CSIT (June 2018) 6(2):187–193
https://doi.org/10.1007/s40012-018-0200-5

S.I. : VISVESVARAYA

Physical layer secrecy performance analysis of multi-user hybrid satellite-terrestrial relay networks

Vinay Bankey[1] · **Prabhat K. Upadhyay**[1]

Received: 16 May 2018 / Accepted: 7 June 2018 / Published online: 18 June 2018

Abstract This paper investigates the secrecy performance of a downlink multi-user amplify-and-forward hybrid satellite-terrestrial relay network (HSTRN) with opportunistic scheduling of terrestrial users. By considering Shadowed-Rician fading for satellite link and Nakagami-*m* fading for terrestrial links, we derive accurate and asymptotic expressions for secrecy outage probability (SOP). Based on the asymptotic behaviour of SOP expression at high signal-to-noise ratio regime, we illustrate practical insights on the achievable diversity order of the system. Subsequently, we also deduce the expression for probability of non-zero secrecy capacity. Finally, numerical and simulation results are provided to vindicate our analysis and to show the impact of various key channel/system parameters such as shadowing severity and number of users on the physical layer secrecy performance of HSTRNs.

Keywords Amplify-and-forward · Hybrid satellite-terrestrial relay network (HSTRN) · Nakagami-*m* fading · Physical layer security · Secrecy outage probability · Shadowed-Rician fading

1 Introduction

Satellite communication has gained enormous popularity in the era of fifth-generation (5G) communications owing to its advantages in various applications such as defence, disaster relief, and navigation [1]. Recently, satellite communication systems have shown a great interest of research in the wireless society due to their capability of providing seamless connectivity and high data rate transmission over a wide coverage area [2]. However, masking effect may result due to severe shadowing and heavy obstacles between the satellite and terrestrial users which causes unavailability of the line-of-sight (LOS) communication [3]. To overcome this problem, researchers have conceived the cooperation of terrestrial relay into satellite communication systems to form a new architecture defined as hybrid satellite-terrestrial relay network (HSTRN) [3, 4]. Such systems mainly exploits cooperative relaying technique in an integrated manner to enhance the reliability and coverage performance, especially in subterranean and indoor environment. A new generation standard known as DVB-SH [5] incorporates the framework of HSTRN to provide Satellite services to Handheld devices (SH).

In recent years, many research efforts have been devoted towards improvement of the performance of HSTRN [6–12]. However, the transmission security aspects are hardly examined for the HSTRN. The information security is one of the major problems in the wireless communication. In the beginning, cryptography techniques were used at upper layers to ensure the security in satellite communication systems [13]. On the contrary, Wyner in [14] has proposed an information-theoretic approach to achieve physical layer security that exploits the characteristics of fading channels. In the context of physical layer security, very limited works have investigated the secrecy performance of the HSTRN [15–18]. In [15], authors have studied maximum ratio combining and transmit zero-forcing beamforming based schemes to ensure the secrecy of a multiple eavesdropper HSTRN. Secrecy performance analysis of a multi-relay HSTRN configuration has been

✉ Vinay Bankey
phd1501202007@iiti.ac.in

Prabhat K. Upadhyay
pkupadhyay@iiti.ac.in

[1] Discipline of Electrical Engineering, Indian Institute of Technology Indore, Indore, Madhya Pradesh 453552, India

examined in [16] and [17], where optimal relay section scheme was studied to select the best relay and to enhance security of the considered system. Moreover, physical layer security of a cognitive HSTRN by considering underlay spectrum sharing technique has been examined in [18]. As far as authors are aware, the secrecy performance analysis of a multi-user HSTRN configuration has not been addressed so far. The main purpose of this paper is to analyse a multi-user HSTRN and to highlight the impact of key parameters on the secrecy performance and achievable diversity order of such system. In fact, the deployment of multiple users makes the proposed configuration more favorable for practical applications.

In light of the above discussion, we conduct a comprehensive secrecy performance analysis of a downlink multi-user amplify-and-forward (AF) based HSTRN by employing opportunistic scheduling of terrestrial users. By adopting Shadowed-Rician fading for satellite link and Nakagami-m fading for terrestrial links, we derive an accurate and asymptotic secrecy outage probability (SOP) expressions which are applicable for arbitrary number of users and arbitrary integer values of the fading severity parameters over the two hops. The asymptotic SOP expression helps us in examining the achievable diversity order of the considered HSTRN. We found that the achievable diversity order of the considered system depends on the fading severity parameter of the relay-destinations links and number of terrestrial users while it remains unaffected by the fading severity parameter of satellite link. We also evaluate the expression for probability of non-zero secrecy capacity of the considered system. We validate our analysis with the help of Monte-Carlo simulation results.

The remainder of this paper is organized as follows. In Sect. 2, we first introduce the system model and then describe the heterogeneous channel models. Further, we perform secrecy performance analysis in Sect. 3. Section 4 presents the numerical and simulation results, and finally, the conclusions are given in Sect. 5.

2 HSTRN description

2.1 System model

As shown in Fig. 1, we consider a downlink HSTRN consisting of a satellite source S, an AF relay R, N destinations $\{D_n\}_{n=1}^{N}$, and an eavesdropper E. All nodes are equipped with a single antenna. The LOS links between S and $\{D_n\}_{n=1}^{N}$ as well as between S and E are not available owing to the masking effect. Therefore, S communicates with $\{D_n\}_{n=1}^{N}$ via a terrestrial AF relay R in the presence of eavesdropper E. The satellite link (i.e., $S \rightarrow R$ link) is

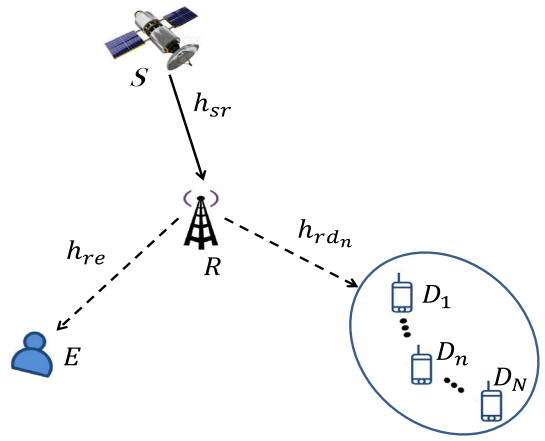

Fig. 1 System model: HSTRN

assumed to undergo Shadowed-Rician fading while terrestrial links (i.e., $R \rightarrow D_n$ and $R \rightarrow E$ links) experience Nakagami-m fading. All the receiving nodes are inflicted by additive white Gaussian noise (AWGN) with zero mean and variance σ^2. Herein, the $S \rightarrow R \rightarrow D_n$ and $S \rightarrow R \rightarrow E$ links are referred to as the main and the wiretap links, respectively.

The overall communication takes place in two time phases by employing an opportunistic user scheduling scheme. In first phase, the satellite source S transmits its signal x_s (with unit energy) to the relay R. Thus, the received signal at R can be given by

$$y_{sr} = \sqrt{P_s} h_{sr} x_s + n_r, \tag{1}$$

where P_s is the transmit power at S, h_{sr} is the channel coefficient between S and R, and n_r is the AWGN at R.

In the second phase, the relay R first amplifies the received signal y_{sr} using a gain factor G and then forwards it to the selected destination D_n. Meanwhile, the eavesdropper tries to overhear the signal transmitted from relay. Therefore, the signals received at destination D_n and eavesdropper E can be given, respectively, as

$$y_{rd_n} = \sqrt{P_r} h_{rd_n} G\, y_{sr} + n_{d_n} \tag{2}$$

and

$$y_{re} = \sqrt{P_r} h_{re} G\, y_{sr} + n_e, \tag{3}$$

where P_r is the transmit power at relay R, h_{rd_n} and h_{re} denote the respective channel coefficients for $R \rightarrow D_n$ and $R \rightarrow E$ links, while n_{d_n} and n_e represent the AWGN variables at the respective nodes.

Based on (2) and (3), the instantaneous received signal-to-noise ratios (SNRs) at D_n and E can be obtained, respectively, as

$$\gamma_{D_n} = \frac{\gamma_{sr}\gamma_{rd_n}}{\gamma_{rd_n} + \frac{1}{G^2\sigma^2}} \tag{4}$$

and

$$\gamma_E = \frac{\gamma_{sr}\gamma_{re}}{\gamma_{re} + \frac{1}{G^2\sigma^2}}, \tag{5}$$

where $\gamma_{sr} = \eta_s|h_{sr}|^2$, $\gamma_{rd_n} = \eta_r|h_{rd_n}|^2$, and $\gamma_{re} = \eta_r|h_{re}|^2$ with $\eta_s = \frac{P_s}{\sigma^2}$ and $\eta_r = \frac{P_r}{\sigma^2}$. For variable gain relaying, the gain factor G in (4) and (5) can be determined as

$$G = \sqrt{\frac{1}{P_s|h_{sr}|^2 + \sigma^2}}, \tag{6}$$

and thus, the instantaneous end-to-end SNRs at D_n and E can be given, respectively, as

$$\gamma_{D_n} = \frac{\gamma_{sr}\gamma_{rd_n}}{\gamma_{sr} + \gamma_{rd_n} + 1}, \tag{7}$$

and

$$\gamma_E = \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr} + \gamma_{re} + 1}. \tag{8}$$

To harness the multiuser diversity in the considered network, we utilize the opportunistic scheduling scheme, where the relay select the best user based on the highest instantaneous SNR of $R \rightarrow D_n$ links as

$$\gamma_{rd} = \max_{1 \le n \le N} \gamma_{rd_n}. \tag{9}$$

Hence, the actual SNR with the scheduled user can be written as

$$\gamma_D = \frac{\gamma_{sr}\gamma_{rd}}{\gamma_{sr} + \gamma_{rd} + 1}. \tag{10}$$

As such, we can define instantaneous capacity of the main link and of the wiretap link 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 HSTRN is given by the positive difference between the capacity of the main link and capacity of the wiretap link [19] as

$$\begin{aligned} C_S &= [C_D - C_E]^+ \\ &= \left[\frac{1}{2}\log_2(1+\gamma_D) - \frac{1}{2}\log_2(1+\gamma_E)\right]^+, \end{aligned} \tag{11}$$

where $[a]^+ \triangleq \max(a, 0)$.

2.2 Channel model

In this subsection, we illustrate the statistical characterization for fading channels of each hop. As the satellite link (i.e., $S \rightarrow R$) follows independent Shadowed-Rician fading distribution, the probability density function (PDF) of $|h_{sr}|^2$ between satellite S and relay R is given by [6, 20]

$$f_{|h_{sr}|^2}(x) = \alpha_s\, \mathrm{e}^{-\beta_s \mathrm{x}}\, {}_1\mathrm{F}_1(\mathrm{m_s}; 1; \delta_s \mathrm{x}),\ \ \mathrm{x} \ge 0, \tag{12}$$

where $\alpha_s = (2b_s m_s/(2b_s m_s + \Omega_s))^{m_s}/2b_s$, $\beta_s = 1/2b_s$, and $\delta_s = \Omega_s/(2b_s(2b_s m_s + \Omega_s))$ with Ω_s and $2b_s$ be the average power of LOS and multipath components, respectively, m_s 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]. We consider only the integer values of the fading severity parameter of the satellite link [16, 21]. Thus, the hypergeometric function can be represented via Kummer's transform [22] as

$${}_1F_1(a; b; x) = \mathrm{e}^{\mathrm{x}} \sum_{\mathrm{n}=0}^{\mathrm{a}-\mathrm{b}} \frac{(\mathrm{a}-\mathrm{b})!\mathrm{x}^{\mathrm{n}}}{(\mathrm{a}-\mathrm{b}-\mathrm{n})!\mathrm{n}!(\mathrm{b})_{\mathrm{n}}}, \tag{13}$$

where $(\cdot)_n$ is the Pochhammer symbol [25, p. xliii]. Thereby, for integer m_s, we can simplify ${}_1F_1(m_s; 1; \delta_s x)$ in (12) using (13) to represent the PDF $f_{|h_{sr}|^2}(x)$ as

$$f_{|h_{sr}|^2}(x) = \alpha_s \sum_{\kappa=0}^{m_s-1} \psi_(\kappa) x^{\kappa} \mathrm{e}^{-(\beta_s - \delta_s)\mathrm{x}}, \tag{14}$$

where $\psi(\kappa) = (-1)^{\kappa}(1-m_s)_{\kappa}\delta_s^{\kappa}/(\kappa!)^2$.

The PDF of γ_{sr} can be thus derived by applying the transformation of variable as

$$f_{\gamma_{sr}}(x) = \alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\psi(\kappa)}{(\eta_s)^{\kappa+1}} x^{\kappa} \mathrm{e}^{-\left(\frac{\beta_s - \delta_s}{\eta_s}\right)\mathrm{x}}. \tag{15}$$

By integrating the PDF in (15) with the aid of [25, eq. 3.351.2], we can obtain the cumulative distribution function (CDF) of γ_{sr} as

$$\begin{aligned} F_{\gamma_{sr}}(x) = 1 - \alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\psi(\kappa)}{(\eta_s)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta_s - \delta_s}{\eta_s}\right)^{-(\kappa+1-p)} \\ \times x^p \mathrm{e}^{-\left(\frac{\beta_s - \delta_s}{\eta_s}\right)\mathrm{x}}. \end{aligned} \tag{16}$$

For terrestrial links, the channel coefficients h_{rd_n} and h_{re} undergo Nakagami-m distribution with fading severity m_d and m_e, and average power Ω_d and Ω_e, respectively. As such, the PDF and CDF of channel gain γ_{rd_n} are given, respectively, by

$$f_{\gamma_{rd_n}}(x) = \left(\frac{m_d}{\varrho_d}\right)^{m_d} \frac{x^{m_d-1}}{\Gamma(m_d)} \mathrm{e}^{-\frac{\mathrm{m_d}}{\varrho_\mathrm{d}}\mathrm{x}} \tag{17}$$

and

$$F_{\gamma_{rd_n}}(x) = \frac{1}{\Gamma(m_d)} \Upsilon\left(m_d, \frac{m_d}{\varrho_d} x\right), \tag{18}$$

where $\varrho_d = \eta_r \Omega_d$, $\Upsilon(\cdot,\cdot)$ and $\Gamma(\cdot)$ represent, respectively, the lower incomplete and the complete gamma functions [25, eq. 8.350]. Similarly, the PDF and CDF of channel gain γ_{re} are given, respectively, as

$$f_{\gamma_{re}}(x) = \left(\frac{m_e}{\varrho_e}\right)^{m_e} \frac{x^{m_e-1}}{\Gamma(m_e)} \mathrm{e}^{-\frac{m_e}{\varrho_e}x} \tag{19}$$

and

$$F_{\gamma_{re}}(x) = \frac{1}{\Gamma(m_e)} \Upsilon\left(m_e, \frac{m_e}{\varrho_e}x\right), \tag{20}$$

where $\varrho_e = \eta_r \Omega_e$.

3 Secrecy performance analysis

Here, we first derive the SOP expression of the considered HSTRN and then analyze the asymptotic behavior of the SOP expression. Subsequently, we also calculate the probability of non-zero secrecy capacity.

3.1 SOP

The secrecy outage event is said to occur when the transmitter sends data at a rate $\mathcal{R}_S$ higher than the secrecy capacity C_S. Hence, the SOP for considered HSTRN is formulated as

$$\mathcal{P}_{\text{sec}} = \Pr[\mathrm{C_S} < \mathcal{R}_\mathrm{S}], \tag{21}$$

which can be expressed using (11) as

$$\mathcal{P}_{\text{sec}} = \Pr\left[\frac{1+\gamma_\mathrm{D}}{1+\gamma_\mathrm{E}} < \gamma_0\right], \tag{22}$$

where $\gamma_0 = 2^{2\mathcal{R}_S}$. On performing some appropriate approximation, (22) can be given as

$$\mathcal{P}_{\text{sec}} \approx \Pr\left[\frac{\gamma_\mathrm{D}}{\gamma_\mathrm{E}} < \gamma_0\right], \tag{23}$$

where we have used the approximation $\frac{1+x}{1+y} \approx \frac{x}{y}$, which is widely adopted in literature [23, 24] and shown to have negligible effect in broad SNR region. Further, on invoking the SNR expressions from (8) and (10) into (23) and doing some manipulations for large transmit power, we obtain

$$\begin{aligned}\mathcal{P}_{\text{sec}} &\approx \Pr\left[\frac{\gamma_{\mathrm{sr}}\gamma_{\mathrm{rd}}}{\gamma_0\gamma_{\mathrm{sr}} + (\gamma_0 - 1)\gamma_{\mathrm{rd}}} < \gamma_{\mathrm{re}}\right] \\ &= \int_0^\infty F_Z(z) f_{\gamma_{re}}(z) dz,\end{aligned} \tag{24}$$

where the last expression results after defining $Z \triangleq \frac{\gamma_{sr}\gamma_{rd}}{\gamma_0\gamma_{sr}+(\gamma_0-1)\gamma_{rd}}$. To proceed further, we require the CDF $F_Z(z)$ which can be derived as

$$\begin{aligned}F_Z(z) = 1 - \int_0^\infty &\left(1 - F_{\gamma_{sr}}\left(\frac{z(\gamma_0-1)(x+z\gamma_0)}{x}\right)\right) \\ &\times f_{\gamma_{rd}}(x + z\gamma_0) dx.\end{aligned} \tag{25}$$

To solve (25), we require the PDF of γ_{rd}. After applying order statistics, $f_{\gamma_{rd}}(x)$ can be given as

$$f_{\gamma_{rd}}(x) = N\left(F_{\gamma_{rd_n}}(x)\right)^{N-1} f_{\gamma_{rd_n}}(x). \tag{26}$$

On invoking (18) with series exploration of $\Upsilon(\cdot,\cdot)$ [25, eq. 8.352.1], the corresponding PDF from (17) into (26), and then applying binomial [25, eq. 1.111] and multinomial [25, eq. 0.314] expansions, we obtain $f_{\gamma_{rd}}(x)$ as

$$\begin{aligned}f_{\gamma_{rd}}(x) = N \sum_{\jmath=0}^{N-1} \binom{N-1}{\jmath} \sum_{l=0}^{\jmath(m_d-1)} \frac{\omega_l^\jmath}{\Gamma(m_d)} (-1)^\jmath \\ \times \left(\frac{m_d}{\varrho_d}\right)^{m_d+l} x^{m_d+l-1} e^{-\left(\frac{m_d}{\varrho_d}\right)(\jmath+1)x},\end{aligned} \tag{27}$$

where the coefficients $\omega_l^\jmath$, for $0 \le l \le \jmath(m_d-1)$, can be calculated recursively (with $\varepsilon_1 = \frac{1}{1!}$) as $\omega_0^\jmath = (\varepsilon_0)^\jmath$, $\omega_1^\jmath = \jmath(\varepsilon_1)$, $\omega_{\jmath(m_d-1)}^\jmath = (\varepsilon_{m_d-1})^\jmath$, $\omega_l^\jmath = \frac{1}{l\varepsilon_0}\sum_{q=1}^{l}[q\jmath - l + q]\varepsilon_q \omega_{l-q}^\jmath$ for $2 \le l \le m_d - 1$, and $\omega_l^\jmath = \frac{1}{l\varepsilon_0}\sum_{q=1}^{m_d-1}[q\jmath - l + q]\varepsilon_q \omega_{l-q}^\jmath$ for $m_d \le l < \jmath(m_d-1)$.

Now, using (16) and (27) into (25), we can obtain $F_Z(z)$ with the help of [25, eq. 3.471.9], and then substituting the resultant of (25) along with (19) into (24), and then solving the integration with the use of [25, eq. 7.813.1], we obtain SOP as given in (28), shown at the top of the next page,

$$\begin{aligned}\mathcal{P}_{\text{sec}} = 1 - N &\sum_{\kappa=0}^{m_s-1} \sum_{p=0}^{\kappa} \sum_{\jmath=0}^{N-1} \sum_{l=0}^{\jmath(m_d-1)} \sum_{q=0}^{t+l} \binom{N-1}{\jmath} \binom{t+l}{q} \frac{\alpha(\gamma_0-1)^p \kappa! \psi(\kappa)}{p!(\eta_s)^{\kappa+1}} \left(\frac{\beta-\delta}{\eta_s}\right)^{-(\kappa+1-p)} \omega_l^\jmath \frac{(-1)^\jmath}{\Gamma(m_d)} \left(\frac{m_d}{\varrho_d}\right)^{m_d+l} \\ &\times (\gamma_0)^{t+l-q} \frac{2\sqrt{\pi}}{\Gamma(m_e)} \left(\frac{m_e}{\varrho_e}\right)^{m_e} \left(\Phi + 2\sqrt{\frac{\beta-\delta}{\eta_s}\gamma_0(\gamma_0-1)\frac{m_d}{\varrho_d}(\jmath+1)}\right)^{-(\mu+l+v)} \left(4\frac{\beta-\delta}{\eta_s}\gamma_0(\gamma_0-1)\right)^v \\ &\times \frac{\Gamma(\mu+l+v)\Gamma(\mu+l-v)}{\Gamma(\mu+l+\frac{1}{2})} {}_2F_1\left(\mu+l+v; v+\frac{1}{2}; \mu+l+\frac{1}{2}; \frac{\Phi - 2\sqrt{\frac{\beta-\delta}{\eta_s}\gamma_0(\gamma_0-1)\frac{m_d}{\varrho_d}(\jmath+1)}}{\Phi + 2\sqrt{\frac{\beta-\delta}{\eta_s}\gamma_0(\gamma_0-1)\frac{m_d}{\varrho_d}(\jmath+1)}}\right).\end{aligned} \tag{28}$$

where $t = p + m_d - 1$, $v = q - p + 1$, $\mu = t + m_e + 1$, $\Phi = \frac{\beta-\delta}{\eta_s}(\gamma_0 - 1) + \frac{m_d}{\varrho_d}(\jmath + 1)\gamma_0 + \frac{m_e}{\varrho_e}$, and ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the hypergeometric function of second kind [25, eq. 9.111].

3.2 Asymptotic analysis

To shed more light onto the considered HSTRN secrecy performance, we analyze the asymptotic behaviour of the SOP expression in the high SNR regime. For this, Z can be simplified as $Z \simeq \min(\gamma_0\gamma_{sr}, (\gamma_0 - 1)\gamma_{rd})$ and the CDF $F_Z(x)$ can be approximated by neglecting the higher order term as

$$F_Z(x) \simeq F_{\gamma_{sr}}((\gamma_0 - 1)x) + F_{\gamma_{rd}}(\gamma_0 x). \tag{29}$$

To proceed, we require asymptotic expressions for $F_{\gamma_{sr}}(x)$ and $F_{\gamma_{rd}}(x)$. At high SNR regime, we assume $\eta_s \to \infty$ and apply the Maclaurin series expansion of the exponential function in (15) to approximate the PDF $f_{\gamma_{sr}}(x)$ as

$$f_{\gamma_{sr}}(x) \simeq \frac{\alpha_s}{\eta_s}, \tag{30}$$

and hence, by integrating (30), the asymptotic behaviour of $F_{\gamma_{sr}}(x)$ can be given as

$$F_{\gamma_{sr}}(x) \simeq \frac{\alpha_s}{\eta_s} x. \tag{31}$$

Likewise, one can derive

$$F_{\gamma_{rd}}(x) \simeq \frac{x^{m_d N}}{[\Gamma(m_d + 1)]^N} \left(\frac{m_d}{\varrho_d}\right)^{m_d N}. \tag{32}$$

Now, invoking (31) and (32) into (29), and substituting the obtained result into (24) along with (19), and then solving the involved integral using [25, eq. 3.351.3], we can obtain the asymptotic SOP expression as

$$\mathcal{P}_{\text{sec}}^{\infty} \simeq \frac{\alpha(\gamma_0 - 1)\varrho_e}{\eta_s} + \frac{(m_d N + m_e - 1)!}{[\Gamma(m_d + 1)]^N \Gamma(m_e)} \left(\frac{m_d}{\varrho_d}\right)^{m_d N} \times \gamma_0^{m_d N} \left(\frac{m_e}{\varrho_e}\right)^{-m_d N}. \tag{33}$$

which clearly reflects the achievable diversity order of $\min(1, m_d N)$.

Remarks: Our asymptotic analysis of SOP reveals that the considered HSTRN attains a diversity order of $\min(1, m_d N)$. Importantly, the diversity order is mainly bottlenecked by the satellite link, whereby it remains unaffected by the fading severity parameter of satellite link.

3.3 Probability of non-zero secrecy capacity

In this subsection, we calculate the probability for existence of non-zero secrecy capacity. The event of non-zero secrecy occurs when the main link is better than the eavesdropper link, which is given by

$$\mathcal{P}(C_S > 0) = \Pr[\gamma_{\text{D}} > \gamma_{\text{E}}]. \tag{34}$$

After invoking (8) and (10) into (34) and performing simplification, (34) can be presented as

$$\mathcal{P}(C_S > 0) = \Pr[\gamma_{\text{rd}} > \gamma_{\text{re}}], = \int_0^{\infty} F_{\gamma_{re}}(x) f_{\gamma_{rd}}(x) dx. \tag{35}$$

After substituting (20) and (27) into (35), the probability for existence of non-zero secrecy capacity can be computed and given as

$$\mathcal{P}(C_S > 0) = 1 - N \sum_{\jmath=0}^{N-1} \binom{N-1}{\jmath} \sum_{l=0}^{\jmath(m_d-1)} \sum_{n=0}^{m_e-1} \times \left(\frac{m_e}{\varrho_e}\right)^n \frac{\omega_l^{\jmath}(-1)^{\jmath}\Gamma(n + m_d + l)}{\Gamma(m_d)n!} \left(\frac{m_d}{\varrho_d}\right)^{m_d+l} \times \left(\frac{m_d}{\varrho_d}(\jmath + 1) + \frac{m_e}{\varrho_e}\right)^{-(n+m_d+l)}. \tag{36}$$

In deriving (36), we have used [25, eq. 3.351.3].

4 Numerical and simulation results

In this section, we present the numerical and simulation results to confirm the validity of the proposed theoretical studies and examine the impact of various system/channel parameters on the secrecy performance of the considered system. In particular, we examine the SOP and existence of non-zero secrecy capacity performance measures under various system/channel parameters. For this, we set $\eta_s = \eta_r$ as transmit SNR. The Shadowing-Rician fading parameters for $S \to R$ link are adopted as $(m_s, b, \Omega_s = 1, 0.063, 0.0007)$ under heavy shadowing and $(m_s, b, \Omega_s = 5, 0.251, 0.279)$ under average shadowing scenarios [21]. For validation of theoretical analysis, we carried out Monte-Carlo simulations.

Figure 2 depicts the SOP performance of the considered HSTRN versus η_s for various number of terrestrial users under average and heavy shadowing scenarios of Shadowed-Rician fading channel. By fixing $\mathcal{R}_S = 0.5$, $m_d = 1$, $m_e = 1$, and $\varrho_e = 2$ dB, SOP curves are drawn using (28). In addition, we also drawn the asymptotic SOP curves using (33) (for the same configuration), which agree very well with the exact ones in the high SNR region. We can

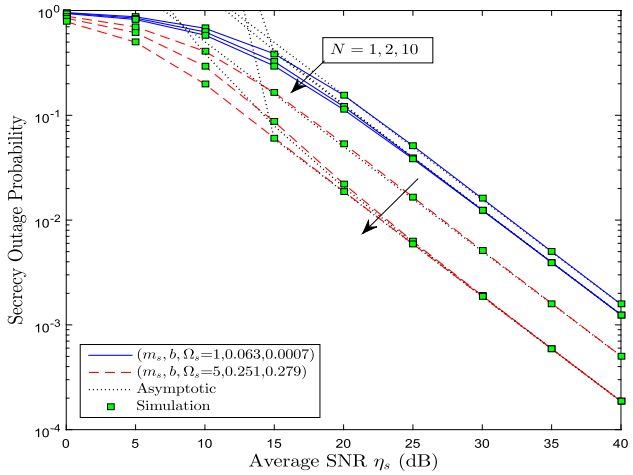

Fig. 2 SOP versus η_s for different number of terrestrial users

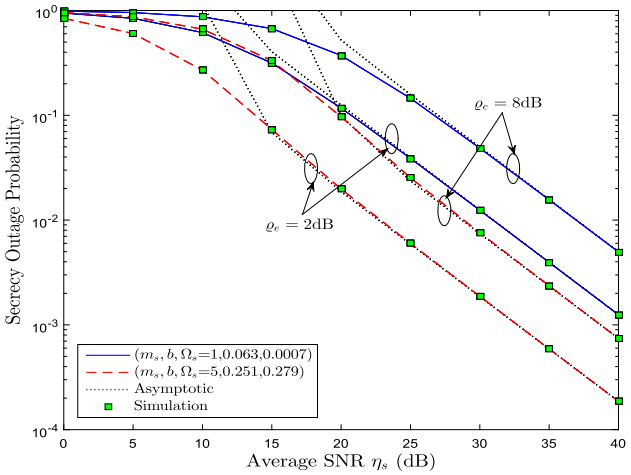

Fig. 4 SOP versus η_s with different ϱ_e

see from this figure that secrecy performance of the system improves with an increase in the number of terrestrial users. However, owing to the bottleneck effect of the satellite link, this performance improvement becomes limited when N increases to a certain extent, as reflected by comparing the curves for $N = 2$ and $N = 10$. It is important to note that the system attains the diversity order of $\min(1, m_d N)$ i.e., unity, which can be seen by the slope of the curves. Moreover, it can be realized that the system performs better under average Shadowed-Rician fading as compared to heavy Shadowed-Rician fading scenario.

In Fig. 3, we illustrate the SOP performance versus η_s with different values of secrecy rate $\mathcal{R}_S$ by assuming $m_d = 1$, $m_e = 2$, $\varrho_e = 2$ dB, and $N = 1$. The curves are plotted under average and heavy shadowed scenarios of $S \rightarrow R$ link. As can be expected, the SOP of the considered HSTRN degrades with an increase in the secrecy rate $\mathcal{R}_S$. Importantly, this increase in the $\mathcal{R}_S$ does not affect the achievable diversity order of the system.

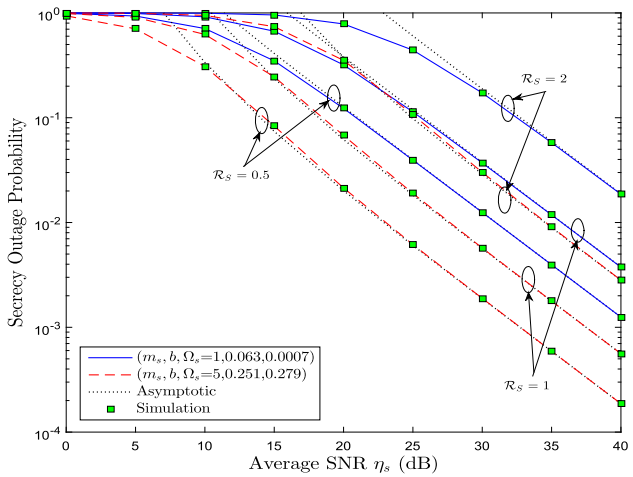

Fig. 3 SOP versus η_s with different $\mathcal{R}_S$

Figure 4 illustrates the SOP of the system for different values of ϱ_e. As shown in the figure, curves are drawn for two different values of ϱ_e (i.e., 2 and 8 dB) under average and heavy shadowing scenarios of Shadowed-Rician fading channels by keeping $N = 2$, $m_d = 2$, $m_e = 1$, and $\mathcal{R}_S = 0.5$. One can clearly observe that the SOP of the considered HSTRN increases as the ϱ_e increases which indicates the detrimental impact of a more powerful eavesdropper.

Figure 5 depicts the probability of non-zero secrecy capacity versus η_s of the considered HSTRN for different number of terrestrial users, where the $S \rightarrow R$ link is subjected to heavy shadowing scenario. For this, we have fixed $m_d = 1$, $m_e = 3$, $\varrho_e = 2$ dB, and $\mathcal{R}_S = 0.5$. The curves for probability of non-zero secrecy capacity are plotted using (36). As shown in the figure, with an increase of the number of terrestrial users, the achievable non-zero secrecy

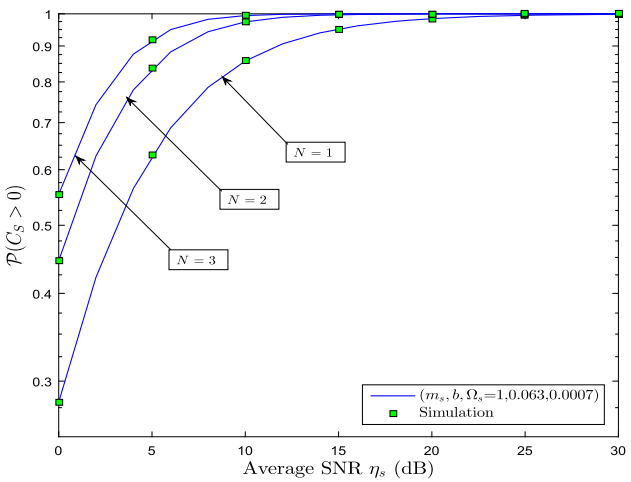

Fig. 5 Probability of non-zero secrecy capacity versus η_s for different N

capacity increases significantly, which enlightens the advantage of deploying multiple terrestrial users.

5 Conclusion

In this paper, we have investigated the secrecy performance of a downlink multi-user HSTRN using AF relaying and opportunistic user scheduling. By following Shadowed-Rician fading for satellite link and Nakagami-*m* fading for terrestrial links, we derived accurate and asymptotic SOP expressions for the considered system. We obtained the system achievable diversity order and revealed that it remains unaffected by the fading severity parameter of satellite link. Furthermore, we derived the expression for probability of non-zero secrecy capacity. We highlighted the impact of various key system/channel parameters on the secrecy performance of the considered system. Our results revealed that the increase of the number of terrestrial users plays an important role in improving the secrecy performance of the considered HSTRN. Moreover, deployment of multiple antennas at satellite could be a crucial study for future investigation.

Acknowledgements 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).

References

1. Chini P, Giambene G, Kota S (2009) A survey on mobile satellite systems. Int J Sat Commun 28(1):29–57
2. Chuberre N, Courseille O, Laine P, Roullet L, Quignon T, Tatard M (2008) Hybrid satellite and terrestrial infrastructure for mobile broadcast services delivery: an outlook to the unlimited mobile TV system performance. Int J Sat Commun 28(5):405–426
3. Evans B, Werner M, Lutz E, Bousquet M, Corazza G, Maral G, Rumeau R (2005) Integration of satellite and terrestrial systems in future media communications. IEEE Trans Wirel Commun 12(5):72–80
4. Sakarellos V, Kourogiorgas C, Panagopoulos A (2014) Cooperative hybrid land mobile satellite-terrestrial broadcasting systems: outage probability evaluation and accurate simulation. Wirel Pers Commun 79(2):1471–1481
5. ETSI EN 102 585 V1.1.2: (2008) Digital video broadcasting (DVB); system specifications for Satellite services to Handheld devices (SH) below 3 GHz
6. Bhatnagar MR, Arti MK (2013) Performance analysis of AF based hybrid satellite-terrestrial cooperative network over generalized fading channels. IEEE Commun Lett 17(10):1912–1915
7. An K, Lin M, Liang T (2015) On the performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling. IEEE Commun Lett 19(10):1722–1725
8. Upadhyay PK, Sharma PK (2016) Max-max user-relay selection scheme in multiuser and multirelay hybrid satellite terrestrial relay systems. IEEE Commun Lett 20(2):268–271
9. Sharma PK, Upadhyay PK, da Costa DB, Bithas PS, Kanatas AG (2017) Overlay spectrum sharing in hybrid satellite-terrestrial systems with secondary network selection. IEEE Trans Wirel Commun 16(10):6586–6601
10. An K, Lin M, Liang T, Wang JB, Wang J, Huang Y, Swindlehurst AL (2015) Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference. IEEE Trans Commun 63(11):4390–4404
11. Bankey V, Upadhyay PK (2018) Ergodic capacity of multiuser hybrid satellite-terrestrial fixed-gain AF relay networks with CCI and outdated CSI. IEEE Trans Veh Technol 67(5):4666–4671
12. Bankey V, Upadhyay PK, da Costa DB, Bithas PS, Kanatas AG, Dias US (2018) Performance analysis of multi-antenna multiuser hybrid satellite-terrestrial relay systems for mobile services delivery. IEEE Access 6:24729–24745
13. Sklavos N, Zhang X (2007) Wireless security and cryptography: specifications and implementations, 1st edn. CRC Press, Baco Raton
14. Wyner AD (1975) The wire-tap channel. Bell Syst Technol J 54(8):1355–1387
15. Huang Q, Lin M, An K, Ouyang J, Zhu WP (2018) Secrecy performance of hybrid satellite-terrestrial relay networks in the presence of multiple eavesdroppers. IET Commun 12(1):26–34
16. Bankey V, Upadhyay PK, (2017) Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes. In: Proceedings IEEE 85th vehicular technology conference(VTC), Sydney, Australia
17. Cao W, Zou Y, Yang Z, Zhu J, (2017) Secrecy outage probability of hybrid satellite-terrestrial relay networks. In: Proceedings of IEEE global communications conference (GLOBECOM 2017), Singapore
18. An K, Lin M, Ouyang J, Zhu W-P (2016) Secure transmission in cognitive satellite terrestrial networks. IEEE J Sel Areas Commun 34(11):3025–3037
19. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456
20. Abdi A, Lau W, Alouini M-S, Kaveh M (2003) A new simple model for land mobile satellite channels: first and second order statistics. IEEE Trans Wireless Commun 2(3):519–528
21. Miridakis NI, Vergados DD, Michalas A (2015) Dual-hop communication over a satellite relay and Shadowed-Rician channels. IEEE Trans Veh Technol 64(9):4031–4040
22. Alfano G, De Maio A (2007) Sum of squared Shadowed-Rice random variables and its application to communication systems performance prediction. IEEE Trans Wirel Commun 6(10):3540–3545
23. Jeon H, Kim N, Choi J, Lee H, Ha J (2011) Bounds on secrecy capacity over correlated ergodic fading channels at high SNR. IEEE Trans Inf Theory 57(4):1975–1983
24. Krikidis I, Thompson JS, McLaughlin S (2009) Relay selection for secure cooperative networks with jamming. IEEE Trans Wirel Commun 8(10):5003–5011
25. Gradshteyn IS, Ryzhik IM (2000) Tables of integrals, series and products, 6th edn. Academic Press, New York