Physical Layer Security of Interference-Limited Land Mobile Satellite Communication Systems

Vinay Bankey*, Prabhat K. Upadhyay*, and Daniel B. da Costa†
*Discipline of Electrical Engineering, Indian Institute of Technology Indore, Madhya Pradesh, India
†Department of Computer Engineering, Federal University of Ceará (UFC), Sobral, Ceará, Brazil
Email: {phd1501202007, pkupadhyay}@iiti.ac.in, danielbcosta@ieee.org

***Abstract*—In this paper, we investigate the secrecy performance of a downlink land mobile satellite (LMS) system, where a satellite transmits signal to a legitimate user in the presence of an eavesdropper at the ground. Herein, we consider that co-channel interference signals are present at the user destination node. By leveraging the statistics of underlying Shadowed-Rician fading channels for satellite links and Nakagami-*m* fading for interfering terrestrial links, we derive an accurate expression for secrecy outage probability (SOP) of the considered LMS system. To gain more insights, we derive an asymptotic expression for SOP at high signal-to-noise ratio regime and illustrate that system can attain a unity diversity order even under the influence of interferers. Subsequently, we also deduce the expression for probability of non-zero secrecy capacity. The analytical results are validated through Monte-Carlo simulations and utilized to reveal the impact of various key channel/system parameters in understanding the physical layer security aspects of LMS system.**

***Index Terms*—Physical layer security, land mobile satellite systems, co-channel interference, Shadowed-Rician fading, secrecy outage probability.**

I. Introduction

Land mobile satellite (LMS) systems are becoming more prevalent in the era of fifth-generation (5G) communications owing to their promising attributes such as broad coverage, navigation, high speed data transmission and inherent multicasting/broadcasting capabilities [1]. In LMS systems, satellite broadcasts signals to serve terrestrial mobile users over a wide area with low cost. The quality of service provided by such LMS systems firmly depends on the broadcasting link between the satellite and the mobile user [2]. Due to inherent broadcasting nature, satellite transmission systems are more vulnerable to suffer from eavesdropper's attacks, such as wiretapping. Therefore, security in LMS systems are becoming a more critical issue. Traditionally, security in satellite communication systems has been ensured by cryptography at upper layers [3], [4]. However, differing from traditional cryptographic techniques, the idea of physical layer security (PLS) has initially been proposed by Wyner [5], which exploits the characteristics of fading channels to improve the security performance. Basically, PLS depends on an information-theoretic metric defined as secrecy rate or secrecy capacity. Under this context, few recent works have analyzed the PLS of satellite networks [6]-[11], and these are briefly discussed next.

978-1-5386-4609-0/18/$31.00 ©2018 IEEE

In [6], authors have introduced PLS technique in satellite communication, where individual secrecy rate constraint was used as key metric to ensure the security. Later in [7], the secrecy performance of satellite communication networks was analyzed for different cases of Shadowed-Rician fading channel. Furthermore, PLS of satellite communication systems has been investigated in [8] and [9] under rain fading channel model. Specifically, the authors in [8] have examined the secrecy performance for satellite networks under rain attenuated environment conditions. While in [9], it was demonstrated that the security could be achieved in multibeam satellite systems through transmit beamforming optimization under rain fading channel. Moreover, authors in [10] have studied secrecy performance of a multi-relay satellite communication system. Authors in [11] have studied the PLS of a cognitive satellite network considering spectrum sharing technique. Although the above-mentioned literature laid a significant research for secrecy of satellite networks, very few works have investigated the secrecy performance of LMS systems [12], [13]. To be specific, in [12], the probability of secrecy outage and positive secrecy capacity have been obtained for LMS communication systems. Likewise in [13], authors have investigated the average secrecy capacity of LMS systems by considering multi-antenna terrestrial nodes. However, as far as the authors are aware, the impact of multiple terrestrial interferers on secrecy performance of LMS systems has not been investigated so far. In fact, a terrestrial user may exist in the intensive environment which causes co-channel interference (CCI) and thus affect communication system's performance adversely [14]-[16]. The terrestrial destination may get affected by CCI from other sets of users and/or earth stations existing nearby. Hence, it is important to analyze the impact of co-channel interferers on LMS systems for their potential deployment in 5G or beyond wireless networks [17].

With above motivation, in this paper, we study the secrecy performance of a LMS system in the presence of an eavesdropper, where the terrestrial user is inflicted by CCI. We derive a novel and accurate expression for secrecy outage probability (SOP) considering Shadowed-Rician fading channels for satellite links and Nakagami-*m* fading for terrestrial interference links. Note that the Shadowed-Rician channel model [1], [20] characterizes accurately the LMS communication channel, where a random line-of-sight (LOS) component follows Nakagami-m distribution with $0 \leq m \leq \infty$, while

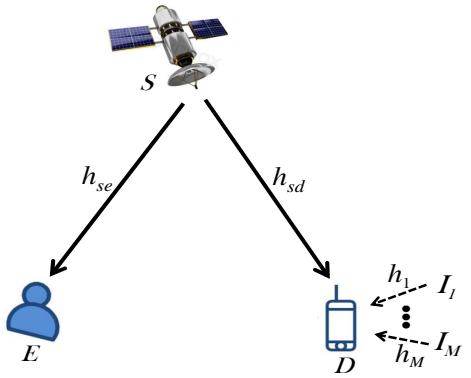

Fig. 1. LMS system model.

the multipath component follows the Rician fading. In the sequel, we study the diversity order of the considered system by computing the asymptotic SOP expression at high signal-to-noise ratio (SNR) regime. In addition, we also derive the expression for probability of non-negative secrecy capacity. Finally, analytical and simulation results are presented to corroborate our analysis and to reveal useful insights for secrecy performance of LMS systems.

II. LMS System Description

A. System Model

As shown in Fig. 1, we consider a downlink LMS system consisting of a satellite source S, a destination D, and an eavesdropper E. All nodes are equipped with a single antenna. The destination node is inflicted by M interferers $\{I_\imath\}_{\imath=1}^{M}$. The $S \to D$ link and $S \to E$ link are referred as main link and the wiretap link, respectively. Herein, we consider that both links experience the independent but non-identically distributed (i.ni.d.) Shadowed-Rician fading and they are inflicted by additive white Gaussian noise (AWGN) with zero mean and variance σ_j^2, for $j \in \{d, e\}$. Hereafter, we use subscript s for source node S, and subscripts d and e for receiving nodes D and E, respectively.

Satellite S transmits its signal x_s, satisfying $\mathbb{E}[|x_s|^2] = 1$, to destination D, where $\mathbb{E}[\cdot]$ represents the expectation operator. The received signal at D can be thus given by

$$y_d = \sqrt{P_s} h_{sd} x_s + \sum_{\imath=1}^{M} \sqrt{P_\imath} h_\imath x_\imath + n_d, \tag{1}$$

where P_s is the transmit power at source S, h_{sd} is the channel coefficient for $S \to D$ link, and n_d represents AWGN at destination D. Herein, $P_\imath$ is the power of the interferer $I_\imath$, $h_\imath$ is the channel coefficient between $\imath$th interferer and D, and $x_\imath$ is the transmitted signal (with unit energy) from $\imath$th interferer.

Meanwhile, eavesdropper E tries to overhear the transmitted signal from S. Thus, the received signal at E can be written as

$$y_e = \sqrt{P_s} h_{se} x_s + n_e, \tag{2}$$

where h_{se} is the channel coefficient between S and E, and n_e is the AWGN variable at E.

From (1), the instantaneous signal-to-interference-plus-noise ratio at destination D can be given as $\gamma_D = \frac{\gamma_{sd}}{\gamma_I + 1}$, where $\gamma_{sd} = \rho_d |h_{sd}|^2$, $\gamma_I = \sum_{\imath=1}^{M} \eta_\imath |h_\imath|^2$, with $\rho_d = \frac{P_s}{\sigma_d^2}$ and $\eta_\imath = \frac{P_\imath}{\sigma_d^2}$. Similarly from (2), the instantaneous SNR at eavesdropper E can be written as $\gamma_E = \rho_e |h_{se}|^2 \triangleq \gamma_{se}$, where $\rho_e = \frac{P_s}{\sigma_e^2}$. As such, we can define instantaneous capacity of the main channel (for destination) and of the wiretap channel (for eavesdropper) by $C_D = \frac{1}{2}\log_2(1 + \gamma_D)$ and $C_E = \frac{1}{2}\log_2(1 + \gamma_E)$, respectively. Thereby, the achievable secrecy capacity of the considered LMS system is given by the non-negative difference between the capacity of the main channel and the wiretap channel [18] as

$$C_{\text{sec}} = [C_D - C_E]^+, \tag{3}$$

where $[z]^+ \triangleq \max(z, 0)$. As the CSI of eavesdropper's channel is available with satellite [13], it can transmit confidential signals at a rate of C_{sec} to ensure perfect secrecy of the considered LMS system.

B. Channel Model

In this subsection, we illustrate the statistical characterization for the derivation of involved probability density function (PDF) and cumulative distribution function (CDF). As both the links (i.e., $S \to D$ and $S \to E$) follow independent Shadowed-Rician fading distribution, the PDF of the squared amplitude of the channel coefficient h_{sj} between satellite S and corresponding terrestrial node (i.e., destination D and eavesdropper E), for $j \in \{d, e\}$, is given by [1], [19]

$$f_{|h_{sj}|^2}(x) = \alpha_j \, \mathrm{e}^{-\beta_j x} \, {}_1F_1\left(m_j; 1; \delta_j x\right), \; x \geq 0, \tag{4}$$

where $\alpha_j = (2b_j m_j/(2b_j m_j + \Omega_j))^{m_j}/2b_j$, $\beta_j = 1/2b_j$, and $\delta_j = \Omega_j/(2b_j(2b_j m_j + \Omega_j))$ with Ω_j and $2b_j$ be the average power of LOS and multipath components, respectively, m_j is the fading severity parameter, and ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hypergeometric function of the first kind [25, eq. 9.210.1]. Since integer-valued fading parameter model is widely adopted in the literature [10], [20], we consider only the integer values of the fading severity parameters of the satellite links. In fact, the hypergeometric function can be represented via Kummer's transform [21] as

$${}_1F_1(a; b; x) = \mathrm{e}^x \sum_{n=0}^{a-b} \frac{(a-b)! x^n}{(a-b-n)! n! (b)_n}, \tag{5}$$

where $(\cdot)_n$ is the Pochhammer symbol [25, p. xliii]. Thereby, for integer m_j, we can simplify ${}_1F_1\left(m_j; 1; \delta_j x\right)$ in (4) using (5) to represent the PDF $f_{|h_{sj}|^2}(x)$ as [10]

$$f_{|h_{sj}|^2}(x) = \alpha_j \sum_{\kappa=0}^{m_j - 1} \psi_j(\kappa) x^\kappa \mathrm{e}^{-(\beta_j - \delta_j)x}, \tag{6}$$

where $\psi_j(\kappa) = (-1)^\kappa (1 - m_j)_\kappa \delta_j^\kappa / (\kappa!)^2$. The PDF of $\gamma_{sd} = \rho_d |h_{sd}|^2$ can be thus derived, by simply applying the transformation of variable, as

$$f_{\gamma_{sd}}(x) = \alpha_d \sum_{\kappa=0}^{m_d - 1} \frac{\psi_d(\kappa)}{(\rho_d)^{\kappa+1}} x^\kappa \mathrm{e}^{-\left(\frac{\beta_d - \delta_d}{\rho_d}\right)x}. \tag{7}$$

Similarly, the PDF of γ_{se} can be given as

$$f_{\gamma_{se}}(x) = \alpha_e \sum_{r=0}^{m_e - 1} \frac{\psi_e(r)}{(\rho_e)^{r+1}} x^r \mathrm{e}^{-\left(\frac{\beta_e - \delta_e}{\rho_e}\right)x}. \tag{8}$$

By integrating the PDF in (7) with the aid of [25, eq. 3.351.2], we can obtain the CDF of γ_{sd} as

$$F_{\gamma_{sd}}(x) = 1 - \alpha_d \sum_{\kappa=0}^{m_d-1} \frac{\psi_d(\kappa)}{(\rho_d)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta_d - \delta_d}{\rho_d}\right)^{-(\kappa+1-p)} \times x^p \mathrm{e}^{-\left(\frac{\beta_d-\delta_d}{\rho_d}\right)x}. \quad (9)$$

Now, we present the statistical characterization of terrestrial CCI links. As mentioned earlier, the interferer-destination links are assumed to undergo Nakagami-*m* fading. Hence, the derivation of exact PDF of γ_I is very complicated since it involves the sum of i.ni.d. Gamma random variables. Therefore, we use a highly accurate approximation method as proposed in [22] and [23], by which the PDF of γ_I can be given effectively to that of a single Gamma random variable as

$$f_{\gamma_I}(y) \approx \left(\frac{m_I}{\Omega_I}\right)^{m_I} \frac{y^{m_I-1}}{\Gamma(m_I)} \mathrm{e}^{-\frac{m_I}{\Omega_I}y}, \quad (10)$$

where the parameters m_I and Ω_I are calculated from moment-based estimators. Hereby, we define $\Phi = \sum_{\imath=1}^{M} |h_\imath|^2$. We assume no power control is used i.e., $P_\imath = P_I$ or $\eta_\imath = \eta_I$, for $\imath = 1, ..., M$. Then, we have $\Omega_I = \eta_I \mathbb{E}[\Phi]$ with $\mathbb{E}[\Phi] = \sum_{\imath=1}^{M} \Omega_\imath$ and $m_I = \frac{(\mathbb{E}[\Phi])^2}{\mathbb{E}[\Phi^2]-(\mathbb{E}[\Phi])^2}$. For this, the exact moments of Φ can be obtained in terms of the individual moments of the summands as

$$\mathbb{E}[\Phi^n] = \sum_{n_1=0}^{n} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{M-1}=0}^{n_{M-2}} \binom{n}{n_1}\binom{n_1}{n_2}\cdots\binom{n_{M-2}}{n_{M-1}} \times \mathbb{E}\left[|h_1|^{2(n-n_1)}\right]\mathbb{E}\left[|h_2|^{2(n_1-n_2)}\right]\cdots\mathbb{E}\left[|h_M|^{2(n_{M-1})}\right], \quad (11)$$

where

$$\mathbb{E}\left[|h_\imath|^n\right] = \frac{\Gamma\left(m_\imath + \frac{n}{2}\right)}{\Gamma(m_\imath)} \left(\frac{\Omega_\imath}{m_\imath}\right)^{\frac{n}{2}}. \quad (12)$$

III. Secrecy Performance Analysis

In this section, we first derive the SOP expression of the considered LMS system and then examine the achievable diversity order through asymptotic behavior of the SOP expression. Subsequently, we also analyze the probability of positive secrecy capacity.

A. Secrecy Outage Probability

The secrecy outage event is said to occur when the secrecy capacity falls below a predefined secrecy rate $\mathcal{R}_\mathrm{s}$. Thus, the SOP of the considered LMS system can be formulated as

$$\mathcal{P}_\mathrm{sec} = \Pr\left[C_\mathrm{sec} < \mathcal{R}_\mathrm{s}\right]. \quad (13)$$

On inserting C_sec from (3) in (13), $\mathcal{P}_\mathrm{sec}$ can be further represented as

$$\mathcal{P}_\mathrm{sec} = \Pr\left[\frac{1+\gamma_D}{1+\gamma_E} < \gamma_\mathrm{s}\right], \quad (14)$$

where $\gamma_\mathrm{s} = 2^{\mathcal{R}_\mathrm{s}}$. Thus, we can write SOP as

$$\mathcal{P}_\mathrm{sec} = \int_0^\infty F_{\gamma_D}(x\gamma_\mathrm{s} + \gamma_\mathrm{s} - 1) f_{\gamma_E}(x) dx. \quad (15)$$

To solve the integral in (15), we first require CDF of γ_D. Under the interference-limited scenario, γ_D can be simplified to $\gamma_D \simeq \frac{\gamma_{sd}}{\gamma_{Id}}$, and hence, $F_{\gamma_D}(x)$ can be given as

$$F_{\gamma_D}(x) = \int_0^\infty F_{\gamma_{sd}}(xy) f_{\gamma_I}(y) dy. \quad (16)$$

On invoking (9) and (10) in (16), we can calculate $F_{\gamma_D}(x)$ with the help of [25, eq. 3.351.3], which is given as

$$F_{\gamma_D}(x) = 1 - \alpha_d \sum_{\kappa=0}^{m_d-1} \frac{\psi_d(\kappa)}{(\rho_d)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta_d - \delta_d}{\rho_d}\right)^{-(\kappa+1-p)} \times x^p \left(\frac{m_I}{\Omega_I}\right)^{m_I} \frac{\Gamma(p+m_I)}{\Gamma(m_I)} \left(\frac{\beta_d-\delta_d}{\rho_d}x + \frac{m_I}{\Omega_I}\right)^{-(p+m_I)}. \quad (17)$$

Finally, by substituting (17) and (8) into (15), performing the simplification using the identity of Meijer's G-function [25, eq. 9.3] as

$$(1+ax)^{-k} = \frac{1}{\Gamma(k)} G^{1,1}_{1,1}\left[ax\middle|\begin{matrix}1-k\\0\end{matrix}\right], \quad (18)$$

and then solving the integration with the aid of [25, eq. 7.813.1], we obtain SOP as given in (19), shown at the top of the next page, where $\chi_d = \left(\frac{\beta_d-\delta_d}{\rho_d}(\gamma_\mathrm{s}-1) + \frac{m_I}{\Omega_I}\right)$.

B. Asymptotic Analysis

To examine the diversity order of system, we perform an asymptotic analysis of SOP at high SNR regime (i.e., assuming $\rho_d \to \infty$). Thus, to evaluate (15), we require the asymptotic expression of $F_{\gamma_D}(x)$. For this, first we apply Maclaurin series expansion as $\mathrm{e}^{-z} \underset{z\to 0}{\simeq} 1 - z$ in (7) and use only initial term since higher order terms tend to zero. Consequently, the PDF in (7) at high SNR follows

$$f_{\gamma_{sd}}(x) \simeq \frac{\alpha_d}{\rho_d} + o(x). \quad (20)$$

and the corresponding CDF can be obtained by integrating (20) as

$$F_{\gamma_{sd}}(x) \simeq \frac{\alpha_d}{\rho_d} x. \quad (21)$$

Further, invoking (21) and (10) in (16), $F_{\gamma_D}(x)$ can be evaluated as

$$F_{\gamma_D}(x) \simeq \frac{\alpha_d x}{\rho_d} \left(\frac{\Omega_I}{m_I}\right) \frac{\Gamma(m_I+1)}{\Gamma(m_I)}. \quad (22)$$

Now, inserting (22) and (8) in (15), and using [24, eq. (24)], the asymptotic expression for SOP can be obtained as

$$\mathcal{P}^\infty_\mathrm{sec} \simeq \frac{\alpha_d}{\rho_d}\Omega_I \left[(\gamma_\mathrm{s}-1) + \gamma_\mathrm{s}\alpha_e \sum_{r=0}^{m_e-1} \frac{\psi_e(r)}{(\rho_e)^{r+1}} \times (r+1)! \left(\frac{\beta_e-\delta_e}{\rho_e}\right)^{-(r+2)}\right]. \quad (23)$$

Remarks: Our asymptotic analysis of SOP reveals that the system attains a diversity order of unity. Importantly, the diversity order is not influenced by the fading severity parameters of satellite links and the co-channel interferers.

C. Existence of Non-zero Secrecy Capacity

Here, we calculate the probability for existence of non-zero secrecy capacity. Non-zero secrecy event occurs when the main $(S \to D)$ link is better than the eavesdropper $(S \to E)$ link, which is given by

$$\mathcal{P}(C_\mathrm{sec} > 0) = \Pr\left[\gamma_D > \gamma_E\right] = 1 - \int_0^\infty F_D(x) f_{\gamma_E}(x) dx. \quad (24)$$

After substituting (17) and (8) into (24), the probability for existence of non-zero secrecy capacity can be computed and

$$\mathcal{P}_{\text{sec}} = 1 - \alpha_d \sum_{\kappa=0}^{m_d-1} \frac{\psi_d(\kappa)}{(\rho_d)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta_d - \delta_d}{\rho_d}\right)^{-(\kappa+1-p)} \left(\frac{m_I}{\Omega_I}\right)^{m_I} \frac{1}{\Gamma(m_I)} \sum_{q=0}^{p} \binom{p}{q} \gamma_{\text{s}}^q \left(\gamma_{\text{s}} - 1\right)^{p-q} \chi_d^{-(p+m_I)}$$
$$\times \alpha_e \sum_{r=0}^{m_e-1} \frac{\psi_e(r)}{(\rho_e)^{r+1}} \left(\frac{\beta_e - \delta_e}{\rho_e}\right)^{-(q+r+1)} G_{2,1}^{1,2}\left[\frac{\frac{\beta_d-\delta_d}{\rho_d}\gamma_{\text{s}}}{\frac{\beta_e-\delta_e}{\rho_e}\chi_d}\middle| \begin{matrix} -(q+r), 1-(p+m_I) \\ 0 \end{matrix}\right]. \quad (19)$$

TABLE I
VALUES OF THE PARAMETERS ESTIMATED FOR THE INTERFERING SIGNALS

No. of interferers	2	3	4	5
m_I	2.9697	5.4340	8.4317	11.9136
Ω_I	3.5	6	9.2	12.7

given as

$$\mathcal{P}(C_{\text{sec}} > 0) = \alpha_d \sum_{\kappa=0}^{m_d-1} \frac{\psi_d(\kappa)}{(\rho_d)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta_d - \delta_d}{\rho_d}\right)^{-(\kappa+1-p)}$$
$$\times \left(\frac{\Omega_I}{m_I}\right)^{p} \frac{\alpha_e}{\Gamma(m_I)} \sum_{r=0}^{m_e-1} \frac{\psi_e(r)}{(\rho_e)^{r+1}} \left(\frac{\beta_e - \delta_e}{\rho_e}\right)^{-(r+1)}$$
$$\times G_{2,1}^{1,2}\left[\frac{(\beta_d - \delta_d)\rho_e \Omega_I}{(\beta_e - \delta_e)\rho_d m_I}\middle| \begin{matrix} -r, 1-(p+m_I) \\ 0 \end{matrix}\right]. \quad (25)$$

In deriving (25), we have used the identity of Meijer's G-function from (18) and [25, eq. 7.813.1].

IV. Numerical and Simulation Results

In this section, we perform the numerical investigations to highlight the secrecy performance of the considered LMS system. For this, we assume that the $S \to D$ and $S \to E$ links follow Shadowed-Rician fading and may experience heavy shadowing (HS) with parameters $(m_j, b_j, \Omega_j) = (1, 0.063, 0.0007)$ and average shadowing (AS) with parameters $(m_j, b_j, \Omega_j) = (5, 0.251, 0.279)$ [20]. Moreover, the channel parameters of interference links are assigned as $\{m_i\}_{i=1}^{5} = \{1, 2, 2.5, 3, 3.5\}$ and $\{\Omega_i\}_{i=1}^{5} = \{1, 2.5, 2.5, 3.2, 3.5\}$. For each set of multiple interfering signals, the required parameters in (10) are computed and illustrated in Table I. To show the impact of interferers on the secrecy performance, we consider M number of interferers at destination node. We fix the interference power $\eta_I = 1$ dB throughout our analysis. Monte-Carlo simulation results are also provided to validate our theoretical analysis.

Fig. 2 shows the SOP curves of considered system for different shadowing scenarios of main (i.e., $S \to D$) and wiretap (i.e., $S \to E$) links. Analytical and asymptotic curves are plotted using (19) and (23), respectively, and they are found to be well aligned at high SNR. Herein, we plot the SOP curves for four possible different cases with two shadowing scenarios (i.e., AS and HS). For this, we set secrecy rate $\mathcal{R}_{\text{s}} = 0.5$, $\rho_e = 2$ dB, and number of interferers $M = 2$. Specifically, we can observe that system gives better performance for the case when $S \to D$ link experiences AS and $S \to E$ link experiences HS. On the other hand, system SOP performance goes worsen when $S \to D$ and $S \to E$ links undergo HS and AS, respectively. Moreover, it is apparent from slopes of the curves that system attains diversity order of one.

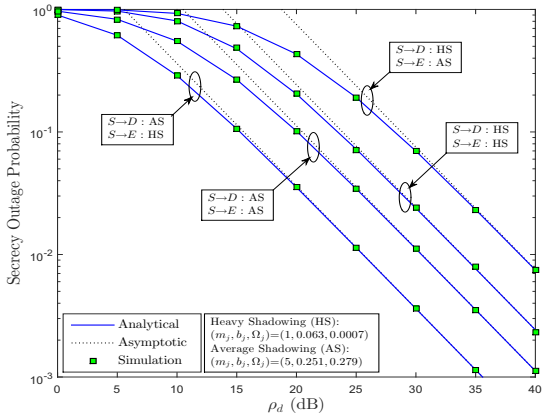

Fig. 2. SOP performance versus ρ_d for different shadowing scenarios.

More importantly, it is found that the diversity order remains unaffected from fading severity parameters of the satellite channels.

Fig. 3 illustrates the impact of multiple interferers on system's SOP performance. Herein, we set $\mathcal{R}_{\text{s}} = 0.5$, $\rho_e = 2$ dB, and we also consider that both the links (i.e., $S \to D$ and $S \to E$) undergo HS. One can observe that the SOP performance of the considered LMS system improves with decreasing number of interferers at destination. For example, better secrecy performance can be realized with less number of interferers at destination as clear from the curves for $M = 1$ as compared to $M = 5$. However, the system diversity order remains unaffected from the number of co-channel interferers.

In Fig. 4, we depict the probability of non-zero secrecy capacity for various values of ρ_e. For this, we have fixed $\mathcal{R}_{\text{s}} = 0.5$ and $M = 3$. The curves are drawn using (25) by considering that both main and wiretap links experience HS. This figure highlights the effect of ρ_e on secrecy performance. As expected, the probability of non-zero secrecy capacity increases with decrease in the eavesdropper's average SNR ρ_e and attains maximum value at high SNR which is reflected clearly by the curves.

V. Conclusion

This paper has investigated the secrecy performance of a downlink LMS system in the presence of CCI at terrestrial user. We derived accurate and asymptotic SOP expressions for the considered system. We characterized the system diversity order and deduced that it remains unaffected by the fading severity parameters of satellite links and the number of co-channel interferers. Furthermore, we derived the expression

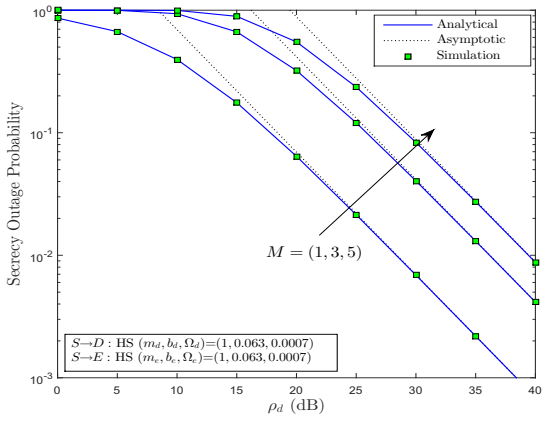

Fig. 3. Impact of different number of interferers on SOP performance.

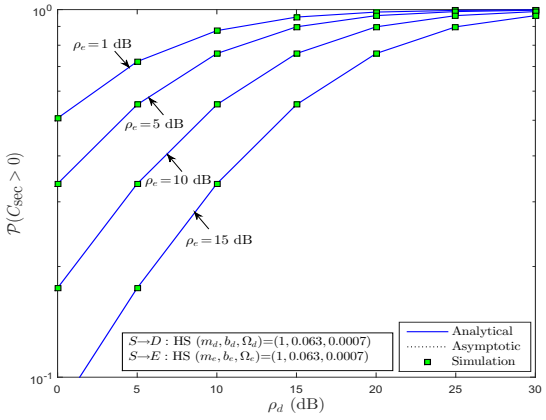

Fig. 4. Probability of positive secrecy capacity for different values of ρ_e.

for probability of non-zero secrecy capacity. Finally, numerical results are provided to vindicate the analytical derivations and enlightened the impact of various key parameters on secrecy performance of the considered LMS system. Moreover, deployment of a multi-antenna satellite with multi-user configuration could be a crucial study for future investigation.

ACKNOWLEDGMENT

This Publication is an outcome of the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology (MeitY), Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia). It was also partly supported by FUNCAP, Edital PRONEM 01/2016.

REFERENCES

[1] A. Abdi, W. 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.

[2] E. Lutz, D. Cygan, M. Dippold, F. Dolainsky, and W. Papke, "The land mobile satellite communication channel-recording, statistics, and channel model," *IEEE Trans. Veh. Technol.*, vol. 40, no. 2, pp. 375-386, May 1991.

[3] N. Sklavos and X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*, 1st ed. Baco Raton, FL, USA: CRC Press, 2007.

[4] H. Cruickshank, M. 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.

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

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

[7] K. Guo, B. Zhang, Y. Huang, and D. Guo, "Secure performance analysis of satellite communication networks in Shadowed-Rician channel," in *Proc. IEEE Int. Symp. on Signal Processing and Inf. Tech. (ISSPIT)*, Limassol, Cyprus, Dec. 2016.

[8] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassiliou, "Secrecy capacity for satellite networks under rain fading," *IEEE Trans. Depend. Secu. Comp.*, vol. 8, no. 5, pp. 777-782, Sep. 2011.

[9] 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.

[10] V. Bankey and P. K. Upadhyay, "Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC)*, Sydney, Australia, June 2017.

[11] K. An, M. Lin, J. Ouyang, and W.-P. Zhu, "Secure transmission in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 3025-3037, Nov. 2016.

[12] 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 and Optical Commun. Conf. (WOCC)*, Chengdu, China, May 2016.

[13] K. An, M. Lin, T. Liang, J. Ouyang, and H. Chen, "Average secrecy capacity of land mobile satellite wiretap channels," in *Proc. Wireless Commun. and Signal Processing (WCSP)*, Yangzhou, China, Oct. 2016.

[14] L. Yang and M. O. Hasna, "Performance analysis of amplify-and-forward hybrid satellite-terrestrial networks with cochannel interference," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5052-5061, Dec. 2015.

[15] P. K. Upadhyay and P. K. Sharma, "Multiuser hybrid satellite-terrestrial relay networks with co-channel interference and feedback latency," in *Proc. European Conf. on Netw. and Commun. (EuCNC)*, Athens, Greece, June 2016, pp. 174-178.

[16] V. Bankey and P. K. Upadhyay, "Ergodic capacity of multiuser hybrid satellite-terrestrial fixed-gain AF relay networks with CCI and outdated CSI," *IEEE Trans. Veh. Technol.*, 2018, DOI: 10.1109/TVT.2018.2793420.

[17] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065-1082, June 2014.

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

[19] M. R. Bhatnagar and Arti M. K., "Performance analysis of AF based hybrid satellite-terrestrial cooperative network over generalized fading channels," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 1912-1915, Oct. 2013.

[20] 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.

[21] G. Alfano and A. De Maio, "Sum of squared Shadowed-Rice random variables and its application to communication systems performance prediction," *IEEE Trans. Wireless Commun.*, vol. 6, no. 10, pp. 3540-3545, Oct. 2007.

[22] D. B. da Costa, H. Ding, and J. Ge, "Interference-limited relaying transmissions in dual-hop cooperative networks over Nakagami-m fading," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 503-505, May 2011.

[23] J. C. S. Santos Filho and M. D. Yacoub, "Nakagami-m approximation to the sum of M non-identical independent Nakagami-m variates," *Electron. Lett.*, vol. 40, no. 15, pp. 951-952, July 2004.

[24] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," in *Proc. Int. Symp. Symbolic and Algebraic Computation (ISSAC)*, Tokyo, Japan, Aug. 1990, pp. 212-224.

[25] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series and Products*, 6th ed. New York: Academic Press, 2000.