\left(R_s,l,d\right)$$
$$=\frac{\left(\beta_B-\delta_B\right)^{l-d}}{\Gamma\left(d\right)\bar{\gamma}_E}$$
$$\times\int_0^{\infty}\exp\left(-\frac{\beta_Ey}{\bar{\gamma}_E}\right){}_1F_1\left(Mm_E;M;\frac{\delta_Ey}{\bar{\gamma}_E}\right)$$

$$\underbrace{\times\mathrm{G}_{1,2}^{1,1}\left[\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\frac{\left(2^{R_s}\left(1+y\right)-1\right)}{\bar{\gamma}_B}\left|\begin{matrix}1-l\\d-l,0\end{matrix}\right.\right]}_{\Phi}dy,$$
$$(34)$$

To solve the integral in (34), we apply the following identity [35, eq. (9.303)]

$$\mathrm{G}_{p,q}^{m,n}\left[x\left|\begin{matrix}a_1,\ldots,a_p\\b_1,\ldots,b_q\end{matrix}\right.\right]$$
$$=\sum_{h=1}^{m}\frac{\prod\limits_{j=1,j\neq h}^{m}\Gamma\left(b_j-b_h\right)\prod\limits_{j=1}^{n}\Gamma\left(1-b_h-a_j\right)}{\prod\limits_{j=m+1}^{q}\Gamma\left(1+b_h-b_j\right)\prod\limits_{j=n+1}^{p}\Gamma\left(a_j-b_h\right)}x^{b_h}$$
$$\times{}_pF_q\left(1+b_h-a_1,\ldots,1+b_h-a_p;1+b_h-b_1,\ldots,\right.$$
$$\left.1+b_h-b_q;\left(-1\right)^{p-m-n}x\right),\quad(35)$$

along with [35, eq. (9.14.1)], and obtain

$$\Phi=\sum_{k=0}^{\infty}\frac{\Gamma\left(d+k\right)}{\Gamma\left(1+d-l+k\right)k!\bar{\gamma}_B^k}\left(-\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\right)^{d-l+k}$$
$$\times\sum_{i=0}^{k}\binom{k}{i}\frac{2^{iR_s}y^i}{\left(2^{R_s}-1\right)^{i-k}}.\quad(36)$$

Therefore, by using (35) and (36) along with [35, eq. (7.813.1)], $J\left(x,l,d\right)$ can be derived as

$$J\left(R_s,l,d\right)$$
$$=\frac{\left(\beta_B-\delta_B\right)^{l-d}}{\Gamma\left(d\right)\Gamma\left(Mm_E\right)}\sum_{k=0}^{\infty}\frac{\Gamma\left(d+k\right)}{\Gamma\left(1+d-l+k\right)k!\bar{\gamma}_B^k}$$
$$\times\left(-\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\right)^{d-l+k}$$
$$\times\sum_{i=0}^{k}\binom{k}{i}\frac{2^{iR_s}\bar{\gamma}_E^i}{\left(2^{R_s}-1\right)^{i-k}\beta_E^{i+1}}\mathrm{G}_{2,2}^{1,2}$$
$$\times\left[-\frac{\delta_E}{\beta_E}\left|\begin{matrix}-i,1-Mm_E\\0,1-M\end{matrix}\right.\right]\quad(37)$$

To this end, the exact secrecy outage probability for the considered LMS system can be directly evaluated by substituting (37) into (34) along with some algebraic manipulations.

D. ASYMPTOTIC SECRECY OUTAGE PROBABILITY

Although the exact analytical expressions for secrecy outage probability have been derived for each scenario, it is still difficult to gain more insights form (33). Therefore, in what follows, we turn to derive the asymptotic secrecy outage probability at high SNR, i.e., $\bar{\gamma}_B\to\infty$, which can reveal two important performance metrics, namely the secrecy diversity order and secrecy array gain.

Using the series representation of Meijer-G function in (35) in conjunction with the property of hypergeometric function as [35]

$${}_pF_q\left(a_1,\ldots,a_p;b_1,\ldots,b_q;x\right)\to1\left(x\to0\right),\quad(38)$$

we get

$$F^{\infty}_{\tilde{\gamma}_B} = \alpha_B^N \sum_{l=0}^{c} \binom{c}{l} \beta_B^{c-l} \frac{1}{\Gamma\left(1+d-l\right)} \left(\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right)^{d-l}. \tag{39}$$

By letting $l = c$ in (39), $F^{\infty}_{\tilde{\gamma}_B}$ can be further simplified as

$$F^{\infty}_{\tilde{\gamma}_B} = \frac{\alpha_B^N}{\Gamma\left(1+N\right)} \left(\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right)^{N}. \tag{40}$$

Then, by substituting (40) and (17) into (26) along with [35, eq. (7.813.1)], the asymptotic secrecy outage probability for the considered LMS system can be calculated as

$$\begin{aligned} P^{\infty}_{out}\left(R_s\right) = {} & \frac{\alpha_B^N \alpha_E^M}{\Gamma\left(N+1\right)\Gamma\left(Mm_E\right)\bar{\gamma}_E \bar{\gamma}_B^N} \left(1+\frac{1}{L}\right)^{N} \\ & \times \sum_{i=0}^{N} \binom{N}{i} \frac{2^{iR_s}}{\left(2^{R_s}-1\right)^{i-N}} \left(\frac{\beta_E}{\bar{\gamma}_E}\right)^{-(i+1)} \\ & \times \mathrm{G}^{1,1}_{1,2}\left[-\frac{\delta_E}{\beta_E}\middle| \begin{matrix} -i, 1-Mm_E \\ 0, M \end{matrix}\right]. \end{aligned} \tag{41}$$

According to [21] and [22], we express the asymptotic secrecy outage probability expression into a general form in terms of the secrecy diversity order G_d and secrecy array gain G_a, namely

$$P^{\infty}_{out}\left(R_s\right) = \phi \bar{\gamma}_B^{-N} = \left(G_c \bar{\gamma}_B\right)^{-G_d}, \tag{42}$$

where ϕ can be written a

$$\begin{aligned} \phi = {} & \frac{\alpha_B^N \alpha_E^M}{\Gamma\left(N+1\right)\Gamma\left(Mm_E\right)\bar{\gamma}_E} \left(1+\frac{1}{L}\right)^{N} \\ & \times \sum_{i=0}^{N} \binom{N}{i} \frac{2^{iR_s}}{\left(2^{R_s}-1\right)^{i-N}}. \end{aligned} \tag{43}$$

Base on (42), the achievable secrecy diversity order and secrecy array gain can be directly obtained as

$$G_d = N, \tag{44}$$

and

$$G_a = \phi^{-\frac{1}{N}}. \tag{45}$$

Remark 2: As can be observed from (42), for the scenario with imperfect CSI estimation at Bob, the achievable secrecy diversity order remains N. This result indicates that the quality of channel estimation does not affect the secrecy diversity order. However, sending more training symbols L could significantly improve the secrecy performance by increasing the secrecy array gain. Also, when there exists imperfect CSI estimation at Bob, the channel qualities for both Bob and Eve only affect the secrecy array gain of the system.

TABLE 1. LMS channel parameters [39].

Shadowing	b_i	m_i	Ω_i
Frequent heavy shadowing (FHS)	0.063	0.739	8.97×10^{-4}
Average shadowing (AS)	0.126	10.1	0.835
Infrequent light shadowing (ILS)	0.158	19.4	1.29

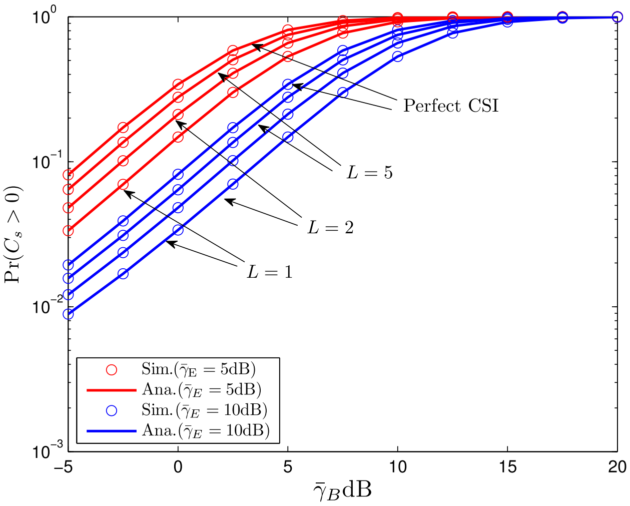


FIGURE 2. The probability of the non-zero secrecy capacity versus $\bar{\gamma}_B$ for different $\bar{\gamma}_E$.

IV. SIMULATION RESULTS

In this section, we provide representative simulation results to examine the impacts of various parameters on the secrecy performance of the considered network. Without loss of generality, we set the predefined rate $R_s = 1$, and the analytical curves are obtained by truncating the infinite series with 20-*th* terms. The simulation results are obtained by performing 10^6 channel realizations, and the different shadowing severities of the satellite links, including the frequent heavy shadowing (FHS), average shadowing (AS), and the infrequent light shadowing (ILS) are shown in Table 1.

Fig. 2 shows the probability of the non-zero secrecy capacity versus $\bar{\gamma}_B$ of the multiple antenna wiretap channels for different $\bar{\gamma}_E$, where we consider $N = 2$, and both main and eavesdropper are subject to the AS scenarios. As can be seen from the figure, the analytical results calculated from (17) are all in excellent agreement with the Monte Carlo simulations, which validates the accuracy of the theoretical derivations. With the increase of $\bar{\gamma}_E$, the probability of non-zero secrecy capacity significantly deceases, which indicates the detrimental effect of a more powerful eavesdropper. Besides, it can be noticed that the curves with imperfect CSI estimations gradually get close to the Perfect CSI cases by increasing the number of training symbols L. This observation suggests that by sending more training symbols, an improved CSI estimation can be achieved.

Fig. 3 examines the impact of antenna number of N on the secrecy outage probability of the system, where we consider $\bar{\gamma}_E = 5$dB and both the main and eavesdropper channels follow the AS scenarios. We can find that the analytical

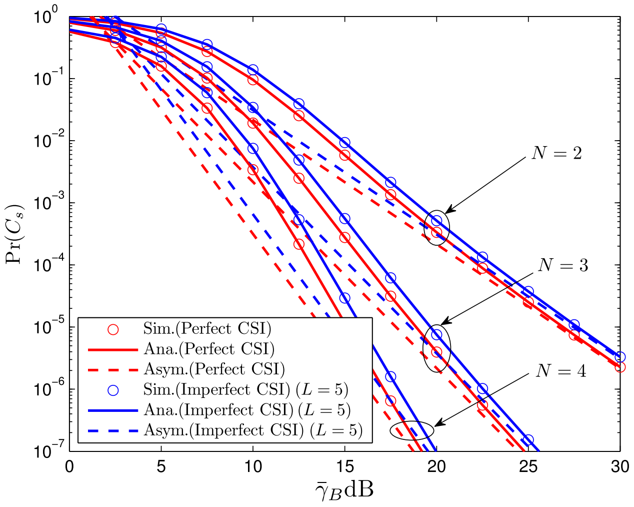


FIGURE 3. The secrecy outage probability versus $\bar{\gamma}_B$ for different antenna configurations.

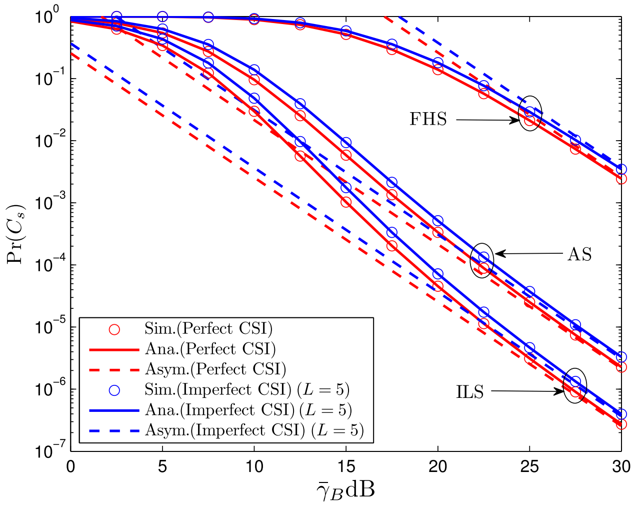


FIGURE 5. The secrecy outage probability versus $\bar{\gamma}_B$ for different shadowing severities of main channel.

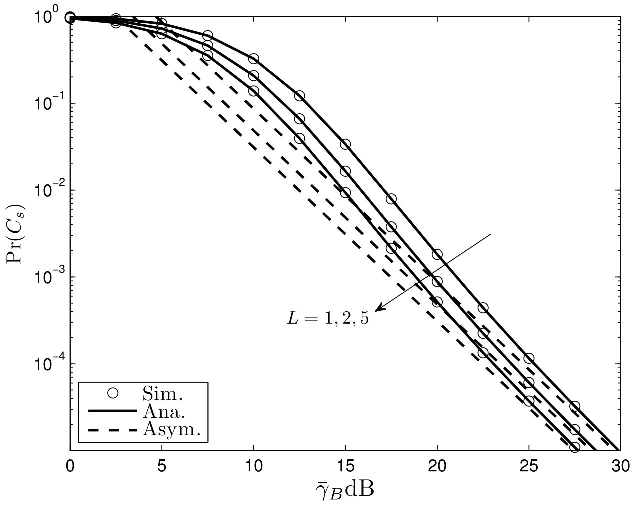


FIGURE 4. The secrecy outage probability versus $\bar{\gamma}_B$ for different number of training symbols *L*.

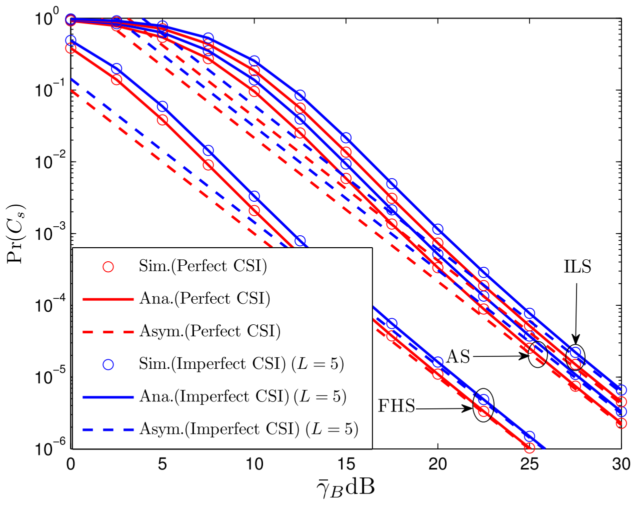


FIGURE 6. The secrecy outage probability versus $\bar{\gamma}_B$ for different shadowing severities of eavesdropper channel.

curves of secrecy outage probability agree well with simulation results with sufficient accuracy, and the asymptotic curves are very tight with the simulation results in high SNR regime, justifying the correctness and effectiveness of the derived expressions. In addition, for both perfect and imperfect CSI estimations, increasing the antenna number N can significantly improve the secrecy performance of the considered system by providing additional secrecy diversity order, which shows that full secrecy diversity order can be achieved for scenarios whether with perfect CSI estimations or not.

Fig. 4 illustrates the secrecy outage probability versus $\bar{\gamma}_B$ for different number of training symbols L with $N = 2$, $\bar{\gamma}_E = 5$dB and both Bob and Eves undergoing the AS cases. As indicated by the parallel slopes of the asymptotic curves, increasing L does not influence the achievable secrecy diversity order. However, an enhanced secrecy outage probability is achieved with the increase of training symbols. This is due to the fact that by sending more training symbols, the more accurate CSI estimation can be obtained at the Bob, which will increase the secrecy array gain.

Fig. 5 shows the impact of different fading severities of the main channel on the secrecy outage probability, where $N = 2$, $\bar{\gamma}_E = 5$dB and the Eves follow the AS. It can be found that the shadowing severities of main channel do not influence the achievable secrecy diversity order of the system. However, the secrecy performance will be enhanced by a weaker shadowing severity of the main channel due to the improve of the secrecy array gain.

Fig. 6 describes the secrecy outage probability versus $\bar{\gamma}_B$ for different shadowing severities of Eves' channel with $N = 2$, $\bar{\gamma}_E = 5$dB and AS for main channel. Apparently, the comparison between FHS, AS and ILS scenarios indicates that although the secrecy diversity order remains the same for all curves, the cases with Eve experiencing weaker shadowing severity lead to a worse secrecy performance.

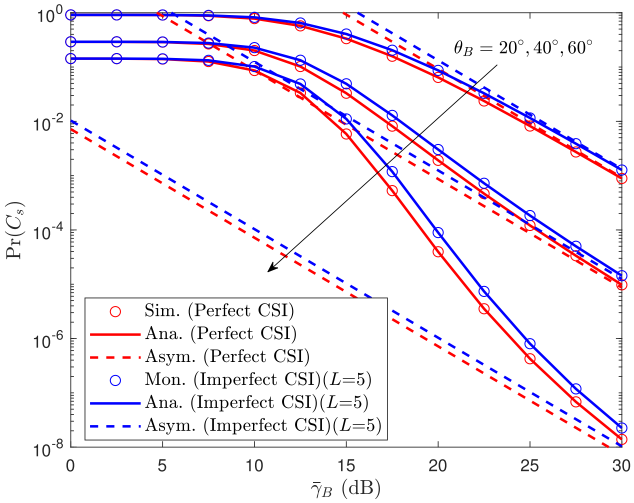


FIGURE 7. The secrecy outage probability versus $\bar{\gamma}_B$ for different elevation angles of main channel.

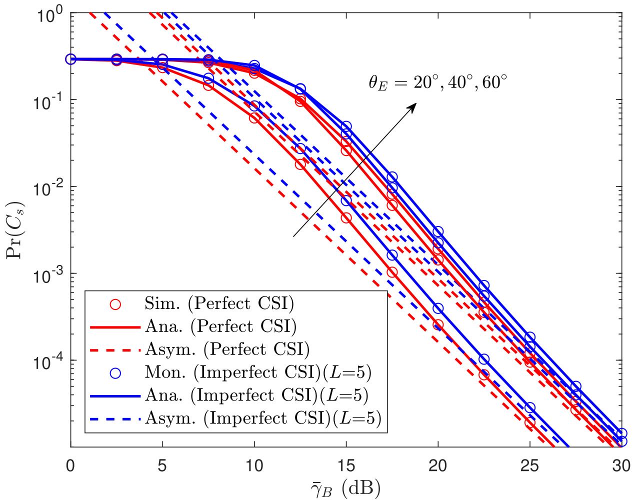


FIGURE 8. The secrecy outage probability versus $\bar{\gamma}_B$ for different elevation angles of eavesdropper channel.

This observation is consistent with the theoretical results that the secrecy performance will be degraded by a mild shadowing severity of the Eves' channel due to the detrimental impact on the secrecy array gain.

Fig. 7 illustrates the secrecy outage probability versus $\bar{\gamma}_B$ for different elevation angles of main channel with $N = 2$, $\bar{\gamma}_E = 5$dB and $\theta_E = 40°$ for Eves' channels. As can be observed, although the secrecy diversity order remains the same for different values of θ_B, the cases with Bob undergoing a higher elevation result in an improved secrecy outage probability. This can be explained the same as Remark 2, since the higher elevation is related to a weaker shadowing severity. Furthermore, as depicted in Fig. 8, we provide the secrecy outage probability versus $\bar{\gamma}_B$ for different elevation angles of Eves' channels with $N = 2$, $\bar{\gamma}_E = 5$dB and $\theta_B = 40°$ for main channels. On the contrary, with the increase of θ_E from 20° to 60°, the secrecy outage performance will be degraded as a weaker shadowing severity is presented.

V. CONCLUSIONS

In this paper, we investigated the secrecy performance of a multiple antenna LMS communication systems in the presence of eavesdropper over Shadowed-Rician fading channels, where the confidential messages send by a single antenna satellite to a multiple antenna legitimate BS with MRC diversity are overheard by a cluster of unauthorized eavesdropper. Specifically, considering only the imperfect CSI is available at Bob, we derived the analytical expressions for the probability of non-zero secrecy capacity and secrecy outage probability of the considered network. Moreover, simple asymptotic secrecy outage probability at high SNR was presented, which concisely characterizes the achievable secrecy diversity order and secrecy array gain. Numerical results were provided to validate the theoretical derivations, and show the impact of various key parameters on the secrecy performance of the system.

APPENDIX

PROOF OF THEOREM 1

As can be observed from (19), to obtain $\Pr\left(C_s > 0\right)$, we first need to derive the $F_{\gamma_E}(x)$. By applying the identity [35, eq. (9.14.1)],

$$ {}_pF_q\left(\alpha_1, \ldots, \alpha_p; \beta_1, \ldots, \beta_q; x\right) = \sum_{k=0}^{\infty} \frac{\left(\alpha_1\right)_k \cdots \left(\alpha_p\right)_k}{\left(\beta_1\right)_k \cdots \left(\beta_p\right)_k} \frac{x^k}{k!}, \tag{A.1} $$

where $(x)_n = x(x+1)(x+n-1) = \Gamma(x+n)/\Gamma(x)$ is the Pochhammer symbol [41], and the equation [35, eq. (3.351.1)], the CDF of γ_E can be written as

$$ F_{\gamma_E}(x) = \alpha_E^M \sum_{k=0}^{\infty} \frac{\Gamma(Mm_E + k)}{\Gamma(Mm_E)\Gamma(M+k)k!} \times \frac{\delta_E^k}{\beta_E^{k+M}} \gamma\left(k+M, \frac{\beta_E}{\bar{\gamma}_E}x\right), \tag{A.2} $$

where $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function [35, eq. (8.350.1)]. Then, using (A.2) and (15) into (19), we have

$$ \begin{aligned} &\Pr\left(C_s > 0\right) \\ &= \alpha_B^N \alpha_E^M \sum_{k=0}^{\infty} \frac{\Gamma(Mm_E + k)}{\Gamma(Mm_E)\Gamma(k+M)k!} \frac{\delta_E^k}{\beta_E^{k+M}} \\ &\quad \times \sum_{l=0}^{c} \binom{c}{l} \beta_B^{c-l} \left[I(l,d) + \varepsilon \delta_B I(l, d+1)\right], \end{aligned} \tag{A.3} $$

where $I(l,d)$ is given by

$$ \begin{aligned} &I(l,d) \\ &= \left(1+\frac{1}{L}\right)^{d-l} \int_0^{\infty} \frac{x^{d-l-1}}{\bar{\gamma}_B^{d-l}\Gamma(d-l)} \gamma\left(k+M, \frac{\beta_E}{\bar{\gamma}_E}x\right) \\ &\quad \times {}_1F_1\left(d; d-l; -\left(\beta_B - \delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right) dx. \end{aligned} \tag{A.4} $$

To obtain the analytical expression of the integral in (A.4), we first employ [42, eq. (8.4.16.1)] and

[35, eq. (8.455.1)] to express the incomplete gamma function $\gamma\left(k+M, \frac{\beta_E}{\bar{\gamma}_E}x\right)$ and confluent hypergeometric function ${}_1F_1\left(d; d-l; -\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right)$ in terms of Meijer-G function as

$$\gamma\left(k+M, \frac{\beta_E}{\bar{\gamma}_E}x\right) = \mathrm{G}^{1,1}_{1,2}\left[\frac{\beta_E}{\bar{\gamma}_E}x \,\middle|\, \begin{matrix}1\\ k+M, 0\end{matrix}\right], \quad (A.5)$$

and

$${}_1F_1\left(d; d-l; -\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\right) = \frac{\Gamma\left(d-l\right)}{\Gamma\left(d\right)} \times \mathrm{G}^{1,1}_{1,2}\left[-\left(\beta_B-\delta_B\right)\left(1+\frac{1}{L}\right)\frac{x}{\bar{\gamma}_B}\,\middle|\, \begin{matrix}1-d\\ 0, 1-d+l\end{matrix}\right], \quad (A.6)$$

where $\mathrm{G}^{m,n}_{p,q}\left[\cdot\,|\cdot\right]$ is the Meijer-G function of single variable [35]. Furthermore, using (A.5) and (A.6) into (A.4) along with [44, eq. (21)], we have

$$I\left(l,d\right) = \left(1+\frac{1}{L}\right)^{d-l}\frac{1}{\beta_B^{d-l}\Gamma\left(d\right)} \times \mathrm{G}^{2,2}_{3,3}\left[\left(1+\frac{1}{L}\right)\frac{\left(\beta_B-\delta_B\right)\bar{\gamma}_E}{\beta_E\bar{\gamma}_B}\,\middle| \cdots \begin{matrix}1-d, -d+l-k-M+1, -d+l+1\\ 0, -d+l, 1-d+l\end{matrix}\right]. \quad (A.7)$$

Thus, by substituting (A.7) into (A.4), we can obtain the closed-form expression of $\Pr\left(C_s>0\right)$ for the considered network as (20).

REFERENCES

[1] A. Vanelli-Coralli *et al.*, "Satellite communications: Research trends and open issues," in *Proc. Int. Workshop Satellite Space Commun.*, Sep. 2007, pp. 71–75.

[2] 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. doi: 10.1109/TAES.2018.2886611.

[3] 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.

[4] L. Liang, S. Iyengar, H. Cruickshank, and Z. Sun, "Security for FLUTE over satellite networks," in *Proc. Int. Conf. Commun. Mobile Comput.*, Kunming, China, Jan. 2009, pp. 485–491.

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

[8] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] 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.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2006, pp. 356–360.

[12] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[13] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[14] N. S. Ferdinand, D. B. da Costa, and M. Latva-Aho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 467–470, Oct. 2013.

[15] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[16] 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.

[17] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[18] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[19] N. S. Ferdinand, D. Benevides da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[20] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K. K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.

[21] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[22] J. Lei, Z. Han, M. 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.

[23] 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.

[24] 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.

[25] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassilio, "Secrecy capacity for satellite networks under rain fading," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 777–782, Sep./Oct. 2011.

[26] 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.

[27] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, to be published. doi: 10.1109/TVT.2019.2893366.Jan. 2019.

[28] 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.

[29] V. Bankey, P. K. Upadhyay, and D. B. da Costa, "Physical layer security of interference-limited land mobile satellite communication systems," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Marrakech, Morocco, Apr. 2018, pp. 1–5.

[30] S. Shi, K. An, G. Li, H. Zhu, and G. Zheng, "Optimal power control in cognitive satellite terrestrial networks with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 34–37, Feb. 2018.

[31] W. Lu, T. Liang, K. An, and H. Yang, "Secure beamforming and artificial noise algorithms in cognitive satellite-terrestrial networks with multiple eavesdroppers," *IEEE Access*, vol. 6, pp. 65760–65771, 2018.

[32] P. Arapoglou, K. Liolis, M. Bertinelli, A. Panagopoulos, P. Cottis, and R. D. Gaudenzi, "MIMO over satellite: A review," *IEEE Commun. Surveys Tut.*, vol. 13, no. 1, pp. 27–51, May 2011.

[33] V. Bankey, P. K. Upadhyay, D. B. da Costa, P. S. Bithas, A. G. Kanatas, and U. S. Dias, "Performance analysis of multi-antenna multiuser hybrid satellite-terrestrial relay systems for mobile services delivery," *IEEE Access*, vol. 6, pp. 24729–24745, 2018.

[34] 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.

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

[36] M. K. Arti and M. R. Bhatnagar, "Two-way mobile satellite relaying: A beamforming and combining based approach," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1187–1190, Jul. 2014.

[37] M. R. Bhatnagar, "Making two-way satellite relaying feasible: A differential modulation based approach," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2836–2847, Aug. 2015.

[38] M. K. Arti, "Channel estimation and detection in satellite communication systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10173–10179, Dec. 2016.

[39] 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.

[40] M. K. Arti, "Performance evaluation of maximal ratio combining in Shadowed-Rician fading land mobile satellite channels with estimated channel gains," *IET Commun.*, vol. 9, no. 16, pp. 2013–2022, Nov. 2015.

[41] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 10th ed. New York, NY, USA: Dover Publications, 1972.

[42] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals Ser*, vol. 3, 1st ed. New York, NY, USA: Gordon Breach Science Publishers, 1990.

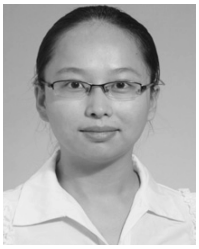
[43] A. M. Mathai and R. K. Saxena, *The H-Function with Applications in Statistics and Other Disciplines*. New York, NY, USA: Wiley, 1978.

[44] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce systems," in *Proc. Int. Conf. Symp. Algebr. Comput.*, Aug. 990, pp. 212–224.

YUSHENG LI received the M.S. degree from the Nanjing Institute of Communications Engineering, Nanjing, China, in 2000. He is currently a Senior Engineer with the Sixty-third Research Institute, National University of Defense Technology, and also with the Nanjing Telecommunication Technology Institute, Nanjing, China. His research interests include digital signal processing in communications and cognitive networks.

KANG AN (M'18) 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. He is currently an Engineer with the Sixty-third Research Institute, National University of Defense Technology, Nanjing, China. 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. He is currently a Research Fellow with the Sixty-Third Research Institute, National University of Defense Technology, Nanjing, and also with the Nanjing Telecommunication Technology Institute, China Electronic System Engineering Company. His research interests include satellite communication, digital signal processing in communications, physical layer security, cooperative communication, and cognitive networks.



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 was a Visiting Ph.D. Student with Heriot-Watt University, Edinburgh, U.K., from 2016 to 2017, under the supervision of Prof. C.-X. Wang. She is currently pursuing the Ph.D. degree with the School of Information and Communications, Guilin University of Electronic Technology, China, and also with the Engineering Training Center, Qinzhou University, China. Her current research interests include satellite-terrestrial networks, cooperative communications, and non-orthogonal multiple access.