Regular Article

Hybrid Satellite-Terrestrial Relaying Networks With Imperfect Channel State Information and Directional Antenna: the Dilemma of Facilitating Reliability and Improving Security

Lam-Thanh Tu[1], Tran Trung Duy[2], Quang-Sang Nguyen[2], Tan N. Nguyen[1], Nguyen Hong Nhu[3], Hien Q. Ta[4], Nguyen Hong Giang[5]

[1] Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[2] Faculty of Telecommunications 2, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam
[3] Faculty of Engineering and Technology, Saigon University, Ho Chi Minh City, Vietnam
[4] School of Electrical Engineering, International University, Ho Chi Minh City, Vietnam and Vietnam National University, Ho Chi Minh City, Vietnam
[5] Telecommunications University, Nha Trang City, Khanh Hoa Province, Vietnam

Correspondence: Lam-Thanh Tu, tulamthanh@tdtu.edu.vn

Communication: received 12 February 2025, revised 18 March 2025, accepted 20 March 2025
Online publication: 25 March 2025, Digital Object Identifier: 10.21553/rev-jec.399

Abstract– **The performance of hybrid satellite-terrestrial relaying (HSTR) networks is investigated in this work. Specifically, we examine the trade-off between reliability and security in HSTR networks using two key parameters: outage probability (OP) and intercept probability (IP). Both metrics are derived in closed-form expressions under the assumption of imperfect channel state information (CSI) for the legitimate channels. Additionally, a directional antenna is employed to compensate for the significant path loss caused by the long transmission distance between the satellite and the ground terminal. Numerical computations are provided to validate the accuracy of the derived framework. Furthermore, our findings reveal that increasing the satellite's transmit power and altitude has opposite effects on security and reliability. Specifically, increasing the transmit power enhances system reliability but reduces security. In contrast, a higher satellite altitude decreases reliability but improves security. These findings are further validated through Monte Carlo-based simulations.**

Keywords– **Hybrid satellite-terrestrial relaying networks, imperfect channel state information, intercept probability, outage probability.**

1 Introduction

Satellite communications have been recognized as a key technology for sixth-generation (6G) mobile networks, offering advantages such as a strong line-of-sight (LOS) path, wide coverage area, and stable data rates [1]. However, satellite communications also have inherent drawbacks. For instance, geostationary orbit (GEO) satellites suffer from low data rates and require expensive, complex ground terminal hardware. Meanwhile, low Earth orbit (LEO) satellites provide limited coverage and require a large constellation to ensure reliability and/or high-speed data rates. To address these challenges, integrating terrestrial relay stations is considered an optimal solution to enhance satellite communication performance. This approach not only expands coverage, particularly in urban areas, but also simplifies terminal hardware requirements and offers several additional advantages [2, 3].

The performance of satellite communications and hybrid satellite-terrestrial relaying (HSTR) networks has been investigated in several studies [4–17]. Nguyen and his colleagues examined the trade-off between security and reliability in HSTR networks under imperfect channel state information (CSI) [4]. However, their study did not consider the Nakagami-*m* fading channel for terrestrial communications in combination with a directional antenna to compensate for severe path loss in satellite communications. In [5], the authors investigated the performance of a two-way HSTR network supported by aerial access nodes combined with non-orthogonal multiple access (NOMA). However, this work did not consider the security aspect of the system. Similarly, Zhang *et al.* in [6] also studied an HSTR network integrating NOMA, but their focus was on resource allocation rather than addressing the trade-off between information security and system reliability. The performance of an HSTR network with multiple relay nodes under imperfect CSI was examined in [7]. The outage probability (OP) of a full-duplex HSTR network under co-channel interference (CCI) was analyzed in [8]. Lan *et al.* in [9] designed and experimentally tested isotropic antennas for satellite communications. The performance of satellite and wireless sensor networks was investigated in [10]. The correlation between information security and reliability in an HSTR network with energy-harvesting relays was analyzed in [11]. In [12], the authors derived the OP and ergodic capacity of HSTR systems considering mmWave and NOMA. However, they did not account for imperfect CSI or the use of directional antennas. The performance of two-way HSTR networks was studied in [13], where the authors derived both the OP and relay selection strategies. However, they did not consider the impact of imperfect CSI. The secrecy performance and phase shift design of reconfigurable intelligent surfaces (RIS)-assisted satellite networks (RISAS) were addressed in [14] and [15]. Son and his colleagues derived the energy OP of unmanned aerial vehicle (UAV)-enabled simultaneous wireless information and power transfer (SWIPT) networks in [16]. The impact of co-channel interference on HSTR networks was investigated in [17].

Although the aforementioned studies have extensively investigated the performance of HSTR networks and the relationship between system reliability and security, they have not considered the use of directional antennas and/or a generalized terrestrial channel. Therefore, in this work, we take a pioneering step in analyzing the trade-off between security and reliability in HSTR networks under imperfect CSI while incorporating directional antennas. Additionally, the terrestrial channel is modeled using a generalized Nakagami-m fading distribution. The main contributions and novelties of the proposed network are summarized as follows:

- We take a pioneering step in studying HSTR systems with imperfect CSI and directional antennas.
- We derive both the OP and intercept probability (IP) in closed-form expressions and validate their accuracy through Monte Carlo simulations. Notably, the derivation framework is challenging, as OP and IP are functions of multiple random variables.
- We provide several valuable insights through numerical results. For instance, in the proposed system, increasing the satellite's transmit power improves system reliability but comes at the cost of higher security risks. Similar trends are observed for other key parameters, such as satellite antenna gain and air-to-ground transmission distance. However, reducing the transmission distance between the relay and the legitimate user enhances system reliability but does not sacrifice the security.

The rest of this paper is structured as follows. Section 2 describes the system model. The derivations of both the OP and IP are provided in Section 3. Simulation results based on the Monte Carlo method are presented in Section 4. Finally, conclusions are drawn in Section 5.

2 System Model

Considering a hybrid satellite-terrestrial relaying network, as illustrated in Figure 1. In this system, a satellite, denoted as S, communicates with a terrestrial user, denoted as U, with the assistance of a ground-based relay station, denoted as R. Additionally, a passive eavesdropper, denoted as E, is present in the network. We assume that all nodes are equipped with a single antenna. Specifically, the satellite is equipped with a directional antenna, while the relay, terrestrial user, and eavesdropper are equipped with omnidirectional antennas.

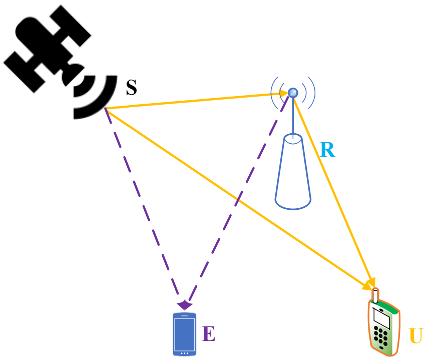

Figure 1. An HSTR network with an eavesdropper.

2.1 Channel modeling

2.1.1 Small-scale fading modeling: The transmitted signals are affected by both small-scale fading and large-scale path loss. More precisely, signals transmitted from the satellite to the relay, legitimate user, and eavesdropper follow a shadowed-Rician distribution. This distribution is particularly suitable for characterizing the strong line-of-sight nature of the air-to-ground (A2G) channel. Let $\beta_{S,X}$ denote the channel coefficient from the satellite S to node X, where $X \in$ {R, E, U}. Assuming it follows a shadowed-Rician distribution, the probability density function (PDF) and cumulative distribution function (CDF) of the channel gain, denoted as $f_{\beta^2_{S,X}}(x)$ and $F_{\beta^2_{S,X}}(x)$, are given by:

$$\begin{aligned} f_{\beta^2_{S,X}}(x) &= \varpi \sum_{v=0}^{m-1} \theta(v)\, x^v \exp\left(-\left(\vartheta-\rho\right)x\right), \\ F_{\beta^2_{S,X}}(x) &= 1 - \varpi \sum_{v=0}^{m-1} \sum_{i=0}^{v} \frac{(-1)^v (1-m)_v \rho^v}{v! i! (\vartheta-\rho)^{(v+1-i)}} x^i \\ &\quad \times \exp\left(-\left(\vartheta-\rho\right)x\right), \end{aligned} \tag{1}$$

where the parameters of the shadowed-Rician distribution are defined as follows:

$$\begin{aligned} \varpi &= \vartheta \left(\frac{2pm}{2pm+q}\right)^m, \vartheta = \frac{1}{2p}, \\ \rho &= \frac{\vartheta q}{2pm+q}, \\ \theta(v) &= \frac{(-1)^v (1-m)_k \rho^k}{(v!)^2}, \end{aligned} \tag{2}$$

where $(x)_v = \prod_{k=0}^{v-1}(x-k)$ denotes the Pochhammer symbol [18, p. xliii]. The parameters $p_{S,X} = p, \forall X$, and $q_{S,X} = q, \forall X$, represent the average power of the line-of-sight and non-line-of-sight (NLOS) components, respectively. Additionally, m_X is the fading parameter of the channel gain from S to X.

For the terrestrial link, we assume that the channel coefficient follows a Nakagami distribution, denoted as $\beta_{R,Y}$, with shape and scale parameters, i.e., $m_{R,Y}$, $\varsigma_{R,Y}$, where $Y \in \{\mathrm{E, U}\}$. As a result, the PDF and CDF of the channel gain follows a Gamma distribution and is given by:

$$\begin{aligned} f_{\beta_{R,Y}^2}(x) &= \frac{x^{m_Y - 1}}{\Gamma(m_Y)\left(\frac{\varsigma_{R,Y}}{m_{R,Y}}\right)^{m_Y}} \exp\left(-\frac{x}{\left(\frac{\varsigma_{R,Y}}{m_{R,Y}}\right)}\right), \\ F_{\beta_{R,Y}^2}(x) &= \frac{1}{\Gamma(m_Y)} \gamma\left(m_Y, \frac{x}{\left(\frac{\varsigma_{R,Y}}{m_{R,Y}}\right)}\right), \end{aligned} \quad (3)$$

where $\Gamma(\bullet)$ and $\gamma(\bullet, \bullet)$ represent the Gamma and lower incomplete Gamma functions, respectively [18].

2.1.2 Large-scale path-loss modeling: In this work, a simplified large-scale path-loss model is employed. More particular, let $\alpha_{Z,X}$ denote the large-scale path loss from node $Z \in \{\mathrm{S, R}\}$ to node $X \in \{\mathrm{R, E, U}\}$. It is given by the following formula

$$\alpha_{Z,X} = K_0 d_{Z,X}^{\mu_X}. \quad (4)$$

Here, K_0 and μ_X represent the path-loss constant and the path-loss exponent, respectively. The parameter K_0 is a function of the carrier frequency and is computed as $K_0 = \left(\frac{4\pi}{\lambda}\right)^2$, where $\lambda = \frac{c}{f_c}$ is the wavelength, c is the speed of light, and f_c is the carrier frequency.

2.2 Directional antenna modeling

The satellite S employs a directional antenna to compensate for the severe path loss between the satellite and terrestrial nodes. Specifically, the following directional antenna model is used for S [19]

$$G_S(\kappa) = \begin{cases} G_{\max} & if \quad |\kappa| \le \tau \\ G_{\min} & if \quad \tau < |\kappa| \le \pi \end{cases}, \quad (5)$$

where $\kappa \in [-\pi, \pi)$ represents the beam direction of the satellite antenna, and τ denotes the main lobe beamwidth. Additionally, $G_{\max}$ and $G_{\min}$ correspond to the antenna gains of the main lobe and side lobe, respectively.

2.3 Imperfect channel sate information modeling

For the CSI, we assume the presence of imperfect channel state information for the main links, i.e., from S to R and U, as well as from R to U. This assumption is highly realistic due to phase errors, satellite movement around the Earth, and other factors. More precisely, the following imperfect CSI model is adopted [20]

$$\bar{\bar{\beta}}_{S,W} = \lambda \beta_{S,W} + \sqrt{1 - \lambda^2}\Xi, \quad W \in \{R, U\}, \quad (6)$$

where $\bar{\bar{\beta}}_{S,W}$ represents the estimated channel coefficient, while $\lambda \in [0, 1]$ denotes the correlation factor between the actual and estimated channel. Additionally, Ξ is an additive white Gaussian noise (AWGN) with zero mean and variance $\omega_{S,W}$. Regarding the eavesdropper's channel state information, both the satellite and relay have only statistical CSI rather than instantaneous CSI.

2.4 Signal-to-noise ratio at legitimate user and eavesdropper

The transmission from the satellite S to the user U occurs in two phases (two time slots). In the first time slot, the satellite transmits signals to both the user U and the relay R. Additionally, due to the nature of the wireless channel, the eavesdropper E also receives signals from S. At the relay R, the decode-and-forward (DF) protocol is applied, meaning that the relay decodes, re-encodes the received information from S, and forwards it to U in the second time slot. Once again, the eavesdropper E also intercepts signals from the relay R during this phase. The mathematical expression for the received signal at node $W \in \{R, U\}$ and at the eavesdropper E in the first phase, transmitted from the satellite, is given as follows:

$$\begin{aligned} y_W^1 &= \sqrt{P_S G_{\max}}\bar{\bar{\beta}}_{S,W} x_S + n_W^1, \\ y_E^1 &= \sqrt{P_S G_{\min}}\beta_{S,E} x_S + n_E^1. \end{aligned} \quad (7)$$

Here, x_S represents the signal transmitted from the satellite, with $\mathbb{E}\left\{|x_S|^2\right\} = 1$, where $\mathbb{E}\{.\}$ denotes the expectation operator. The terms n_W^1 and n_E^1 represent the AWGN at nodes W and E, respectively, with variance given by $\sigma_W^2 = \sigma_E^2 = 10^{\left(-174 + 10\log_{10}(\mathrm{BW}) + F_{dB}\right)/10}$, where BW represents the transmission bandwidth, and F [dB] is the receiver noise figure. Additionally, P_S denotes the transmit power of the satellite.

In (7), we assume that the satellite S knows the direction of both the user U and the relay R, allowing it to adjust its antenna beam towards the intended users, thereby achieving maximum gain. Conversely, the antenna gain at the eavesdropper E corresponds to the side lobe gain.

The received signals at the user U and the eavesdropper E from the relay R in the second phase are given as follows:

$$\begin{aligned} y_U^2 &= \sqrt{P_R}\bar{\bar{\beta}}_{R,U} x_R + n_U^2, \\ y_E^2 &= \sqrt{P_R}\beta_{R,E} x_R + n_E^2, \end{aligned} \quad (8)$$

where x_R represents the signal transmitted by the relay node R, with $\mathbb{E}\left\{|x_R|^2\right\} = 1$, and P_R denotes the relay's transmit power. Both U and E employ the selection combining (SC) technique to combine the direct and indirect links. Consequently, the signal-to-noise ratio (SNR) at U and E is given by (9) at the top of the next page.

Here, (9) is attained by substituting (6) into (7) and (8) and combining with the SC technique. $\max\{\bullet\}$ and $\min\{\bullet\}$ are the maximum and minimum functions.

2.5 Performance metrics

In this paper, two key performance metrics, i.e., outage probability and intercept probability, are analyzed as the primary indicators of system performance. The OP represents system reliability, with a lower OP indicating higher reliability. Conversely, the IP reflects system security, where a higher IP signifies weaker information security. The outage probability is measured

$$
\begin{aligned}
\gamma_U =& \max\left\{\frac{\lambda^2 P_S G_{\max}\left(\beta_{S,U}^2+\left(1-\lambda^2\right)\omega_{S,U}/\lambda^2\right)}{\alpha_{S,U}\sigma_U^2}, \min\left\{\frac{\lambda^2 P_S G_{\max}\left(\beta_{S,R}^2+\left(1-\lambda^2\right)\omega_{S,R}/\lambda^2\right)}{\alpha_{S,R}\sigma_R^2},\right.\right.\\
&\left.\left.\frac{\lambda^2 P_R\left(\beta_{R,U}^2+\left(1-\lambda^2\right)\omega_{R,U}/\lambda^2\right)}{\alpha_{R,U}\sigma_R^2}\right\}\right\},\\
\gamma_E =& \max\left\{\frac{P_S G_{\min}\beta_{S,E}^2}{\alpha_{S,E}\sigma_E^2}, \min\left\{\frac{\lambda^2 P_S G_{\max}\left(\beta_{S,R}^2+\left(1-\lambda^2\right)\omega_{S,R}/\lambda^2\right)}{\alpha_{S,R}\sigma_R^2}, \frac{P_R\beta_{R,E}^2}{\alpha_{R,E}\sigma_E^2}\right\}\right\}. \qquad (9)
\end{aligned}
$$

at the legitimate user U, while the intercept probability is evaluated at the eavesdropper E. These two metrics are mathematically expressed as follows:

$$
\begin{aligned}
\mathrm{OP} =& \Pr\left\{\gamma_U \le \gamma_{th}\right\},\\
\mathrm{IP} =& \Pr\left\{\gamma_E \ge \gamma_{th}\right\}. \qquad (10)
\end{aligned}
$$

Here, $\Pr\{.\}$ denotes the probability operator. The SNR threshold, γ_{th}, is defined as $\gamma_{th}=2^{2R/\mathrm{BW}}-1$, where R (in bps) represents the target rate.

3 Performance Analysis

3.1 Outage Probability Analysis

The OP defined in (10) is computed as a closed-form expression and is given by (11) as follows

$$
\begin{aligned}
\mathrm{OP}\left(\gamma_{th}\right) =& \left(1-\varpi\sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)^i\right.\\
&\left.\times\exp\left(-(\vartheta-\rho)\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)\right)\right)H\left(\gamma_{th}-\kappa_1\right)\\
&\times\left[1-\frac{1}{\Gamma\left(m_U\right)}\Gamma\left(m_U,\frac{\gamma_{th}-\kappa_3}{\Omega_3}\right)\right.\\
&\times\left(\varpi\sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)^i\right.\\
&\left.\left.\times\exp\left(-(\vartheta-\rho)\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)\right)\right)\right]. \qquad (11)
\end{aligned}
$$

Here, $\overline{F}_X(x)=1-F_X(x)$ denotes the complementary cumulative distribution function of the random variable (RV) X, and $H(x)$ represents the Heaviside step function.

Proof: We commence the proof by reformulating the definition of the OP as follows

$$
\begin{aligned}
\mathrm{OP}\left(\gamma_{th}\right) =& \Pr\left\{\gamma_U < \gamma_{th}\right\}\\
=& \Pr\left\{\max\left\{\Omega_1\beta_{S,U}^2+\kappa_1,\right.\right.\\
&\left.\left.\min\left\{\Omega_2\beta_{S,R}^2+\kappa_2,\Omega_3\beta_{R,U}^2+\kappa_3\right\}\right\}<\gamma_{th}\right\}\\
=& \Pr\left\{\Omega_1\beta_{S,U}^2+\kappa_1<\gamma_{th},\right.\\
&\left.\min\left\{\Omega_2\beta_{S,R}^2+\kappa_2,\Omega_3\beta_{R,U}^2+\kappa_3\right\}<\gamma_{th}\right\}\\
=& \Pr\left\{\Omega_1\beta_{S,U}^2+\kappa_1<\gamma_{th}\right\} \qquad (12)\\
&\times\Pr\left\{\min\left\{\Omega_2\beta_{S,R}^2+\kappa_2,\Omega_3\beta_{R,U}^2+\kappa_3\right\}<\gamma_{th}\right\},
\end{aligned}
$$

where $\Omega_1=\frac{\lambda^2 P_S G_{\max}}{\alpha_{S,U}\sigma_U^2}$, $\Omega_2=\frac{\lambda^2 P_S G_{\max}}{\alpha_{S,R}\sigma_R^2}$, $\Omega_3=\frac{\lambda^2 P_R}{\alpha_{R,U}\sigma_R^2}$, $\kappa_1=\frac{P_S G_{\max}\left(1-\lambda^2\right)\omega_{S,U}}{\alpha_{S,U}\sigma_U^2}$, $\kappa_2=\frac{P_S G_{\max}\left(1-\lambda^2\right)\omega_{S,R}}{\alpha_{S,R}\sigma_R^2}$, and $\kappa_3=\frac{P_R\left(1-\lambda^2\right)\omega_{R,U}}{\alpha_{R,U}\sigma_R^2}$. The final equation in (12) is derived due to the independence of the direct and indirect links.

The first probability term in (12) is computed as follows

$$
\begin{aligned}
&\Pr\left\{\Omega_1\beta_{S,U}^2+\kappa_1<\gamma_{th}\right\}\\
&=\Pr\left\{\beta_{S,U}^2<\frac{\gamma_{th}-\kappa_1}{\Omega_1},\gamma_{th}>\kappa_1\right\}\\
&=\Pr\left\{\beta_{S,U}^2<\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right\}H\left(\gamma_{th}-\kappa_1\right)\\
&=F_{\beta_{S,U}^2}\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)H\left(\gamma_{th}-\kappa_1\right)\\
&=\left(1-\varpi\sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)^i\right.\\
&\quad\left.\times\exp\left(-(\vartheta-\rho)\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)\right)\right)H\left(\gamma_{th}-\kappa_1\right), \qquad (13)
\end{aligned}
$$

where $F_{\beta_{S,U}^2}\left(\frac{\gamma_{th}-\kappa_1}{\Omega_1}\right)$ is attained by substituting the CDF of $\beta_{S,U}^2$ in (1). To compute the second probability term in (12), we proceed as follows

$$
\begin{aligned}
&\Pr\left\{\min\left\{\Omega_2\beta_{S,R}^2+\kappa_2,\Omega_3\beta_{R,U}^2+\kappa_3\right\}<\gamma_{th}\right\}\\
&=1-\Pr\left\{\Omega_2\beta_{S,R}^2+\kappa_2>\gamma_{th},\Omega_3\beta_{R,U}^2+\kappa_3>\gamma_{th}\right\}\\
&=1-\Pr\left\{\beta_{S,R}^2>\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right\}\Pr\left\{\beta_{R,U}^2>\frac{\gamma_{th}-\kappa_3}{\Omega_3}\right\}\\
&=1-\overline{F}_{\beta_{R,U}^2}\left(\frac{\gamma_{th}-\kappa_3}{\Omega_3}\right)\overline{F}_{\beta_{R,U}^2}\left(\frac{\gamma_{th}-\kappa_3}{\Omega_3}\right)\\
&=1-\frac{1}{\Gamma\left(m_U\right)}\Gamma\left(m_U,\frac{\gamma_{th}-\kappa_3}{\Omega_3}\right)\\
&\quad\times\left(\varpi\sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)^i\right.\\
&\quad\left.\left.\times\exp\left(-(\vartheta-\rho)\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)\right)\right)\right]. \qquad (14)
\end{aligned}
$$

Here, the third equation is obtained due to the independence between the S → R link and the R → D link; the final equation is derived by substituting the CCDF of RVs $\beta_{S,R}^2$ and $\beta_{R,U}^2$, respectively, from (3) and (1), as referenced in [21]. Finally, the OP of the considered network is presented in (11), thus concluding the proof.

3.2 Intercept Probability Analysis

The intercept probability denotes the probability that an eavesdropper successfully wiretaps the secure information of a legitimate user. It is formulated and computed as follows

$$\begin{aligned}\mathrm{IP}\left(\gamma_{th}\right) = 1 - &\left(1 - \varpi \sum_{v=0}^{m-1} \sum_{i=0}^{v} \frac{(-1)^{v}(1-m)_{v}\rho^{v}}{v!i!(\vartheta-\rho)^{(v+1-i)}} \left(\frac{\gamma_{th}}{\Omega_4}\right)^{i}\right.\\ &\left.\times \exp\left(-\left(\vartheta-\rho\right)\left(\frac{\gamma_{th}}{\Omega_4}\right)\right)\right) \left[1 - \frac{1}{\Gamma\left(m_E\right)}\Gamma\left(m_E, \frac{\gamma_{th}}{\Omega_5}\right)\right.\\ &\times \left(1 - \varpi \sum_{v=0}^{m-1} \sum_{i=0}^{v} \frac{(-1)^{v}(1-m)_{v}\rho^{v}}{v!i!(\vartheta-\rho)^{(v+1-i)}} \left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)^{i}\right.\\ &\left.\left.\times \exp\left(-\left(\vartheta-\rho\right)\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)\right)\right)\right]. \qquad (15)\end{aligned}$$

Here, $\Omega_4 = \frac{P_S G_{\min}}{\alpha_{S,E}\sigma_E^2}$ and $\Omega_5 = \frac{P_R}{\alpha_{R,E}\sigma_E^2}$.

Proof: The proof of (15) is given below

$$\begin{aligned}&\mathrm{IP}\left(\gamma_{th}\right) = \Pr\left\{\gamma_E > \gamma_{th}\right\} = \Pr\left\{\max\left\{\Omega_4\beta_{S,E}^2,\right.\right.\\ &\left.\left.\min\left\{\Omega_2\beta_{S,R}^2 + \kappa_2, \Omega_5\beta_{R,E}^2\right\}\right\} > \gamma_{th}\right\}\\ &= 1 - \Pr\left\{\max\left\{\Omega_4\beta_{S,E}^2,\right.\right.\\ &\left.\left.\min\left\{\Omega_2\beta_{S,R}^2 + \kappa_2, \Omega_5\beta_{R,E}^2\right\}\right\} < \gamma_{th}\right\}\\ &= 1 - \Pr\left\{\Omega_4\beta_{S,E}^2 < \gamma_{th}\right\}\\ &\times \Pr\left\{\min\left\{\Omega_2\beta_{S,R}^2 + \kappa_2, \Omega_5\beta_{R,E}^2\right\} < \gamma_{th}\right\}\\ &= 1 - F_{\beta_{S,E}^2}\left(\frac{\gamma_{th}}{\Omega_4}\right)\\ &\times \left(1 - \Pr\left\{\min\left\{\Omega_2\beta_{S,R}^2 + \kappa_2, \Omega_5\beta_{R,E}^2\right\} > \gamma_{th}\right\}\right)\\ &= 1 - F_{\beta_{S,E}^2}\left(\frac{\gamma_{th}}{\Omega_4}\right)\\ &\times \left(1 - \Pr\left\{\Omega_2\beta_{S,R}^2 + \kappa_2 > \gamma_{th}\right\}\Pr\left\{\Omega_5\beta_{R,E}^2 > \gamma_{th}\right\}\right)\\ &= 1 - F_{\beta_{S,E}^2}\left(\frac{\gamma_{th}}{\Omega_4}\right) \qquad (16)\\ &\times \left(1 - \Pr\left\{\beta_{S,R}^2 > \frac{\gamma_{th}-\kappa_2}{\Omega_2}\right\}\Pr\left\{\beta_{R,E}^2 > \frac{\gamma_{th}}{\Omega_5}\right\}\right)\\ &= 1 - F_{\beta_{S,E}^2}\left(\frac{\gamma_{th}}{\Omega_4}\right)\\ &\times \left(1 - \overline{F}_{\beta_{S,R}^2}\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)\overline{F}_{\beta_{R,E}^2}\left(\frac{\gamma_{th}}{\Omega_5}\right)\right).\end{aligned}$$

Here, the fourth equation is obtained due to the independence of the direct and indirect links; the fifth equation is derived by utilizing the definition of the CDF of the RV $\beta_{S,E}^2$; the seventh equation is derived from the fact that the first and second hops of the indirect links are uncorrelated, and the final equation is obtained by utilizing the definition of the CCDF of RVs $\beta_{S,R}^2$, and $\beta_{R,E}^2$, respectively. Finally, by substituting $F_{\beta_{S,E}^2}\left(\frac{\gamma_{th}}{\Omega_4}\right)$, $\overline{F}_{\beta_{S,R}^2}\left(\frac{\gamma_{th}-\kappa_2}{\Omega_2}\right)$, and $\overline{F}_{\beta_{R,E}^2}\left(\frac{\gamma_{th}}{\Omega_5}\right)$ from (1) and (3) into (16), we derive (15). This concludes the proof.

Remark: *Upon inspection of* (11) *and* (15), *it is observed that increasing the scale parameter of the eavesdropper link from the relay to the eavesdropper enhances the IP. Similar observations hold for the scale parameter of the legitimate link from the relay to the destination. Furthermore, increasing the relay's transmit power facilitates an increase in both the IP and the OP.*

4 Numerical Results

In this section, simulation results based on the Monte Carlo method are presented to evaluate the performance of the proposed model. Unless otherwise stated, the parameters listed in Table II are used throughout this section. For the air-to-ground link, we consider three distinct cases: light shadowing (LS), moderate shadowing (MS), and heavy shadowing (HS). The corresponding parameter sets for these cases are provided in Table I.

Table I
Air-to-Ground channel parameters [8, 14].

Parameters	m	p	q
Heavy shadowing (HS)	1	0.063	0.0007
Moderate shadowing (MS)	3	0.163	0.15
Light shadowing (LS)	5	0.251	0.279

Table II
Simulation Parameters [22].

Parameters	Value
The iteration number of the Monte Carlo simulations	2.5×10^6
Carrier frequency	$f_c = 2.5$ GHz
Noise figure	6 dB
The maximal beam gain	$G_{\max} = 40$ dBi
The minimum beam gain	$G_{\min} = 0$ dBi
The main lobe beamwidth	$\tau = 30^o$
The expected target rate	$R_{\text{th}} = 100$ kbps
Correlation coefficient	$\lambda = 0.9$
Path-loss exponent for air-to-ground links	$\mu_{S,X}$ = 2.25
Path-loss exponent for terrestrial links	$\mu_{R,Y}$ = 2.85
Transmission bandwidth	BW = 1 MHz
Satellite transmit power	P_S = 30 dBm
Relay transmit power	P_R = 30 dBm
Transmission distance from S → X, X ∈ {R, E, U}	$d_{S,X}$ = 500 km (LEO)
Transmission distance from R → U	$d_{R,U}$ = 100 m
Transmission distance from R → E	$d_{R,E}$ = 80 m
Shape and scale parameters link from R → E	$m_{R,E}$ = 2.5 and $\varsigma_{R,E}$ = 2.5
Shape and scale parameters link from R → U	$m_{R,U}$ = 3.5 and $\varsigma_{R,U}$ = 3.5

Figure 2 examines the outage probability as a function of the satellite transmit power P_S under both heavy and light shadowing conditions. The results indicate

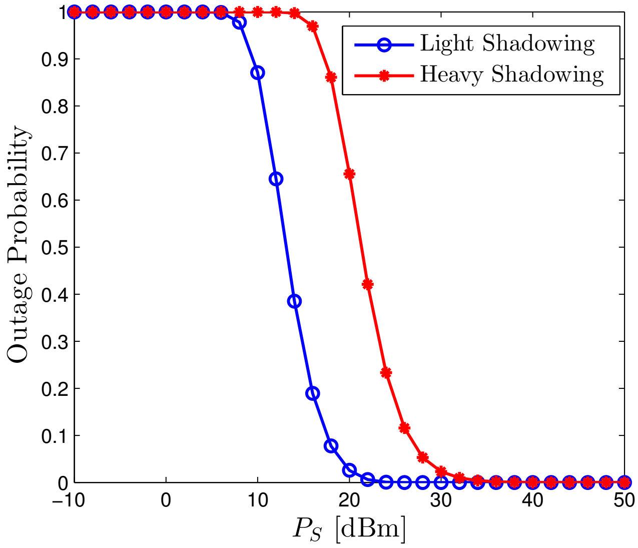

Figure 2. OP versus satellite transmit power for two cases, heavy and light shadowing. Solid lines are computed via (11) while markers are based on Monte-Carlo simulations.

that increasing P_S significantly enhances OP performance. Specifically, for both shadowing scenarios, the OP approaches zero when $P_S \geq 30$ dBm. Furthermore, Figure 2 demonstrates that light shadowing yields better performance than heavy shadowing. For example, to achieve an OP of 0.1, the light shadowing scenario requires only $P_S = 17$ dBm, whereas the heavy shadowing scenario necessitates a much higher P_S of 26 dBm.

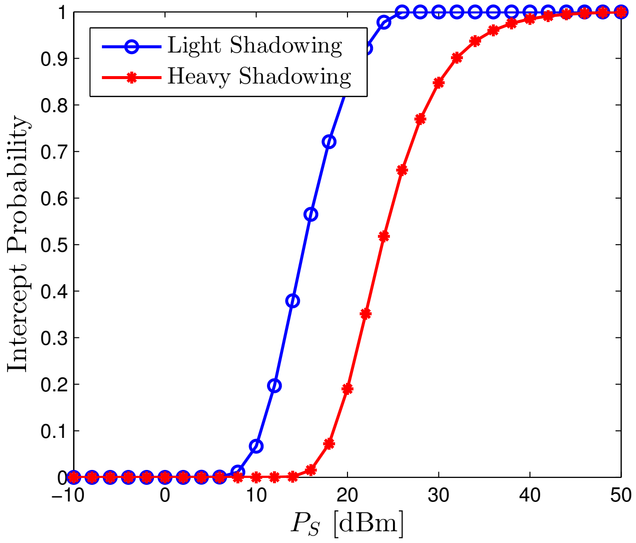

Figure 3. IP versus satellite transmit power for two cases, heavy and light shadowing. Solid lines are computed via (15) while markers are based on Monte-Carlo simulations.

Figure 3 analyzes the intercept probability as a function of the satellite transmit power P_S. The results clearly show that IP increases with P_S, indicating a decline in system security. This occurs because as P_S increases, the received signal strength improves not only at the legitimate user but also at the eavesdropper. Consequently, while system reliability improves, security is compromised. Additionally, the results confirm that the light shadowing scenario provides better overall performance compared to the heavy shadowing case.

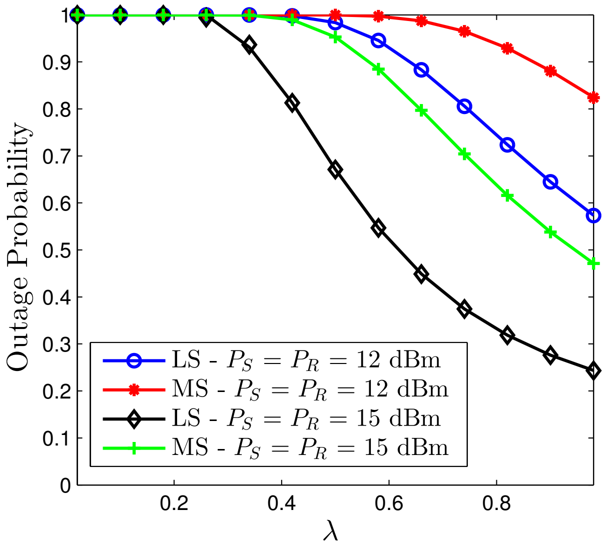

Figure 4. OP vs. correlation coefficient for two scenarios, light and average shadowing with $P_S = P_R = 12$ and $P_S = P_R = 15$ [dBm]. Solid lines are computed via (11) while markers are based on Monte-Carlo simulations.

Figure 4 illustrates the OP performance concerning the channel estimation coefficient λ. The results show that as $\lambda \to 1$, OP improves significantly, confirming that perfect CSI estimation yields the best performance. Additionally, Figure 4 highlights the notable impact of λ in both light and average shadowing scenarios. Specifically, for $P_S = P_R = 12$ dBm, when $\lambda < 0.6$, the OP remains at 1, whereas for $\lambda = 1$, the OP decreases to 0.83 in the average shadowing case. In contrast, for the light shadowing scenario, the effect of λ is more pronounced, with the OP varying by approximately 0.45 as λ increases from 0 to 1. Furthermore, increasing the transmit power at both P_S and P_R significantly improves the OP and compensates for channel correlation. For example, in the LS case, with $P_S = P_R = 15$ dBm, achieving OP = 0.6 requires $\lambda = 0.55$, whereas for the same OP value under $P_S = P_R = 12$ dBm, λ must be increased to 0.96.

Figure 5 illustrates the impact of the correlation coefficient λ on IP. In contrast to OP, IP increases with λ, indicating that higher channel estimation accuracy leads to a greater security risk. This suggests that when channel estimation errors are lower, the system becomes more susceptible to eavesdropping. Additionally, in favorable channel conditions, the vulnerability to wiretapping is further exacerbated. We observe once again that increasing the transmit power at both the source and the relay not only enhances OP performance but also raises the security risk, as IP increases. From Figures 4 and 5, it is evident that a trade-off exists between security and reliability in the considered system under the influence of the correlation coefficient. Therefore, a potential extension of this study is to

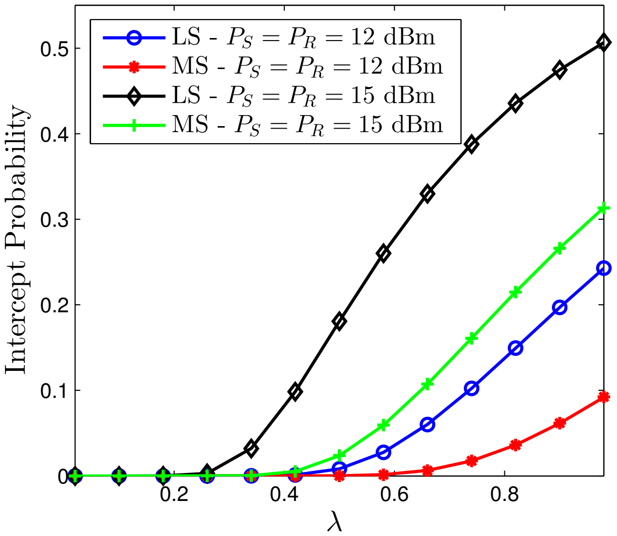

Figure 5. IP vs. correlation coefficient for two scenarios, light and average shadowing with $P_S = P_R = 12$ and $P_S = P_R = 15$ [dBm]. Solid lines are computed via (15) while markers are based on Monte-Carlo simulations.

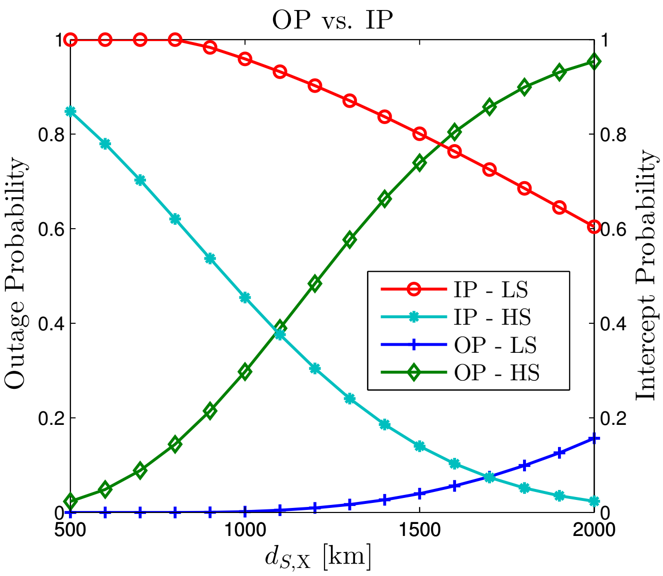

Figure 6. OP and IP vs. $d_{S,X}$ for two scenarios, heavy and light shadowing. All curves are plotted by (11) and (15).

determine an optimal λ that balances both IP and OP performance.

Figure 6 examines the variations in OP and IP as functions of the transmission distance from the satellite to the ground (i.e., satellite altitude). The results indicate that increasing the transmission distance improves system security (IP decreases) but simultaneously degrades system reliability (OP increases). This trade-off highlights the need for careful optimization of both satellite transmission distance and transmit power to achieve a balanced trade-off between security and reliability. Future research can explore strategies to optimize these parameters for enhanced system performance.

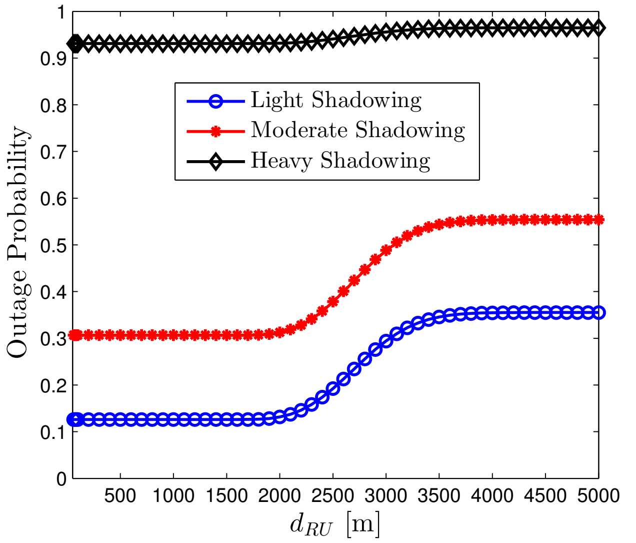

Figure 7. OP vs. $d_{R,U}$ for three scenarios, heavy, average, and light shadowing. Solid lines are computed via (11) while markers are based on Monte-Carlo simulations.

Figure 7 examines the outage probability performance as a function of the transmission distance between the relay and the main user ($d_{R,U}$) under different shadowing conditions, namely light, moderate, and heavy shadowing. The results indicate that increasing $d_{R,U}$ degrades OP performance across all scenarios. However, the extent of degradation varies significantly depending on the shadowing conditions. Specifically, under light shadowing, the worst OP remains just above 0.3, whereas under heavy shadowing, it approaches nearly 1. Interestingly, the OP remains constant when $d_{R,U}$ increases beyond a certain threshold. This phenomenon occurs because, as $d_{R,U} \to \infty$, the system performance becomes constrained by the direct link between the satellite and the user, rendering the impact of the relay negligible, regardless of the shadowing conditions.

We do not provide a corresponding figure for intercept probability versus $d_{R,U}$ because IP remains unaffected. Since $d_{R,U}$ only influences the legitimate user's channel and has no impact on the eavesdropper's channel, it does not alter system security.

Figure 8 illustrates the impact of antenna gain on OP under various shadowing conditions for a carrier frequency operating in the L-band at $f_c = 1.616$ GHz. The results indicate that favorable channel conditions play a crucial role in enhancing system reliability. Additionally, the findings emphasize the significant role of antenna gain in mitigating the severe path loss associated with long-distance air-to-ground or satellite communications. Specifically, across all scenarios, the system remains in outage when the maximum antenna gain $G_{\max}$ is below 12 dBi. However, when $G_{\max}$ reaches approximately 40 dBi, the system achieves near-perfect reliability, i.e., OP $\approx$ 0, regardless of shadowing conditions.

Figure 9 illustrates the IP performance as a function of the maximum antenna gain $G_{\max}$ under different shadowing conditions. Once again, we observe an inverse relationship between OP and IP with respect

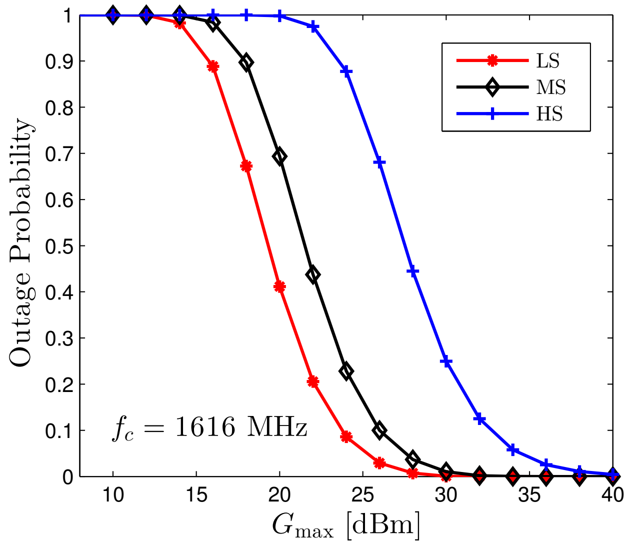

Figure 8. OP vs. $G_{\max}$ for various shadowing conditions with carrier frequency, $f_c = 1.616$ [GHz]. Solid lines are computed via (11) while markers are based on Monte-Carlo simulations.

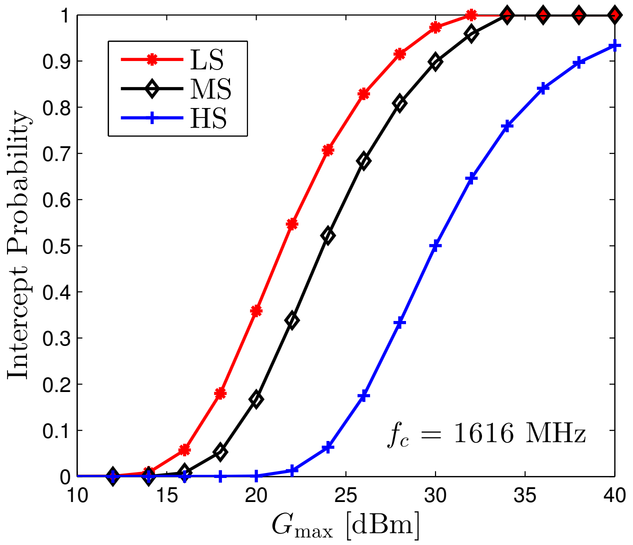

Figure 9. IP vs. $G_{\max}$ for various shadowing conditions with carrier frequency, $f_c = 1.616$ [GHz]. Solid lines are computed via (15) while markers are based on Monte-Carlo simulations.

to $G_{\max}$. Specifically, while OP decreases as $G_{\max}$ increases, IP exhibits a monotonically increasing trend. This indicates that higher antenna gain enhances system reliability but simultaneously makes the system more vulnerable to eavesdropping.

5 Conclusion

This paper investigated the performance of a hybrid satellite-terrestrial relay network, considering imperfect channel state information and directional antennas. Specifically, we analyzed two key performance metrics: OP and IP. Our results reveal that increasing the satellite transmit power enhances system reliability but simultaneously compromises security. Likewise, increasing the satellite altitude has opposing effects on OP and IP, emphasizing the need to optimize satellite altitude for balanced performance in hybrid satellite-terrestrial networks and satellite communications. Moreover, the impact of imperfect CSI primarily affects the legitimate channel, as only statistical CSI is available for the eavesdropper's channel. This study opens several avenues for future research. One promising direction is the application of friendly jamming techniques to enhance security without degrading reliability. Another potential extension is the integration of radio-frequency energy harvesting at the terrestrial relay and/or end users to improve the network's energy efficiency.

References

[1] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 70–109, 2021. [Online]. Available: https://doi.org/10.1109/comst.2020.3028247.

[2] T. Q. Duong, D. B. da Costa, M. Elkashlan, and V. N. Q. Bao, "Cognitive Amplify-and-Forward Relay Networks Over Nakagami-m Fading," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 5, pp. 2368–2374, 2012. [Online]. Available: https://doi.org/10.1109/tvt.2012.2192509.

[3] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2019. [Online]. Available: https://doi.org/10.1109/comst.2018.2865607.

[4] T. N. Nguyen, T. V. Chien, D.-H. Tran, V.-D. Phan, M. Voznak, S. Chatzinotas, Z. Ding, and H. V. Poor, "Security-Reliability Trade-Offs for Satellite-Terrestrial Relay Networks with a Friendly Jammer and Imperfect CSI," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 5, pp. 7004–7019, 2023. [Online]. Available: https://doi.org/10.1109/taes.2023.3282934.

[5] K. Guo, H. Shuai, X. Li, L. Yang, T. A. Tsiftsis, A. Nallanathan, and M. Wu, "Two-Way Satellite-HAP-Terrestrial Networks with Non-Orthogonal Multiple Access," *IEEE Transactions on Vehicular Technology*, pp. 1–15, 2023. [Online]. Available: https://doi.org/10.1109/tvt.2023.3307457.

[6] Y. Zhang, H. Zhang, H. Zhou, and W. Li, "Interference cooperation based resource allocation in NOMA terrestrial-satellite networks," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, Dec. 2021. [Online]. Available: https://doi.org/10.1109/globecom46510.2021.9685107.

[7] T. N. Nguyen, D.-H. Tran, T. Van Chien, V.-D. Phan, M. Voznak, and S. Chatzinotas, "Security and Reliability Analysis of Satellite-Terrestrial Multirelay Networks With Imperfect CSI," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2824–2835, 2023.

[8] T. N. Nguyen, L.-T. Tu, D.-H. Tran, V.-D. Phan, M. Voznak, S. Chatzinotas, and Z. Ding, "Outage Performance of Satellite Terrestrial Full-Duplex Relaying Networks With co-Channel Interference," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1478–1482, 2022, doi: 10.1109/LWC.2022.3175734.

[9] N.-L. Nguyen, C. D. Bui, S. N. Quang, T. T. Duy, T. N. Nguyen, and L.-T. Tu, "A Stacked Planar Antenna

Array with Frequency Selective Surface for Downlink Applications of Small Satellites," *IETE Journal of Research*, vol. 70, no. 7, pp. 6115–6123, Jan. 2024. [Online]. Available: http://dx.doi.org/10.1080/03772063.2023.2297385.

[10] W.-Q. Wang and D. Jiang, "Integrated Wireless Sensor Systems via Near-Space and Satellite Platforms: A Review," *IEEE Sensors Journal*, vol. 14, no. 11, p. 3903–3914, Nov. 2014. [Online]. Available: http://dx.doi.org/10.1109/JSEN.2014.2356580.

[11] T. N. Nguyen, L.-T. Tu, P. Fazio, T. Van Chien, C. V. Le, H. T. T. Binh, and M. Voznak, "On the Dilemma of Reliability or Security in Unmanned Aerial Vehicle Communications Assisted by Energy Harvesting Relaying," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 1, pp. 52–67, 2024.

[12] N.-T. Nguyen, H.-N. Nguyen, N.-L. Nguyen, A.-T. Le, T. N. Nguyen, and M. Voznak, "Performance Analysis of NOMA-Based Hybrid Satellite-Terrestrial Relay System Using mmWave Technology," *IEEE Access*, vol. 11, pp. 10 696–10 707, 2023.

[13] W. Zeng, J. Zhang, D. W. K. Ng, B. Ai, and Z. Zhong, "Two-Way Hybrid Terrestrial-Satellite Relaying Systems: Performance Analysis and Relay Selection," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7011–7023, 2019, doi: 10.1109/TVT.2019.2916992.

[14] S.-P. Le, T. N. Nguyen, T. Le-Tien, T. T. Duy, T.-T. Nguyen, D. W. K. Ng, L.-T. Tu, and M. Voznak, "On the Secrecy Performance of Reconfigurable Intelligent Surfaces-Assisted Satellite Networks Under Shadow-Rician Channels," *IEEE Transactions on Aerospace and Electronic Systems*, pp. 1–14, 2025.

[15] H. Son and M. Jung, "Phase Shift Design for RIS-Assisted Satellite-Aerial-Terrestrial Integrated Network," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 6, p. 9799–9806, Dec. 2023. [Online]. Available: http://dx.doi.org/10.1109/TAES.2023.3301464.

[16] V. S. Nguyen and T. H. Nguyen, "Energy Outage Analysis of Aerial UAV-Enabled SWIPT Deployments," *IEEE Access*, vol. 12, pp. 27 147–27 157, 2024.

[17] N.-T. Nguyen, H.-N. Nguyen, A.-T. Le, N. D. Nguyen, D.-T. Do, and M. Voznak, "Impact of CCI on performance analysis of downlink satellite-terrestrial systems: outage probability and ergodic capacity perspective," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, Auguts 2022. [Online]. Available: http://dx.doi.org/10.1186/s13638-022-02140-4.

[18] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, Amsterdam, 2007.

[19] L.-T. Tu and M. Di Renzo, "Analysis of millimeter wave cellular networks with simultaneous wireless information and power transfer," in *Proceedings of the 2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, 2017, pp. 39–43.

[20] L.-T. Tu, V. N. Q. Bao, and B. An, "On the performance of outage probability in underlay cognitive radio with imperfect CSI," in *Proceedings of the 2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, 2013, pp. 125–130.

[21] T. B. Doan and T. H. Nguyen, "Exploiting SWIPT for Coordinated-NOMA Systems Under Nakagami-m Fading," *IEEE Access*, vol. 12, pp. 19 216–19 228, 2024.

[22] Q. S. Nguyen, V. H. Nguyen, T. D. Tran, L. N. Nguyen, and L.-T. Tu, "On the Security and Reliability Trade-off of the Satellite Terrestrial Networks with Fountain Codes and Friendly Jamming," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 10, no. 4, p. 3, 12 2023, doi: 10.4108/eetinis.v10i4.4192.

Lam-Thanh Tu (M'25) received the Ph.D. degree from the University of Paris Sud, Paris-Saclay University, France, in 2018. From 2022, he has been with the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam. Since 2023, he has been an associate editor of the IEEE Communications Letters and a managing editor of the Advances in Electrical and Electronic Engineering. His research interests include stochastic geometry, LoRa networks, reconfigurable intelligent surfaces, covert communications, and artificial intelligence applications for wireless communications.

Tran Trung Duy received the Ph.D degree in electrical engineering from University of Ulsan, South Korea in 2013. From 2013, he joined Posts and Telecommunications Institute of Technology, HoChiMinh city campus (PTIT-HCM). From 2022, he is an associate Professor of Wireless Communications at PTIT-HCM. From 2017, he is an associate editor for REV Journal on Electronics and Communications Journal and EAI Endorsed Transactions on Industrial Networks and Intelligent Systems Journal. His major research interests are cooperative communications, cooperative multi-hop, cognitive radio, physical-layer security, energy harvesting, hardware impairments and Fountain codes.

Quang-Sang Nguyen received the B.E. degree in Electrical Engineering from Ho Chi Minh City University of Transport, Vietnam, in 2010, the M.E. degree in Telecommunications Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2013, and the Ph.D. degree in Electrical Engineering from the University of Ulsan, South Korea, in 2017. From 2017 to 2021, he was a Lecturer at Duy Tan University, Vietnam. Since May 2021, he has been a Lecturer at Ho Chi Minh City University of Transport, Vietnam. In September 2024, he joined the Post and Telecommunications Institute of Technology, Ho Chi Minh City, as a Lecturer. He also served as a Research Fellow at Queen's University Belfast, United Kingdom, where he contributed to advancements in wireless communications. Dr. Sang's research interests include cooperative communications, cognitive radio networks, physical layer security, non-orthogonal multiple access (NOMA), short-packet communications, and backscatter communications. His work primarily focuses on secure and energy-efficient communication solutions for next-generation wireless networks. Dr. Sang can be contacted via email at sangnq@ptit.edu.vn.

Tan N. Nguyen (member IEEE) was born in 1986 in Nha Trang City, Vietnam. He received a BS degree in electronics in 2008 from Ho Chi Minh University of Natural Sciences and an MS degree in telecommunications engineering in 2012 from Vietnam National University. He received a Ph.D. in communications technologies in 2019 from the Faculty of Electrical Engineering and Computer Science at VSB – Technical University of Ostrava, Czech Republic. He joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam, in 2013, and since then has been lecturing. He started as the **Editor-in-Chief** of Advances in Electrical and Electronic Engineering (AEEE) journal in 2023. He was appointed as **Associate Professor** of Electronics in 2024. His major interests are cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security.

Hong-Nhu Nguyen received a B.Sc. in Electronics Engineering from Ho Chi Minh City University of Technology in 1998 and an M.Sc. in Electronics Engineering from the University of Transport and Communications (Vietnam) in 2012. He is currently working as a lecturer at Saigon University, Ho Chi Minh City, Vietnam. He received a Ph.D. in communication technology from the Faculty of Electrical Engineering and Computer Science at VSB - Technical University of Ostrava, Czech Republic in 2021. His research interest includes applied electronics, wireless communications, cognitive radio, NOMA, and energy harvesting. He can be contacted at email: nhu.nh@sgu.edu.vn

Hien Quang Ta received the B.S. degree in electrical and electronic engineering from the Ho Chi Minh University of Technology, Vietnam, and the Ph.D. degree in electrical engineering from Iowa State University, Ames, IA, USA. He is currently a Lecturer with the School of Electrical Engineering, International University — Vietnam National University, Ho Chi Minh City, Vietnam. His current research interests are primarily in the area of wireless communications and networking.

Nguyen Hong Giang was born in Hai Phong City, Vietnam. He received his B.S. degree in Communication Command from Telecommunications University, Ministry of Defence, Vietnam, in 2002, and his B.Eng. degree in Electrical Engineering from Le Quy Don Technical University, Hanoi, Vietnam, in 2006. He obtained his M.Eng. degree in Electronics Engineering from Posts and Telecommunications Institute of Technology, Vietnam, in 2011. He obtained his Ph.D. in Computer Science from the University of Da Nang in 2018. He is currently a lecturer at the Faculty of Information Technology, Telecommunications University, Nha Trang, Khanh Hoa Province, Vietnam. His research interests include Computer Networking, Physical Security, Network Security, and Secure Machine Learning.