

# Security and Reliability Analysis of Satellite-Terrestrial Multi-Relay Networks with Imperfect CSI

Tan N. Nguyen, *Member, IEEE*, Dinh-Hieu Tran, *Graduate Student Member, IEEE*, Trinh Van Chien, *Member, IEEE*, Van-Duc Phan, Miroslav Voznak, *Senior Member, IEEE*, Symeon Chatzinotas, *Senior Member, IEEE*,

**Abstract**—This work investigates the security and reliability analysis for a novel satellite-terrestrial (SatTer) network. Specifically, a satellite attempts to transmit confidential information to a ground user (GU) via the support of multiple relay nodes in the presence of an eavesdropper that tries to overhear the information. A friendly jammer is deployed to improve the secure transmission between the satellite and the relays. Furthermore, satellite-to-relay generalized Rician fading channels and imperfect channel state information (CSI) are deployed to examine a general system model. In this context, the closed-formed expressions for the outage probability (OP) and intercept probability (IP) are derived corresponding to an amplify-and-forward (AF)-based relaying scheme, which is challenging and has not been studied before. Finally, the exactness of the mathematical analyses is validated through Monte Carlo simulations. Furthermore, the effects of various key parameters (e.g., channel estimation errors, satellite’s transmit power, relay’s transmit power, number of relays, and fading severity parameter) are examined.

**Index Terms**—Cooperative relay, imperfect CSI, physical layer security, satellite communications, shadowed Rician channel

## I. INTRODUCTION

Recently, the Internet of Things (IoT) has been spread worldwide due to its various applications such as smart cities, smart farming, wearable devices, healthcare, and smart communications [1]–[3]. Nevertheless, the explosive growth of the number of IoT devices (IoTDs) has brought new challenges to the traditional cellular networks due to its

Manuscript received XXX; revised XXX; accepted XXX. Date of publication XXX; date of current version XXX. This research was financially supported by Van Lang University, Vietnam, and was supported in part by the Ministry of Education, Youth and Sports of the Czech Republic under the grant SP2021/25 and e-INFRA CZ (ID:90140). (*Corresponding author: Van-Duc Phan.*)

Tan N. Nguyen is with the Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam. (e-mail:nguyennhattan@tdtu.edu.vn).

Dinh-Hieu Tran is currently with Nokia Bell Labs, France, and was with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), the University of Luxembourg, Luxembourg. (e-mail:dinh-hieu.tran@nokia.com).

Trinh Van Chien is with the School of Information and Communication Technology (SoICT), Hanoi University of Science and Technology (HUST), 100000 Hanoi, Vietnam. (e-mail: chientv@soict.hust.edu.vn).

Van-Duc Phan is at Faculty of Automotive Engineering, School of Engineering and Technology, Van Lang University, Ho Chi Minh City, Vietnam (email: duc.pv@vlu.edu.vn).

Miroslav Voznak is at VSB – Technical University of Ostrava, 17. listopadu 2172/15, 708 00 Ostrava, Czech Republic. (e-mail: miroslav.voznak@vsb.cz).

Symeon Chatzinotas is at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), the University of Luxembourg, Luxembourg. (e-mail: symeon.chatzinotas@uni.lu).

© 2021 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

restricted resources, e.g., fixed locations, limited spectrum, and power [4]–[6]. Furthermore, IoTDs are usually distributed in harsh environments such as forests, deserts, mountains, or maritime. Therefore, it is more difficult for the current cellular networks to provide seamless and cost-efficient services to a massive amount of IoTDs in these scenarios [7]. Thanks to recent projects such as SpaceX and OneWeb, SPUTNIX, thousands of low earth orbit (LEO) satellites are being launched to provide global coverage and high throughput supporting the traditional terrestrial communication networks [8]–[10]. Therefore, satellite communications have become a promising solution to overcome the limitations of IoT networks.

Besides many advantages, satellite communications (SatComs) are not without limitations [5], [11]. Due to considerable distance, obstacles, and shadowing effects between satellite and ground users (GUs), Line-of-sight (LoS) links between them are not always guaranteed [12]. Therefore, the hybrid satellite-terrestrial relay network (HSTRN) has been proposed to leverage the benefits of both terrestrial and space communications to improve network performance [13]–[18]. In [13], the authors investigated the HSTRN by considering the direct link between satellite and destination, interference at relay and destination, and the hardware impairment (HI) effects. In [14], the authors studied the HSTRN by optimizing the beam-forming factors at the relay to maximize the total capacity. Moreover, they proposed two scheduling schemes, namely user fairness and best user scheduling. The work in [15] analyzed the performance analysis of two-way HSTRN, where the transmission links between relay to satellite and relay to users follow  $\kappa$ - $\mu$  shadowed fading and Nakagami-m distribution, respectively. In contrast to [13], [14] only considered a fixed terrestrial user as a relay, an unmanned aerial vehicle (UAV) has been proposed to act as a relay in [16]–[20].

Beyond the in-depth analysis of satellite-terrestrial networks in the works mentioned above, they did not consider the security aspect of their systems. Due to the broadcast nature and wide coverage range of SatComs, the security and privacy of this communication system are not guaranteed. Conventional cryptography methods have been applied at the upper layers to improve information security. Nevertheless, these encryption methods require a high computational burden due to service management and key distribution [21], [22]. In this context, physical layer security (PLS) can be considered a complementary solution, where it can achieve secure transmission by leveraging the characteristics of wireless channels [21], [23]–[28]. The authors in [21] studied the PLS in HSTRN in which a multi-antenna satellite tried to communicate with

multi-antenna destinations via the help of multi-antenna relays in the presence of an eavesdropper. Non-orthogonal multiple access (NOMA) and HI were investigated with HSTRN in [23]. Moreover, the authors in [23] studied two security schemes, i.e., colluding and non-colluding scenarios. In [24], UAVs were played as a flying relay (or an eavesdropper) to transfer (or overhear) information from source to destination in HSTRN. In [25], the authors proposed a novel hybrid satellite-aerial-terrestrial networks (HSATNs), where ground users could obtain content from a cache-enabled UAV or a NOMA-based satellite. Moreover, the authors derived the outage and hit probability of the considered system model with stochastic geometry. Regarding the relay/backscatter-aided terrestrial communications, the authors in [26]–[28] derived the closed-form expression of the secrecy channel capacity, OP, and IP to demonstrate the system robustness under attacks.

The previous works have addressed the different new challenges in HSTRN, such as HI, NOMA, interference, two-way relaying, and UAV-enabled relaying. Nevertheless, none of these works consider a jammer to improve the information secrecy. Recently, few research works have investigated PLS in HSTRN with jammer [29]–[33]. The work in [29] studied the secrecy problem in multi-beam satellite systems by applying the cooperative jamming method. Moreover, they proposed an alternating algorithm by jointly optimizing the power allocation and beamforming factors. The authors in [30] investigated a satellite and UAV system under hostile jamming environments. The authors designed the UAV trajectory to avoid jamming signals, where the UAV performed reconnaissance tasks and transferred the collected data to the satellite. The work in [31] investigated physical layer security in cognitive satellite-terrestrial networks with jamming, where dual-hop communications were considered under RF and optical links in the first and second hop, respectively. The authors in [32] investigated the closed-form expressions of the secrecy channel capacity and OP for a single relay and perfect CSI. In [33], the work considered a new system model in which intelligent reflecting surface (IRS) enabled PLS in satellite-terrestrial networks.

Despite significant achievements in the above studies, most of the previous works have concentrated on resource allocation perspectives under the availability of instantaneous channel state information (CSI) [5], [11], [14], [16]–[20], [29], [30]. In contrast, there are only a few works on deriving the analytical results for satellite-terrestrial integrated networks [13], [21], [23], [31], but only based on perfect CSI and not for the IP and OP under the physical security perspectives with a friendly jammer. Consequently, there is still room for research on security and reliability in satellite-terrestrial (SatTer) networks. In this paper, we present an amplify-and-forward (AF)-based SatTer network for secure communication in the presence of an

eavesdropper.<sup>1</sup> The main contributions of this work are given as follows:

- To the best of our knowledge, this is the first work that mathematically obtains the closed-form expressions for the IP and OP in AF-based SatTer networks in the presence of an eavesdropper with imperfect CSI and generalized shadowed Rician channels. In particular, a friendly jammer is considered to broadcast the artificial noise to decrease the eavesdropping ability of the illegitimate party. Furthermore, the closed-form expressions based on particular CSI offer low-cost designs to evaluate the IP and OP in practice.
- Monte Carlo simulations are performed to verify the correctness of mathematical analyses for various parameter settings. Moreover, the simulations also provide the trade-off between security and reliability in the considered system model.
- Insightful discussions on the impact of different key parameters of SatTer networks on its security-reliability trade-off are numerically provided. Specifically, the satellite’s transmit power, number of relays, and relay transmit power can be suitably selected to reduce the eavesdropper’s effects and enhance the system performance.

The remainder of the paper is organized as follows: The system model and problem formulation are given in Section II. The derivation of key performance metrics, including the OP and throughput of the proposed model, is presented in Section III-A. Numerical results are shown in Section IV. Section V concludes the paper.

## II. SYSTEM MODEL

We study the downlink (DL) scenario of the physical layer security in an HSTRN. The system model consists of one satellite  $S$  communicating with one destination  $D$  via the support of multiple relays  $R_n$  with  $n \in \{1, \dots, N\}$ . Moreover, due to the masking effect and severe shadowing, it does not exist a direct link between  $S \rightarrow D$  [21], [34], [35]. Besides, an eavesdropper  $E$  tries to wiretap confidential information from relay  $R_n$  [36]–[38]. To reduce the eavesdropping ability of the illegitimate party, we deploy one friendly jammer  $J$  that broadcasts the artificial noise.<sup>2</sup> Notably, the jamming noise is known to the legitimate destination and it can be canceled, while it is unknown to the eavesdropper [31], [41].

### A. Channel model

In practice, it is difficult to obtain perfect channel state information (CSI) due to channel estimation errors (CEEs).

<sup>1</sup>In this paper, we select the AF relaying for analysis since it is easy to implement in practice due to its simple hardware with the only main cost of an amplifier. In contrast, a DF has costly hardware with at least one radio frequency chain on other supplementary components to decode and separate the noise and desired signal. A consideration of the DF relaying is left for future work.

<sup>2</sup>Broadcasting the artificial noise is one solution for physical security as no prior information about the network is available. Accordingly, the energy consumption for a friendly jammer is necessary to boost the security of the legitimate destination. Some particular devices can be considered as friendly jammers to broadcast artificial noise, for instance, in military applications [39]. The legitimate destination knows the signals transmitted from the friendly jammer using a specific signal encoding structure [40].

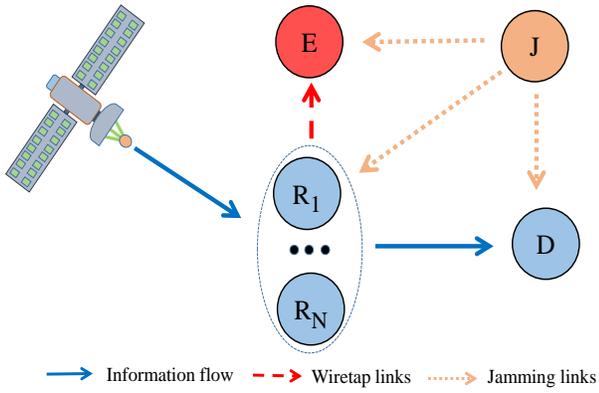


Fig. 1. The considered system model

Consequently, channel estimation methods, such as linear minimum mean square error (MMSE) channel estimator [42] are necessary to obtain CSI. Therefore, the channel can be modeled as

$$\hat{h}_i = h_i + e_i, \quad (1)$$

where  $e_i$  with  $i \in (\text{SR}_n, \text{R}_n\text{D}, \text{R}_n\text{E}, \text{JE}, \text{JR}_n, \text{JD})$  is the CEEs with  $e_i \sim CN(0, \mu_i^2)$  and  $\hat{h}_i$  signifies the estimated channel of the real channel  $h_i$ . Without loss of generality, let us assume that the estimated channels between two GUs in terrestrial communications follow block Rayleigh fading, whereas channel coefficients are unchanged during one transmission block and vary over different blocks.<sup>3</sup> As a result, the channel gains can be represented as  $\gamma_{\text{R}_n\text{E}} = |h_{\text{R}_n\text{E}}|^2$ ,  $\gamma_{\text{R}_n\text{D}} = |h_{\text{R}_n\text{D}}|^2$ , etc. are exponential random variables (RVs). More specifically, the probability density function (PDF) and cumulative distribution function (CDF) are respectively given as [45], [46]:

$$F_X(x) = 1 - \exp(-\lambda x), \quad (2)$$

$$f_X(x) = \frac{\partial F_X(x)}{\partial x} = \lambda \exp(-\lambda x), \quad (3)$$

where  $\lambda$  is the rate parameter of  $X$ . Next, we consider Shadowed-Rician fading model for the satellite links [35], which has been widely applied in different satellite services using the S-band, UHF-band, Ka-band, and L-band [47]. Therein, the PDF of  $\gamma_{\text{SR}_n} = |h_{\text{SR}_n}|^2$  between  $\text{S} \rightarrow \text{R}_n$  is given by [21], [34]

$$f_{\gamma_{\text{SR}_n}}(x) = \alpha_n \exp(-\beta_n x) {}_1F_1(m_n; 1; \delta_n x), \quad x \geq 0, \quad (4)$$

where  $\alpha_n \triangleq \beta_n \left( \frac{2b_n m_n}{2b_n m_n + \Omega_n} \right)^{m_n}$ ,  $\beta_n \triangleq \frac{1}{2b_n}$ ,  $\delta_n \triangleq \frac{\beta_n \Omega_n}{2b_n m_n + \Omega_n}$ , with  $\Omega_n$  and  $2b_n$  denote the average power of LoS and multi-path components at relay  $\text{R}_n$ , respectively. Moreover,  $m_n$  implies the fading severity parameter at relay  $\text{R}_n$  and  ${}_1F_1(\cdot; \cdot; \cdot)$  denotes the confluent hyper-geometric function of the first kind [48, Eq.9.210.1]. For arbitrary integer-valued fading severity parameters, one can simplify  ${}_1F_1(m_n; 1; \delta_n x)$

in (3) to express the PDF of  $\gamma_{\text{SR}_n}$  as [49]

$$f_{\gamma_{\text{SR}_n}}(x) = \alpha_n \sum_{k=0}^{m_n-1} \zeta_n(k) x^k \exp(-(\beta_n - \delta_n)x), \quad (5)$$

where the following definition holds

$$\zeta_n(k) = \frac{(-1)^k (1 - m_n)_k \delta_n^k}{(k!)^2}, \quad (6)$$

and  $(\cdot)_k$  is the Pochhammer symbol [48, Eq. p. xliii]. The corresponding CDF denoted by  $F_{\gamma_{\text{SR}_n}}(x)$  is formulated as

$$F_{\gamma_{\text{SR}_n}}(x) = \Pr(\gamma_{\text{SR}_n} < x) = \int_0^x f_{\gamma_{\text{SR}_n}}(x) dx, \quad (7)$$

which can be obtained in closed form as follows:

$$\begin{aligned} F_{\gamma_{\text{SR}_n}}(x) &= 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^k \frac{\zeta_n(k) k!}{p!} \vartheta_1^{-A_1} x^p \exp(-\vartheta_1 x) \\ &= 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^k \frac{(-1)^k (1 - m_n)_k \delta_n^k}{k! p!} \vartheta_1^{-A_1} x^p \exp(-\vartheta_1 x), \end{aligned} \quad (8)$$

where  $A_1 \triangleq k + 1 - p$ ,  $\vartheta_1 \triangleq \beta_n - \delta_n$ . The first equality in (8) is obtained by applying [48, Eq.3.351.1], while the second equality in (8) is achieved by utilizing the detail expression of  $\zeta_n(k)$  defined in (6) and then doing some algebra. We hereafter exploit the fundamental achievement in (8) to work on the analysis of the IP and OP.

## B. Information transmission

In this subsection, we describe the AF relaying protocol that is used to forward the data from  $\text{S} \rightarrow \text{R}_n$ . Because all GUs work in the half-duplex mode, the signal transmission from  $\text{S} \rightarrow \text{D}$  through two-time phases [50], [51]. In the first one,  $\text{S}$  transmits its data  $x_S$  to the relay  $\text{R}_n$ . Therefore, the received signal at  $\text{R}_n$  can be expressed as:

$$y_{\text{R}_n} = \hat{h}_{\text{SR}_n} x_S + n_{\text{R}_n} = (h_{\text{SR}_n} + e_{\text{SR}_n}) x_S + n_{\text{R}_n}, \quad (9)$$

where  $x_S$  is the symbol signal with  $\text{E}\{|x_S|^2\} = P_S$ ,  $\text{E}\{\cdot\}$  denotes the expectation operation;  $n_{\text{R}_n}$  is the zero mean additive white Gaussian noise (AWGN) with variance  $N_0$  at relay  $\text{R}_n$ .

In the second phase, relay  $\text{R}_n$  first amplifies received signal  $y_{\text{R}_n}$  with scale parameter  $G$  and then relays it to the destination  $\text{D}$ . At the same time, the eavesdropper can detect the transmitted signal from  $\text{R}_n$  and try to overhear the confidential information. The cooperative jamming technique can be used to reduce the eavesdropping link's quality. Specifically, the single antenna friendly jammer ( $\text{J}$ ) is employed to continuously generate artificial noises to the eavesdropper. Furthermore, the relays and destination are the legitimate users and are assumed to be known the coding sequence of the jammer. Therefore, they can cancel the jammer's interference. Furthermore, it is assumed that the eavesdropper cannot intercept signal from  $\text{S}$  due to the masking effect or severe fading. Therefore, the eavesdropper monitors only transmitted signal from relay  $\text{R}_n$  [21], [52]. Consequently, the received signal at the destination

<sup>3</sup>The channel model considered in this paper matches well with actual measurements from the propagation environments with rich scatterers around the receivers and without a dominant path [43]. A more general model such as [44] should be considered in a future work.

D and the eavesdropper E are respectively given as

$$\begin{aligned} y_D &= (h_{R_n D} + e_{R_n D}) G_{Y_{R_n}} + n_D \\ &= (h_{R_n D} + e_{R_n D}) G[(h_{SR_n} + e_{SR_n})x_S + n_{R_n}] + n_D, \end{aligned} \quad (10)$$

$$\begin{aligned} y_E &= (h_{R_n E} + e_{R_n E}) G[(h_{SR_n} + e_{SR_n})x_S \\ &\quad + n_{R_n}] + (h_{JE} + e_{JE})x_J + n_E, \end{aligned} \quad (11)$$

where  $n_D$  and  $n_E$  are the zero mean AWGN with variance  $N_0$  at  $n_D$  and  $n_E$ , respectively;  $x_J$  the transmit signal at jammer J and E  $\{ |x_J|^2 \} = P_J$ . Based on (9), the scale parameter G can be determined as

$$G = \sqrt{\frac{P_{R_n}}{P_S (\gamma_{SR_n} + \mu_{SR_n}^2) + N_0}}. \quad (12)$$

where  $P_{R_n}$  is the transmit power of  $R_n$ . For simplicity, we assume that CEEs values at each S-R<sub>n</sub> or R<sub>n</sub>-D or R<sub>n</sub>-E links are the same, i.e.,  $\mu_{SR_1}^2 = \mu_{SR_2}^2 = \dots = \mu_{SR_n}^2 = \mu_{SR}^2, \forall n \in \{1, 2, \dots, N\}$ , etc. From (10), (11) and (12), the signal to noise ratio (SNR) at D and eavesdropper E can be given as

$$\gamma_D = \frac{\Psi \Phi \gamma_{SR_n} \gamma_{R_n D}}{\gamma_{R_n D} \Phi \vartheta_2 + \gamma_{SR_n} \Psi (\mu_{RD}^2 \Phi + 1) + \Xi}, \quad (13)$$

$$\gamma_E = \frac{\Psi \Phi \gamma_{SR_n} \gamma_{R_n E}}{\gamma_{R_n E} \Phi \vartheta_2 + \gamma_{SR_n} \Psi \Lambda_1 + \gamma_{JE} \Theta \vartheta_2 + \Lambda}, \quad (14)$$

where  $\Psi \triangleq \frac{P_S}{N_0}$ ,  $\Xi \triangleq (\Psi \mu_{SR}^2 + 1) (\Phi \mu_{RD}^2 + 1)$ ,  $\Phi \triangleq \frac{P_R}{N_0}$ ,  $\vartheta_2 \triangleq (\Psi \mu_{SR}^2 + 1)$ ,  $\Theta \triangleq \frac{P_J}{N_0}$ ,  $\Lambda \triangleq (\Psi \mu_{SR}^2 + 1) (\Phi \mu_{RE}^2 + \Theta \mu_{JE}^2 + 1)$ ,  $\Lambda_1 \triangleq (\mu_{RE}^2 \Phi + \Theta \mu_{JE}^2 + \Theta \gamma_{JE} + 1)$ . In (13), we assume that the legitimate destination knows the coding sequence of the friendly jammer, they can exploit the same mechanism to generate artificial noise, e.g., using a standard hardware with the same random seed [31], [41] or the orthogonality between artificial noise and legitimate channel [40].

*Remark 1:* In this work, we apply the partial relay selection (PRS) method. Specifically, we propose a sub-optimal relay selection protocol in which the best relay  $a$ -th is selected, as follows:<sup>4</sup>

$$a = \underbrace{\arg \max}_{n=1,2,\dots,N} \{ \gamma_{SR_n} \} \Leftrightarrow \gamma_{SR_a} = \max_{n=1,2,\dots,N} \{ \gamma_{SR_n} \}. \quad (15)$$

To the best of our knowledge, all mentioned works in the literature, for example, [21], [49], only considered identical independent distribution (i.i.d.) Shadowed-Rician fading channels with the same parameters, i.e.,  $m_n$ ,  $\Omega_n$ , and  $b_n$ , between  $S \rightarrow R_n, \forall n = \{1, \dots, N\}$ . Motivated by these observations, in this work, we investigate the generalized i.i.d. Shadowed-Rician channel, where S can transmit its information to each relay with different parameters. Alternatively, our framework is a generic version of the previous works. The CDF of  $\gamma_{SR_a}$  can be computed as:

$$F_{\gamma_{SR_a}}(x) = \Pr \left( \max_{n=1,2,\dots,N} \{ \gamma_{SR_n} \} < x \right) = \prod_{n=1}^N F_{\gamma_{SR_n}}(x). \quad (16)$$

<sup>4</sup>The partial relay selection in (15) is sufficiently simple to implement in practice where the requirements of low latency are needed. However, it is a sub-optimal selection, and a better one is left for future work.

In order for further processing, by substituting (8) into (16), it yields the following equality

$$\begin{aligned} F_{\gamma_{SR_a}}(x) &= \prod_{n=1}^N \left( 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^k \frac{(-1)^k (1-m_n)_k (\delta_n)^k}{k! p!} \right. \\ &\quad \left. \vartheta_1^{-(k+1-p)} \times x^p \exp(-\vartheta_1 x) \right). \end{aligned} \quad (17)$$

Let us denote the second term of the product in (17) as  $x_n = \sum_{k=0}^{m_n-1} \sum_{p=0}^k \frac{\alpha_n (-1)^k (1-m_n)_k (\delta_n)^k}{k! p! \vartheta_1^{A_1}} x^p \exp(-\vartheta_1 x)$ , then we obtain the following result

$$\begin{aligned} F_{\gamma_{SR_a}}(x) &= \prod_{n=1}^N (1 - x_n) \\ &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \underbrace{\sum_{n_1=1}^N \dots \sum_{n_n=1}^N \prod_{t=1}^n x_{n_t}}_{n_1 \neq n_2 \dots \neq n_n}. \end{aligned} \quad (18)$$

We note that the result in (18) is obtained from (17) by induction. From the obtained result in (18), we further manipulate the expression  $x_{n_t}$  follows:

$$\begin{aligned} \prod_{t=1}^n x_{n_t} &= \sum_{k_1=0}^{m_{n_1}-1} \sum_{p_1=0}^{k_1} \dots \sum_{k_n=0}^{m_{n_n}-1} \sum_{p_n=0}^{k_n} \prod_{t=1}^n \alpha_{n_t} \times \\ &\quad \frac{(-1)^{k_t} (1-m_{n_t})_{k_t} (\delta_{n_t})^{k_t}}{k_t! p_t! \vartheta_3^{A_3}} x^{A_2} \exp \left( - \sum_{t=1}^n \vartheta_3 x \right), \end{aligned} \quad (19)$$

where  $A_2 \triangleq \sum_{t=1}^n p_t$ ,  $A_3 \triangleq k_t + 1 - p_t$ ,  $\vartheta_3 \triangleq \beta_{n_t} - \delta_{n_t}$ . After that, the closed-form expression of the CDF of  $\gamma_{SR_a}$  is given in Lemma 1.

*Lemma 1:* Based on (18) and (19),  $F_{\gamma_{SR_a}}(x)$  can be expressed as

$$\begin{aligned} F_{\gamma_{SR_a}}(x) &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum^* \alpha_{n_t} \\ &\quad \times \frac{(-1)^{k_t} (1-m_{n_t})_{k_t} (\delta_{n_t})^{k_t}}{k_t! p_t! \vartheta_3^{A_3}} x^{A_2} \exp \left( - \sum_{t=1}^n \vartheta_3 x \right), \end{aligned} \quad (20)$$

where the summation notation  $\sum^*$  is defined as

$$\sum^* = \sum_{n_1=1}^N \dots \sum_{n_n=1}^N \sum_{k_1=0}^{m_{n_1}-1} \sum_{p_1=0}^{k_1} \dots \sum_{k_n=0}^{m_{n_n}-1} \sum_{p_n=0}^{k_n} \prod_{t=1}^n. \quad (21)$$

The preliminary result on the CDF of  $\gamma_{SR_a}$  visualizes the influences of all the available relays to the partial relay selection and the SNR value. We hereafter utilize the key result in (20) to analyze the IP and OP.

### III. PERFORMANCE ANALYSIS

This section derives the analytical results of the OP and IP with insightful observations.

### A. Outage Probability (OP) Analysis

For a given maximum SNR value, the OP of system can be defined as:

$$\text{OP} = \Pr(\gamma_D < \gamma_{th}), \quad (22)$$

where  $\gamma_{th} = 2^{2C_{th}} - 1$ ,  $C_{th}$  is the predefined threshold of the system, and  $\Pr(\cdot)$  is the probability of an event.

*Theorem 1:* The analytical expression of the OP can be mathematically represented as

$$\begin{aligned} \text{OP} &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \\ &\sum_{k_t}^* \alpha_{n_t} \frac{2(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RD}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\times \left( \frac{\gamma_{th}}{\Psi} \right)^{A_2} \exp \left( - \sum_{t=1}^n \vartheta_3 \frac{\gamma_{th} \vartheta_2}{\Psi} - \lambda_{RD} \tilde{\gamma}_{th} \right) \\ &\times \sum_{q=0}^{A_2} \binom{A_2}{q} \vartheta_2^{A_2-q} \tilde{\Xi}^q \left( \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \tilde{\Xi}}{\lambda_{RD} \Psi} \right)^{\frac{-q+1}{2}} \\ &K_{-q+1} \left( 2 \sqrt{\sum_{t=1}^n \vartheta_3 \frac{\gamma_{th} \lambda_{RD} \tilde{\Xi}}{\Psi}} \right), \end{aligned} \quad (23)$$

where  $K_v(\cdot)$  is the modified Bessel function of the second kind and  $v$ -th order.

*Proof:* See Appendix A. ■

From (23), the OP is upper bounded by one ideally. Nonetheless, the complicated term shows a reduction in the amount of the OP is complicatedly expressed by several aspects, for example, the relay selection and the effectiveness of the friendly jammer. We notice that an asymptotic analysis is challenging and left for future work since the transmit power of the satellite and the selected relay is independent of each other.

### B. Intercept Probability (IP) Analysis

The confidential information can be intercepted if eavesdropper successfully decodes received signals, i.e.,  $\gamma_E \geq \gamma_{th}$ . Therefore, the IP can be defined by following the similar methodology in [53], [54] as follows

$$\text{IP} = \Pr(\gamma_E \geq \gamma_{th}) = 1 - \Pr(\gamma_E < \gamma_{th}). \quad (24)$$

In order to obtain the analytical from, we base on (14) and (24) to reformulate the IP as follows

$$\begin{aligned} \text{IP} &= 1 - \Pr \left( \frac{\Psi \Phi \gamma_{SR_a} \gamma_{R_a E}}{\Lambda_6} < \gamma_{th} \right) \\ &= 1 - \int_0^{+\infty} Q \times f_{\gamma_{JE}}(x) dx, \end{aligned} \quad (25)$$

where  $Q \triangleq \Pr \left( \frac{\Psi \Phi \gamma_{SR_a} \gamma_{R_a E}}{\Lambda_6} < \gamma_{th} \right)$ ,  $\Lambda_6 \triangleq \gamma_{R_a E} \Phi \vartheta_2 + \gamma_{SR_a} \Psi \vartheta_5 + \gamma_{JE} \Theta \vartheta_2 + \Lambda$ , and  $\vartheta_5 \triangleq (\mu_{RE}^2 \Phi + \Theta \mu_{JE}^2 + \Theta \gamma_{JE} + 1)$ . From on (25),  $Q$  can be

calculated as

$$\begin{aligned} Q &= \Pr \left( \Psi \Phi \gamma_{SR_a} \gamma_{R_a E} < \gamma_{th} (\Lambda_7 + \Lambda_8) \right) \\ &= \Pr \left( \Psi \gamma_{SR_a} [\Phi \gamma_{R_a E} - \gamma_{th} \Lambda_8] < \gamma_{th} \Lambda_7 \right) \\ &= \begin{cases} \Pr \left( \gamma_{SR_a} < \frac{\gamma_{th} \Lambda_7}{\Lambda_9} \right), & \text{if } \gamma_{R_a E} > \frac{\gamma_{th} \vartheta_5}{\Phi} \\ 1 & \text{if } \gamma_{R_a E} \leq \frac{\gamma_{th} \vartheta_5}{\Phi} \end{cases} \\ &= \int_0^{\Delta(x)} f_{\gamma_{R_a E}}(y) dy \\ &+ \int_{\Delta(x)}^{+\infty} F_{\gamma_{SR_a}} \left( \frac{\gamma_{th} [y \vartheta_2 + \Omega(x)]}{\Psi [y - \Delta(x)]} \right) f_{\gamma_{R_a E}}(y) dy. \end{aligned} \quad (26)$$

where  $\Lambda_7 \triangleq [\gamma_{R_a E} \Phi \vartheta_2 + x \Theta \vartheta_2 + \Lambda]$ ,  $\Lambda_8 \triangleq \gamma_{SR_a} \Psi (\mu_{RE}^2 \Phi + \Theta \mu_{JE}^2 + \Theta x + 1)$ ,  $\Lambda_9 \triangleq \Psi [\Phi \gamma_{R_a E} - \gamma_{th} \vartheta_5]$ ,  $\Omega(x) \triangleq \frac{x \Theta \vartheta_2 + \Lambda}{\Phi}$ ,  $\Delta(x) \triangleq \frac{\gamma_{th} \vartheta_5 s}{\Phi} = \tilde{\gamma}_{th} + \frac{\gamma_{th} \Theta x}{\Phi}$ ,  $\tilde{\gamma}_{th} \triangleq \frac{\gamma_{th} (\mu_{RE}^2 \Phi + \Theta \mu_{JE}^2 + 1)}{\Phi}$ . By using (20),  $Q$  in (26) can be thus re-written as

$$\begin{aligned} Q &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \\ &\sum_{k_t}^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RE}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\times \int_{\Delta(x)}^{+\infty} \left( \frac{\gamma_{th} [y \vartheta_2 + \Omega(x)]}{\Psi [y - \Delta(x)]} \right)^{\sum_{t=1}^n p_t} \\ &\exp \left( - \sum_{t=1}^n \vartheta_3 \left( \frac{\gamma_{th} [y \vartheta_2 + \Omega(x)]}{\Psi [y - \Delta(x)]} \right) - \lambda_{RE} y \right) dy, \end{aligned} \quad (27)$$

Let us denote  $z = y - \Delta(x)$ , then (27) can be expressed as

$$\begin{aligned} Q &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum_{k_t}^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RE}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\times \exp \left( - \sum_{t=1}^n \frac{\vartheta_3 \gamma_{th} \vartheta_2}{\Psi} - \lambda_{RE} \Delta(x) \right) \left( \frac{\gamma_{th}}{\Psi} \right)^{A_2} \\ &\times \int_0^{+\infty} \left( \vartheta_2 + \frac{\vartheta_6}{z} \right)^{A_2} \exp \left( - \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \vartheta_6}{\Psi z} - \lambda_{RE} z \right) dz, \end{aligned} \quad (28)$$

where  $\vartheta_6 \triangleq \Delta(x) \vartheta_2 + \Omega(x)$ . By applying the Binomial Theorem,  $Q$  can be calculated as

$$\begin{aligned} Q &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \\ &\sum_{k_t}^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RE}}{k_t! p_t!} \vartheta_3^{-A_3} \\ &\times \exp \left( - \sum_{t=1}^n \frac{\vartheta_3 \gamma_{th} \vartheta_2}{\Psi} - \lambda_{RE} \Delta(x) \right) \left( \frac{\gamma_{th}}{\Psi} \right)^{A_2} \\ &\times \sum_{q=0}^{A_2} \binom{A_2}{q} \vartheta_2^{A_2-q} \vartheta_6^q \int_0^{+\infty} z^{-q} \times \\ &\exp \left( - \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \vartheta_6}{\Psi z} - \lambda_{RE} z \right) dz. \end{aligned} \quad (29)$$

*Lemma 2:* With using the same approach as (23), the

TABLE I  
SIMULATION PARAMETERS.

Symbol	Parameter name	Fixed value	Varying range
$C_{th}$	SNR threshold of the system	1	none
$\mu_{SR}$	CEEs of S-R link	0.25	none
$\mu_{RD}$	CEEs of R-D link	0.25	none
$\mu_{RE}$	CEEs of R-E link	0.25	none
$\mu_{JE}$	CEEs of R-E link	0.25	none
$\Psi$	Transmit power-to-noise-ratio from satellite	20 dB	0 to 50 dB
$\Phi$	Transmit power-to-noise-ratio from relay	10 dB	none
$\Theta$	Transmit power-to-noise-ratio from jammer	1 dB	none
$N$	Number of relays	1-3	none

closed-formed expression of  $Q$  can be expressed as

$$\begin{aligned}
Q &= 1 + 2 \sum_{n=1}^N \frac{(-1)^n}{n!} \sum_{k_t}^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RE}}{k_t! p_t! \vartheta_3^{A_3}} \\
&\times \exp \left( -\frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \vartheta_2}{\Psi} - \lambda_{RE} \Delta(x) \right) \\
&\times \left( \frac{\gamma_{th}}{\Psi} \right)^{A_2} \sum_{q=0}^{A_2} \binom{A_2}{q} \vartheta_2^{A_2-q} \vartheta_6^{\frac{q+1}{2}} \left( \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th}}{\Psi \lambda_{RE}} \right)^{-\frac{q+1}{2}} \\
&\times K_{-q+1} \left( 2 \sqrt{\frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \lambda_{RE} \vartheta_6}{\Psi}} \right). \quad (30)
\end{aligned}$$

*Theorem 2:* Finally, by applying [48, Eq.6.592.4], the closed-formed expression in terms of IP can be mathematically represented as

$$\begin{aligned}
IP &= \sum_{n=1}^N \frac{(-1)^{n+1}}{n!} \times \left( \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th}}{\Psi \lambda_{RE}} \right)^{-\frac{q+1}{2}} \\
&\times \sum_{k_t}^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{RE} \lambda_{JE}}{k_t! p_t! \vartheta_3^{A_3}} \\
&\times \exp \left( \Lambda_{10} \tilde{\Lambda} - \lambda_{RE} \tilde{\gamma}_{th} - \frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \vartheta_2}{\Psi} \right) \quad (31) \\
&\times \left( \frac{\gamma_{th}}{\Psi} \right)^{\sum_{t=1}^n p_t} \sum_{q=0}^{\sum_{t=1}^n p_t} \binom{\sum_{t=1}^n p_t}{q} \vartheta_2^{A_2-q} (\tilde{\Lambda})^{\frac{q+3}{2}} \\
&\times \sum_{w=0}^{\infty} \frac{(-1)^w 2^{q+2w+1} \left( \frac{[\lambda_{JE} + \frac{\gamma_{th} \lambda_{RE} \Theta}{\Phi}] \tilde{\Lambda}}{\vartheta_7 \vartheta_2 \gamma_{th}} \right)^w}{w! \zeta^{q+2w+1}} \\
&\times G_{1,3}^{3,0} \left( \frac{\zeta^2}{4} \middle| \begin{matrix} 0 \\ -1, 1+w, q+w \end{matrix} \right),
\end{aligned}$$

where  $\zeta = 2 \sqrt{\frac{\sum_{t=1}^n \vartheta_3 \gamma_{th} \lambda_{RE} \tilde{\Lambda}}{\Psi}}$ , and  $G_{p,q}^{m,n} \left( z \middle| \begin{matrix} a_1, \dots, a_p \\ b_1, \dots, b_q \end{matrix} \right)$  is the Meijer G-function.

*Proof:* See Appendix B. ■

*Remark 2:* This paper derives the closed-form expressions for the IP and OP, independent of the small-scale fading coefficients and therefore working for a long time. We provide an initial mechanism to analyze the security and reliability of an integrated satellite-terrestrial multi-relay network under imperfect CSI. Since the analytical results in Theorems 1 and 2 are only the multivariate functions of channel statistics, the IP and OP can be evaluated at a lower cost than numerically

averaging over many different realizations of the small-scale fading coefficients. This fact reduces the cost of the system design and can be easily deployed in practice.

*Remark 3:* The system-level design makes steps toward practical applications. One of the possible scenarios is that a satellite provides mobile streaming services and the Internet to ordinary handheld devices located in indoor areas such as multi-floor buildings. Under this scenario, the end device can certainly not receive signals from the satellite directly. As a result, a terrestrial network and a set of gap-filler are necessary to help the end device fully access these services [55], [56].

#### IV. NUMERICAL RESULTS

In this section, Monte-Carlo simulations are presented to evaluate the efficiency of the proposed HSTRN and the influences of various parameters on the system performance. The simulation parameters are given in Table I [57] and [58]. Unless other stated, we assume the SNR threshold of the system is set as  $C_{th} = 1$  bps/Hz,  $(m,b,\Omega)=(1,0.0635,0.0007)$  for heavy shadowing (HS) case and  $(m,b,\Omega)=(5,0.25,0.279)$  for average shadowing (AS) case. For ease of notation and clear observation, we denote methods with CEEs = 0.25-N = 1, perfect CSI-N = 1, CEEs = 0.25-N = 3, perfect CSI-N = 3, imperfect CSI- $\Phi$  = 5 dB- $\Psi$  = 20 dB-N = 3, and imperfect CSI- $\Phi$  = 10 dB- $\Psi$  = 20 dB-N = 3 are proposed method 1 (PM1), proposed method 2 (PM2), proposed method 3 (PM3), proposed method 4 (PM4), proposed method 5 (PM5), and proposed method 6 (PM6), respectively.

In Figs. 2 and 3, we investigate the influences of satellite's transmit power to the outage and intercept probability with heavy shadowing, respectively. The setting parameters for Figs. 2 and 3 are given as  $C_{th} = 1$  bps/Hz and  $\Phi=20$  dB. As given in Fig. 2, the OP is significantly enhanced with a higher value of  $\Psi$ , i.e.,  $\Psi$  from 0 to 50 dB. We stress that the value  $\Psi$  reaches 50 dB, which is impractical, but the range is selected to demonstrate the convergence and to have a full vision of the OP and IP. For example, the OP values of PM1 with high shadowing are 0.9783, 0.6742, and 0.5639 corresponding to  $\Psi$  equals 10, 20, and 30 dB, respectively. Moreover, we can observe from Fig. 2 that the OP value is decreased to a saturated value with the increasing of  $\Psi$ . For example, when  $\Psi$  values ranges from 35  $\rightarrow$  50 dB, the OP values of PM1 and PM3 converge to 0.5495 and 0.2430, respectively. This is because a higher  $\Psi$  value, the more the satellite's transmit power is. Therefore, the receiver D has more chance to successfully decode the received signals from relay  $R_n$ . Furthermore, the outage performance is significantly

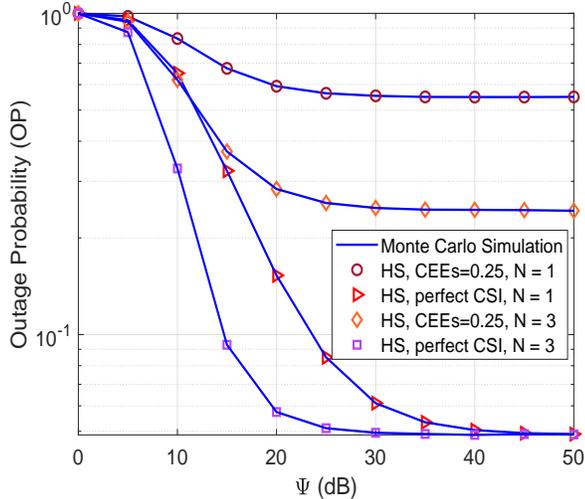


Fig. 2. OP in HS case versus  $\Psi$  with  $C_{th} = 1(\text{bps/Hz})$  and  $\Phi=20$  dB.

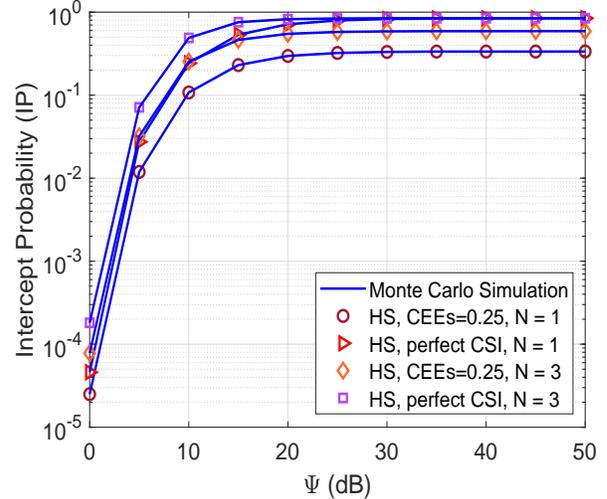


Fig. 3. IP in HS versus  $\Psi$  with  $C_{th} = 1(\text{bps/Hz})$ ,  $\Phi=20$  dB and  $\Theta=1$  dB.

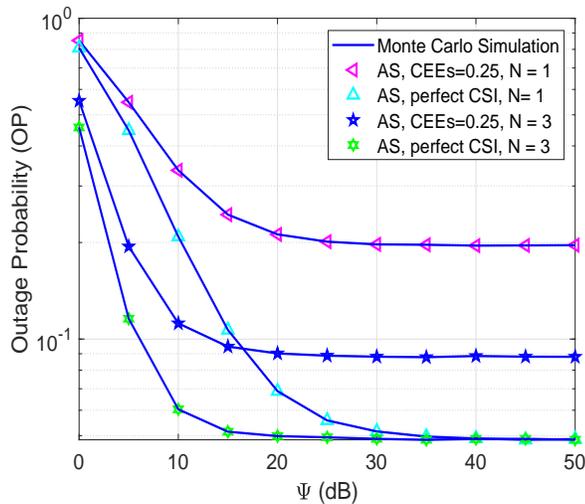


Fig. 4. OP in AS case versus  $\Psi$  with  $C_{th} = 1(\text{bps/Hz})$  and  $\Phi=20$  dB.

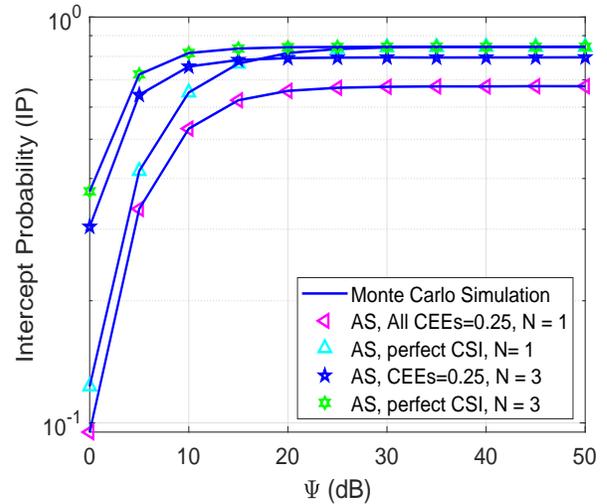


Fig. 5. IP in AS versus  $\Psi$  with  $C_{th} = 1(\text{bps/Hz})$ ,  $\Phi=20$  dB and  $\Theta=1$  dB.

improved with a higher number of relay. This is because the satellite can select a better relay with higher channel gain from  $R_n \rightarrow D$ , which can improve the total throughput received at the destination.

In Fig. 3, we can see that the IP is enhanced with a higher value of  $\Psi$ . More specifically, the IP values of PM1 with high shadowing (HS) are 0.0119, 0.1077, and 0.2305 corresponding to  $\Psi$  values equals 5, 10, and 15 dB, respectively. That is because a better signal-to-noise ratio (SNR) can be obtained at the eavesdropper with higher values of  $\Psi$ , as shown in Eq. (14). It also can be observed that the intercept performance of the proposed schemes with perfect CSI is better than that compared to imperfect CSI with a higher value of  $\Psi$ . For instance, at  $\Psi$  equals 50 dB, the IP values of the PM1 and PM4 are 0.3357 and 0.8442, respectively. This is because the eavesdropper can perfectly decode received signals with perfect CSI, which greatly improves the intercept performance.

Figs. 4 and 5 illustrate the influences of the satellite's transmit power to the OP and IP with average shadowing (AS) effects, respectively. As observed from Fig. 4, the outage

values of the proposed schemes with perfect CSI, i.e., PM2 and PM4, are better than that as compared to imperfect CSI ones, i.e., PM1 and PM3. Specifically, when  $\Psi$  equals 40 dB, the outage values of PM1 and PM3 impose 0.1956 and 0.049, respectively. Moreover, the proposed schemes converge to saturation value faster with higher number of relays, i.e.,  $N$  from 1 to 3. For example, the PM2 and PM4 schemes converge to saturation value at  $\Psi$  equals 40 and 30 dB, respectively. In contrast to Fig. 4, the intercept performance in Fig. 5 is greatly increased with higher value of satellite's transmit power. Specifically, when  $\Psi$  increases from 10 to 20 dB, the IP of the PM1 is 0.5310 and 0.6579, respectively. Similar to Fig. 3, the intercept performance of proposed schemes with

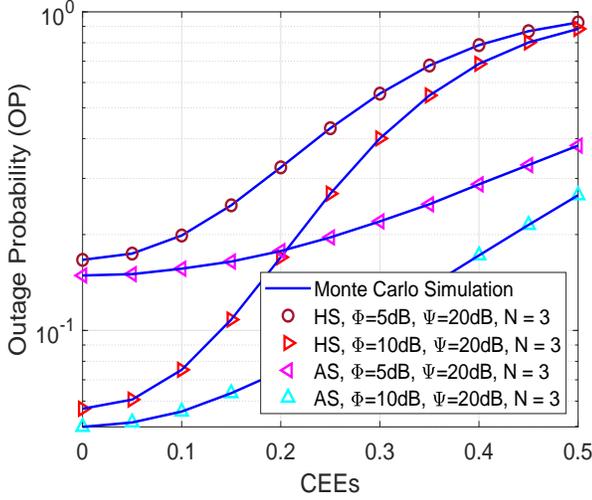


Fig. 6. OP versus all CEEs with  $N = 3$ ,  $C_{th} = 1$  bps/Hz and  $\Psi = 20$  dB.

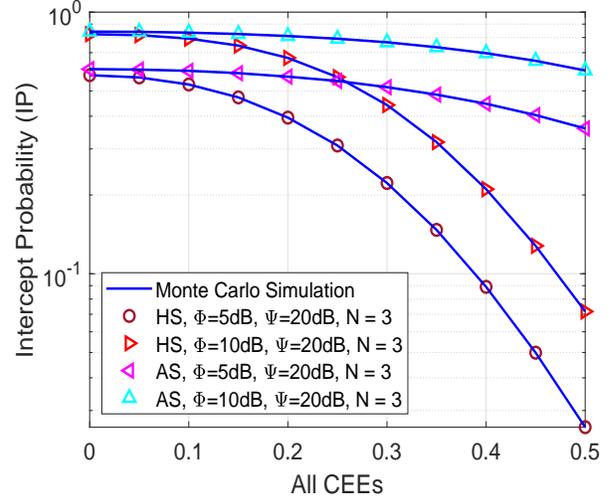


Fig. 7. IP versus all CEEs with  $N = 3$ ,  $C_{th} = 1$  bps/Hz,  $\Psi = 20$  dB,  $\Phi = 5$  dB and  $\Theta = 1$  dB.

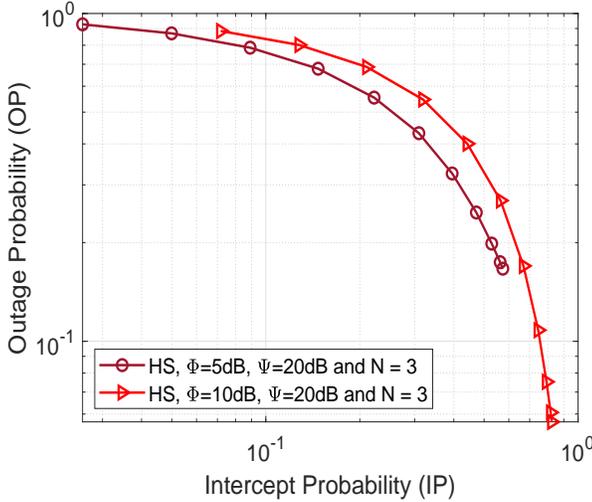


Fig. 8. OP versus IP in HS case with  $\Psi = 20$  dB,  $C_{th} = 1$  (bps/Hz),  $N = 3$  and  $\Theta = 1$  dB.

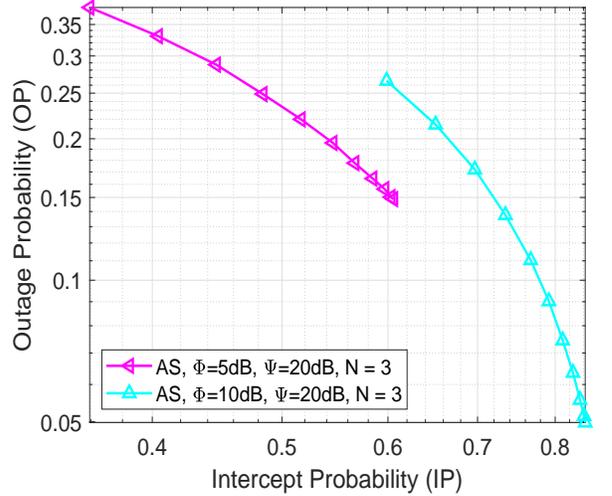


Fig. 9. OP versus IP in AS case with  $\Psi = 20$  dB,  $C_{th} = 1$  (bps/Hz),  $N = 3$  and  $\Theta = 1$  dB.

perfect CSI outperforms imperfect ones.<sup>5</sup>

In Figs. 6 and 7, we show the influences of CEEs to the outage and intercept performance with heavy and average shadowing effects, respectively. The setting parameters for Figs. 6 and 7 are given as  $C_{th} = 1$  bps/Hz,  $N = 3$ ,  $\Psi = 20$  dB,  $\Phi = 5$  dB and  $\Theta = 1$  dB. First, we can observe from Fig. 6 that the outage performance of the HS-based schemes is worse than that compared to the AS-based schemes. Specifically, at CEEs equals 0.1, PM5 with HS and PM5 with AS impose 0.1983 and 0.1563, respectively. Moreover, the gap between PM5 with HS and PM5 with AS is larger with higher of CEEs values. For instance, the gap between these schemes are 0.0423, 0.1475,

<sup>5</sup>Concerning the values of the OP, some reach one under certain conditions, and it is, of course, ideal for many practical applications under a finite resource budget. The rationale behind this is to justify the help of relays to enhance security and reliability in satellite-terrestrial networks once sufficient radio resources are available. We stress that there are parameter settings that increase the number of relays the OP dramatically decreases. The OP facilitates approximately 10-fold as the number of relays increases from 1 to 3, as shown in Figs. 2 and 4.

and 0.2354 at CEEs equals 0.1, 0.2, and 0.3, respectively. This shows significant effects of the shadowing effects on network performance. Second, it is also can be seen that the outage performance is enhanced by increasing  $\phi$  value. This can be explained by the fact that the higher the  $\phi$  value is, the better SNR at the destination can be obtained, as shown in Eq. (13). It can be seen from Fig. 7 that the intercept performance is significantly degraded with higher CEEs values. For instance, when CEEs is between 0.1 and 0.3, the IP value of PM5 with HS is 0.529, 0.3951, and 0.2222, respectively. Moreover, the intercept performance of the HS-based schemes is significantly degraded as compared to AS-based ones, which is in contrast to Fig. 6.

In Figs. 8 and 9, we investigate the security-reliability trade-off with parameters are setting as Figs. 3 and 5. It is clear to see that for any specific IP, the OP of PM5 with HS (or AS) is higher than that compared to PM6 with HS (or AS). For example, when IP equals 0.4, the OP of the PM5 with HS is 0.315, while the OP of the PM6 with HS is 0.422.

Additionally, Figs. 8 and 9 also show that PM6 scheme with HS obtains the best OP compared to other HS-based and AS-based ones.

## V. CONCLUSION AND DISCUSSION

This paper has studied the physical layer security in terms of security and reliability trade-off of a satellite amplify-and-forward multi-relay network, consisting of one satellite, multiple relays, one destination in the presence of one eavesdropper. Especially, a jammer has been implemented to create artificial noise in order to eliminate the influence of the eavesdropper on system performance. Based on this system model, the closed-form expressions of OP and IP were derived by considering generalized Shadowed Rician and Rayleigh fading in the first and second hop, respectively. Then, these mathematical analyses have been validated through simulation results. In particular, the values of the satellite's transmit power, number of relays, and relay transmit power can be selected appropriately to reduce the influences of the eavesdropper.

## APPENDIX

### A. Proof of Theorem 1

Based on (13) and (22), the OP can be rewritten as follows:

$$\begin{aligned} \text{OP} &= \Pr \left( \frac{\Psi \Phi \gamma_{\text{SR}_a} \gamma_{\text{R}_a\text{D}}}{\gamma_{\text{R}_a\text{D}} \Phi \vartheta_2 + \gamma_{\text{SR}_a} \Psi \vartheta_4 + \Xi} < \gamma_{\text{th}} \right) \\ &= \Pr (\gamma_{\text{SR}_a} \Lambda_3 < \gamma_{\text{th}} [\gamma_{\text{R}_a\text{D}} \Phi \vartheta_2 + \Xi]) \end{aligned} \quad (32)$$

$$\begin{aligned} &= \begin{cases} \Pr \left( \gamma_{\text{SR}_a} < \frac{\Lambda_2}{\Lambda_3} \right), & \text{if } \gamma_{\text{R}_a\text{D}} > \frac{\gamma_{\text{th}} \vartheta_4}{\Phi} \\ 1, & \text{if } \gamma_{\text{R}_a\text{D}} \leq \frac{\gamma_{\text{th}} \vartheta_4}{\Phi} \end{cases} \\ &= \int_0^{\tilde{\gamma}_{\text{th}}} f_{\gamma_{\text{R}_a\text{D}}}(x) dx + \int_{\tilde{\gamma}_{\text{th}}}^{+\infty} F_{\gamma_{\text{SR}_a}} \left( \frac{\Lambda_4}{\Lambda_5} \right) f_{\gamma_{\text{R}_a\text{D}}}(x) dx, \end{aligned}$$

where  $\tilde{\gamma}_{\text{th}} \triangleq \frac{\gamma_{\text{th}} (\mu_{\text{RD}}^2 \Phi + 1)}{\Phi}$ ,  $\vartheta_4 \triangleq (\mu_{\text{RD}}^2 \Phi + 1)$ ,  $\Lambda_2 \triangleq [\gamma_{\text{R}_a\text{D}} \Phi \vartheta_2 + \Xi]$ ,  $\Lambda_3 \triangleq \Psi [\Phi \lambda_{\text{R}_a\text{D}} - \gamma_{\text{th}} \vartheta_4]$ ,  $\Lambda_4 \triangleq [x \Phi \vartheta_2 + \Xi]$ ,  $\Lambda_5 \triangleq \Psi [\Phi x - \gamma_{\text{th}} \vartheta_4]$ . By substituting (20) into (32), the OP can be mathematically represented by

$$\begin{aligned} \text{OP} &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{\text{RD}}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\quad \times \int_{\tilde{\gamma}_{\text{th}}}^{+\infty} \left( \frac{\gamma_{\text{th}} [x \vartheta_2 + \frac{\Xi}{\Phi}]}{\Psi [x - \tilde{\gamma}_{\text{th}}]} \right)^{\sum_{t=1}^n p_t} \\ &\quad \times \exp \left( - \sum_{t=1}^n \vartheta_3 \left( \frac{\gamma_{\text{th}} [x \vartheta_2 + \frac{\Xi}{\Phi}]}{\Psi [x - \tilde{\gamma}_{\text{th}}]} \right) - \lambda_{\text{RD}} x \right) dx. \end{aligned} \quad (33)$$

By denoting  $y = x - \tilde{\gamma}_{\text{th}}$ , (33) can be further reformulated as

$$\begin{aligned} \text{OP} &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{\text{RD}}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\quad \times \int_0^{+\infty} \left( \frac{\gamma_{\text{th}} [(y + \tilde{\gamma}_{\text{th}}) (\mu_{\text{SR}}^2 \Psi + 1) + \frac{\Xi}{\Phi}]}{\Psi y} \right)^{\sum_{t=1}^n p_t} \\ &\quad \times \exp \left( - \sum_{t=1}^n \vartheta_3 \left( \frac{\gamma_{\text{th}} [(y + \tilde{\gamma}_{\text{th}}) \vartheta_2 + \frac{\Xi}{\Phi}]}{\Psi y} \right) - \lambda_{\text{RD}} (y + \tilde{\gamma}_{\text{th}}) \right) dy \\ &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{\text{RD}}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\quad \times \left( \frac{\gamma_{\text{th}}}{\Psi} \right)^{A_2} \exp \left( - \sum_{t=1}^n \vartheta_3 \frac{\gamma_{\text{th}} \vartheta_2}{\Psi} - \lambda_{\text{RD}} \tilde{\gamma}_{\text{th}} \right) \\ &\quad \times \int_0^{+\infty} \left( \vartheta_2 + \frac{\Xi}{y} \right)^{\sum_{t=1}^n p_t} \exp \left( - \frac{\sum_{t=1}^n \vartheta_3 \frac{\gamma_{\text{th}} \Xi}{\Psi}}{y} - \lambda_{\text{RD}} y \right) dy, \end{aligned} \quad (34)$$

where  $\Xi = [\tilde{\gamma}_{\text{th}} (\mu_{\text{SR}}^2 \Psi + 1) + \frac{\Xi}{\Phi}]$ . By applying Binomial Theorem, i.e.,  $(x + y)^m = \sum_{q=0}^m \binom{m}{q} x^{m-q} y^q$ , (34) can be rewritten as

$$\begin{aligned} \text{OP} &= 1 + \sum_{n=1}^N \frac{(-1)^n}{n!} \sum^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{\text{RD}}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\quad \times \left( \frac{\gamma_{\text{th}}}{\Psi} \right)^{A_2} \exp \left( - \sum_{t=1}^n \vartheta_3 \frac{\gamma_{\text{th}} \vartheta_2}{\Psi} - \lambda_{\text{RD}} \tilde{\gamma}_{\text{th}} \right) \\ &\quad \times \sum_{q=0}^{A_2} \binom{A_2}{q} \vartheta_2^{A_2-q} \Xi^q \int_0^{+\infty} y^{-q} \\ &\quad \times \exp \left( - \frac{\sum_{t=1}^n \vartheta_3 \frac{\gamma_{\text{th}} \Xi}{\Psi}}{y} - \lambda_{\text{RD}} y \right) dy. \end{aligned} \quad (35)$$

By adopting [48, Eq.3.471.9], the analytical expression of the OP can be obtained in the theorem after doing some algebra.

### B. Proof of Theorem 2

Based on the result obtained from Lemma 2, by substituting (30) into (25), the IP can be calculated as

$$\begin{aligned} \text{IP} &= 2 \sum_{n=1}^N \frac{(-1)^{n+1}}{n!} \sum^* \alpha_{n_t} \frac{(-1)^{k_t} (1 - m_{n_t})_{k_t} (\delta_{n_t})^{k_t} \lambda_{\text{RE}} \lambda_{\text{JE}}}{k_t! p_t! \vartheta_3^{A_3}} \\ &\quad \times \left( \frac{\sum_{t=1}^n \vartheta_3 \gamma_{\text{th}}}{\Psi \lambda_{\text{RE}}} \right)^{\frac{-q+1}{2}} \exp \left( - \frac{\sum_{t=1}^n \vartheta_3 \gamma_{\text{th}} \vartheta_2}{\Psi} \right) \\ &\quad \times \left( \frac{\gamma_{\text{th}}}{\Psi} \right)^{A_2} \sum_{q=0}^{\sum_{t=1}^n p_t} \binom{A_2}{q} \vartheta_2^{A_2-q} \\ &\quad \times \int_0^{+\infty} \vartheta_6^{\frac{q+1}{2}} \exp(-\lambda_{\text{JE}} x - \lambda_{\text{RE}} \Delta(x)) \\ &\quad \times K_{-q+1} \left( 2 \sqrt{\frac{\sum_{t=1}^n \vartheta_3 \gamma_{\text{th}} \lambda_{\text{RE}} \vartheta_6}{\Psi}} \right) dx. \end{aligned} \quad (36)$$

Based on (36), we have

$$\begin{aligned} \Delta(x)\vartheta_2 + \Omega(x) &= \tilde{\gamma}_{th}\vartheta_2 + \frac{\gamma_{th}\Theta x}{\Phi}\vartheta_2 + \frac{x\Theta\vartheta_2 + \Lambda}{\Phi} \\ &= \vartheta_2 \left( \tilde{\gamma}_{th} + \frac{\gamma_{th}\Theta x}{\Phi} + \frac{x\Theta}{\Phi} \right) + \frac{\Lambda}{\Phi}, \end{aligned} \quad (37)$$

$$\begin{aligned} &\exp(-\lambda_{JE}x - \lambda_{RE}\Delta(x)) \\ &= \exp\left(-\lambda_{JE}x - \lambda_{RE}\tilde{\gamma}_{th} - \frac{\gamma_{th}\lambda_{RE}\Theta x}{\Phi}\right) \\ &= \exp\left(-\lambda_{RE}\tilde{\gamma}_{th}\right) \exp\left(-x\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]\right). \end{aligned} \quad (38)$$

Next, by denoting  $t \triangleq \frac{x\left[\left(\frac{\Theta}{\Phi}+1\right)\vartheta_2\gamma_{th}\right]}{\tilde{\Lambda}} + 1$ , (37) and (38) can be respectively rewritten as

$$\begin{aligned} \Delta(x)\vartheta_2 + \Omega(x) &= t\tilde{\Lambda}, \\ \exp(-\lambda_{JE}x - \lambda_{RE}\Delta(x)) &= \exp\left(\frac{\tilde{\Lambda}\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]}{\vartheta_7\vartheta_2\gamma_{th}} - \lambda_{RE}\tilde{\gamma}_{th}\right) \\ &\times \exp\left(-\frac{\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]t\tilde{\Lambda}}{\vartheta_7\vartheta_2\gamma_{th}}\right), \end{aligned} \quad (39)$$

where  $\tilde{\Lambda} \triangleq \tilde{\gamma}_{th}\vartheta_2 + \frac{\Lambda}{\Phi}$ ,  $\vartheta_7 \triangleq \frac{\Theta}{\Phi} + 1$ . By substituting (39) and (40) into (36), it yields

$$\begin{aligned} \text{IP} &= 2 \sum_{n=1}^N \frac{(-1)^{n+1}}{n!} \left( \frac{\sum_{t=1}^n \vartheta_3\gamma_{th}}{\Psi\lambda_{RE}} \right)^{\frac{-q+1}{2}} \\ &\sum_{n_t}^* \frac{(-1)^{k_t}(1-m_{n_t})_{k_t}(\delta_{n_t})^{k_t}\lambda_{RE}\lambda_{JE}}{k_t!p_t!\vartheta_3^{A_3}} \\ &\times \exp\left(\Lambda_{10}\tilde{\Lambda} - \lambda_{RE}\tilde{\gamma}_{th} - \frac{\sum_{t=1}^n \vartheta_3\gamma_{th}\vartheta_2}{\Psi}\right) \\ &\times \left(\frac{\gamma_{th}}{\Psi}\right)^{A_2} \sum_{q=0}^{A_2} \binom{A_2}{q} \frac{\vartheta_2^{A_2-q}\tilde{\Lambda}^{\frac{q+3}{2}}}{\vartheta_7\vartheta_2\gamma_{th}} \\ &\times \int_1^{+\infty} (t)^{\frac{q+1}{2}} \exp(-\Lambda_{10}t\tilde{\Lambda}) \\ &\times K_{-q+1}\left(2\sqrt{\frac{\sum_{t=1}^n \vartheta_3\gamma_{th}\lambda_{RE}t\tilde{\Lambda}}{\Psi}}\right) dt. \end{aligned} \quad (41)$$

where  $\Lambda_{10} \triangleq \frac{\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]}{\vartheta_7\vartheta_2\gamma_{th}}$ . Next, we apply the Maclaurin series as follows:

$$\begin{aligned} &\exp\left(-\frac{\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]t\tilde{\Lambda}}{\vartheta_7\vartheta_2\gamma_{th}}\right) \\ &= \sum_{w=0}^{\infty} \frac{(-1)^w \left(\frac{\left[\lambda_{JE} + \frac{\gamma_{th}\lambda_{RE}\Theta}{\Phi}\right]\tilde{\Lambda}}{\vartheta_7\vartheta_2\gamma_{th}}\right)^w}{w!} t^w. \end{aligned} \quad (42)$$

By substituting (42) into (41), the IP can be re-calculated as

$$\begin{aligned} \text{IP} &= 2 \sum_{n=1}^N \frac{(-1)^{n+1}}{n!} \left( \frac{\sum_{t=1}^n \vartheta_3\gamma_{th}}{\Psi\lambda_{RE}} \right)^{\frac{-q+1}{2}} \\ &\sum_{n_t}^* \frac{(-1)^{k_t}(1-m_{n_t})_{k_t}(\delta_{n_t})^{k_t}\lambda_{RE}\lambda_{JE}}{k_t!p_t!\vartheta_3^{A_3}} \\ &\times \exp\left(\tilde{\Lambda}\Lambda_{10} - \lambda_{RE}\tilde{\gamma}_{th} - \frac{\sum_{t=1}^n \vartheta_3\gamma_{th}\vartheta_2}{\Psi}\right) \\ &\times \left(\frac{\gamma_{th}}{\Psi}\right)^{A_2} \sum_{q=0}^{A_2} \binom{A_2}{q} \frac{\vartheta_2^{A_2-q}\tilde{\Lambda}^{\frac{q+3}{2}}}{\vartheta_7\vartheta_2\gamma_{th}} \\ &\times \sum_{w=0}^{\infty} \frac{(-1)^w \left(\Lambda_{10}\tilde{\Lambda}\right)^w}{w!} \int_1^{+\infty} (t)^{\frac{q+1+2w}{2}} \\ &\times K_{-q+1}\left(2\sqrt{\frac{\sum_{t=1}^n \vartheta_3\gamma_{th}\lambda_{RE}t\tilde{\Lambda}}{\Psi}}\right) dt. \end{aligned} \quad (43)$$

After computing the integral in (43) and doing some algebra, we obtain the result as shown in the theorem.

## REFERENCES

- [1] P. X. Nguyen, D.-H. Tran, O. Onireti, P. T. Tin, S. Q. Nguyen, S. Chatzinotas, and H. V. Poor, "Backscatter-assisted data offloading in OFDMA-based wireless-powered mobile edge computing for IoT networks," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9233–9243, June 2021.
- [2] T. N. Nguyen, D.-H. Tran, V.-D. Phan, M. Voznak, S. Chatzinotas, B. Ottersten, and H. V. Poor, "Throughput enhancement in FD-and SWIPT-enabled IoT networks over non-identical Rayleigh fading channels," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10 172 – 10 186, June 2021.
- [3] D.-H. Tran, V.-D. Nguyen, S. Chatzinotas, T. X. Vu, and B. Ottersten, "UAV relay-assisted emergency communications in IoT networks: Resource allocation and trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1621–1637, March 2021.
- [4] X. Li, W. Feng, J. Wang, Y. Chen, N. Ge, and C.-X. Wang, "Enabling 5G on the ocean: A hybrid satellite-UAV-terrestrial network solution," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 116–121, December 2020.
- [5] T. Van Chien, E. Lagunas, T. H. Ta, S. Chatzinotas, and B. Ottersten, "User scheduling and power allocation for precoded multi-beam high throughput satellite systems with individual quality of service constraints," *IEEE Transactions on Vehicular Technology*, 2022, major revision.
- [6] T. N. Nguyen, D.-H. Tran, T. V. Chien, V.-D. Phan, M. Voznak, P. T. Tin, S. Chatzinotas, D. W. K. Ng, and H. V. Poor, "Security-reliability trade-off analysis for SWIPT-and AF-based IoT networks with friendly jammers," *IEEE Internet of Things Journal*, pp. 1–1, 2022, early access.
- [7] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14 399–14 417, September 2021.
- [8] "OneWeb non-geostationary satellite system (attachment A)," August 2013.
- [9] SpaceX, "SpaceX non-geostationary satellite system (attachment A)," November 2018.
- [10] R. Deng, B. Di, and L. Song, "Ultra-dense LEO satellite based formation flying," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3091–3105, May 2021.
- [11] V.-P. Bui, T. Van Chien, E. Lagunas, J. Grotz, S. Chatzinotas, and B. Ottersten, "Robust congestion control for demand-based optimization in precoded multi-beam high throughput satellite communications," *IEEE Transactions on Communications*, 2022, early access.
- [12] A. Vanelli-Corali, G. E. Corazza, G. Karagiannidis, P. Mathiopoulos, D. Michalopoulos, C. Mosquera, S. Papaharalabos, and S. Scalise, "Satellite communications: Research trends and open issues," in *Proc. 2007 international works. sat. and space commun.* IEEE, September 2007, pp. 71–75.

- [13] K. Guo, M. Lin, B. Zhang, J.-B. Wang, Y. Wu, W.-P. Zhu, and J. Cheng, "Performance analysis of hybrid satellite-terrestrial cooperative networks with relay selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9053–9067, August 2020.
- [14] Q. Huang, M. Lin, W.-P. Zhu, S. Chatzinotas, and M.-S. Alouini, "Performance analysis of integrated satellite-terrestrial multiantenna relay networks with multiuser scheduling," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 4, pp. 2718–2731, August 2020.
- [15] 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 Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7011–7023, July 2019.
- [16] G. Pan, J. Ye, Y. Zhang, and M.-S. Alouini, "Performance analysis and optimization of cooperative satellite-aerial-terrestrial systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6693–6707, October 2020.
- [17] P. K. Sharma, D. Gupta, and D. I. Kim, "Outage performance of 3D mobile UAV caching for hybrid satellite-terrestrial networks," *IEEE Trans. Vehicular Technol.*, vol. 70, no. 8, pp. 8280–8285, August 2021.
- [18] H. D. Tran, S. Chatzinotas, and B. Ottersten, "Satellite- and Cache-assisted UAV: A Joint Cache Placement, Resource Allocation, and Trajectory Optimization for 6G Aerial Networks," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 40–54, January 2022.
- [19] H. Tran-Dinh, T. X. Vu, S. Chatzinotas, and B. Ottersten, "Energy-efficient trajectory design for UAV-enabled wireless communications with latency constraints," in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*. IEEE, November 2019, pp. 347–352.
- [20] D.-H. Tran, V.-D. Nguyen, S. Gautam, S. Chatzinotas, T. X. Vu, and B. Ottersten, "Resource allocation for UAV relay-assisted IoT communication networks," in *2020 IEEE Globecom Workshops*. IEEE, December 2020, pp. 1–7.
- [21] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2488–2501, March 2019.
- [22] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1862–1874, September 2015.
- [23] K. Guo, K. An, F. Zhou, T. A. Tsiftsis, G. Zheng, and S. Chatzinotas, "On the secrecy performance of noma-based integrated satellite multiple-terrestrial relay networks with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3661–3676, April 2021.
- [24] P. K. Sharma and D. I. Kim, "Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2770–2784, August 2020.
- [25] X. Zhang, B. Zhang, K. An, G. Zheng, S. Chatzinotas, and D. Guo, "Stochastic geometry-based analysis of cache-enabled hybrid satellite-aerial-terrestrial networks with non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 1272 – 1287, February 2021.
- [26] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, September 2021.
- [27] X. Li, M. Zhao, M. Zeng, S. Mumtaz, V. G. Menon, Z. Ding, and O. A. Dobre, "Hardware impaired ambient backscatter NOMA systems: Reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, April 2021.
- [28] X. Li, H. Mengyan, Y. Liu, V. G. Menon, A. Paul, and Z. Ding, "IQ imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2995 – 3008, October-December 2020.
- [29] G. Cui, Q. Zhu, L. Xu, and W. Wang, "Secure beamforming and jamming for multibeam satellite systems with correlated wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 348–12 353, October 2020.
- [30] C. Han, A. Liu, K. An, H. Wang, G. Zheng, S. Chatzinotas, L. Huo, and X. Tong, "Satellite-assisted UAV trajectory control in hostile jamming environments," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3760 – 3775, April 2021.
- [31] M. Bouabdellah and F. E. Bouanani, "A PHY layer security of a jamming-based underlay cognitive satellite-terrestrial network," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 4, pp. 1266–1279, December 2021.
- [32] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photonics Journal*, vol. 11, no. 1, pp. 1–14, 2019.
- [33] S. Xu, J. Liu, Y. Cao, J. Li, and Y. Zhang, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 2007–2011, February 2021.
- [34] M. R. Bhatnagar and A. 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, October 2013.
- [35] K. An, M. Lin, T. Liang, J.-B. Wang, J. Wang, Y. Huang, and A. L. Swindlehurst, "Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4390–4404, November 2015.
- [36] D. H. Ha, T. N. Nguyen, M. H. Q. Tran, X. Li, P. T. Tran, and M. Voznak, "Security and reliability analysis of a two-way half-duplex wireless relaying network using partial relay selection and hybrid TPSR energy harvesting at relay nodes," *IEEE Access*, vol. 8, pp. 187 165–187 181, October 2020.
- [37] V.-D. Phan, T. N. Nguyen, A. V. Le, and M. Voznak, "A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting," *Sensors*, vol. 21, no. 17, p. 5692, August 2021.
- [38] P. Tran Tin, T. N. Nguyen, T. T. Duy, M. Voznak *et al.*, "Secrecy performance enhancement for underlay cognitive radio networks employing cooperative multi-hop transmission with and without presence of hardware impairments," *Entropy*, vol. 21, no. 2, p. 217, February 2019.
- [39] P. Sharma, K. K. Sarma, and N. E. Mastorakis, "Artificial intelligence aided electronic warfare systems-recent trends and evolving applications," *IEEE Access*, vol. 8, pp. 224 761–224 780, 2020.
- [40] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system," *IEEE Access*, vol. 7, pp. 58 353–58 360, 2019.
- [41] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319–1329, February 2016.
- [42] X. Li, M. Huang, C. Zhang, D. Deng, K. M. Rabie, Y. Ding, and J. Du, "Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments," *IEEE Access*, vol. 7, pp. 102 644–102 661, July 2019.
- [43] T. Van Chien, H. Q. Ngo, S. Chatzinotas, B. Ottersten, and M. Debbah, "Uplink power control in massive MIMO with double scattering channels," *IEEE Transactions on Wireless Communications*, vol. 21, no. 3, pp. 1989–2005, March 2022.
- [44] M. D. Yacoub, "The  $\alpha$ - $\mu$  distribution: A physical fading model for the stacy distribution," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 1, pp. 27–34, January 2007.
- [45] T. N. Nguyen, T. H. Q. Minh, P. T. Tran, M. Voznak, T. T. Duy, T.-L. Nguyen, and P. T. Tin, "Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods," *Ad hoc networks*, vol. 84, pp. 178–187, March 2019.
- [46] P. T. Tin, T. N. Nguyen, D.-H. Tran, M. Voznak, V.-D. Phan, and S. Chatzinotas, "Performance enhancement for full-duplex relaying with time-switching-based SWIPT in wireless sensors networks," *Sensors*, vol. 21, no. 11, p. 3847, June 2021.
- [47] 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, October 2016.
- [48] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products - Seventh Edition*. Elsevier, February 2007.
- [49] P. K. Upadhyay and P. K. Sharma, "Max-max user-relay selection scheme in multiuser and multirelay hybrid satellite-terrestrial relay systems," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 268–271, February 2015.
- [50] T. N. Nguyen, P. T. Tran, and M. Voznak, "Wireless energy harvesting meets receiver diversity: A successful approach for two-way half-duplex relay networks over block rayleigh fading channel," *Computer Networks*, vol. 172, p. 107176, May 2020.
- [51] B. C. Nguyen, T. M. Hoang, P. T. Tran, and T. N. Nguyen, "Outage probability of NOMA system with wireless power transfer at source and full-duplex relay," *AEU-international Journal of Electronics and Communications*, vol. 116, p. 152957, March 2020.
- [52] Q. Huang, M. Lin, K. An, J. Ouyang, and W.-P. Zhu, "Secrecy performance of hybrid satellite-terrestrial relay networks in the presence of multiple eavesdroppers," *IET Commun.*, vol. 12, no. 1, pp. 26–34, January 2018.

- [53] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 286–12 290, October 2020.
- [54] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, January 2015.
- [55] T. ETSI, "102 585 V1. 1.2 (2008-04):Digital video broadcasting (DVB)," *System Specifications for Satellite services to Handheld devices (SH) below 3 GHz*.
- [56] 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*, 2022.
- [57] 3GPP, "Study on new radio (NR) to support non-terrestrial networks," May 2019.
- [58] X. Yue, Y. Liu, Y. Yao, T. Li, X. Li, R. Liu, and A. Nallanathan, "Outage behaviors of NOMA-based satellite network over shadowed-rician fading channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6818–6821, June 2020.

**Tan N. Nguyen** (nguyennhattan@tdtu.edu.vn) 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 PhD 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 as been lecturing. His major interests are cooperative communications, cognitive radio, and physical layer security.

**Dinh-Hieu Tran** (S'20) was born in 1989 in Vietnam, growing up in Gia Lai. He received a BE degree in Electronics and Telecommunication Engineering Department from Ho Chi Minh City University of Technology, Vietnam, in 2012. In 2017, he completed an MS degree with honours in Electronics and Computer Engineering at Hongik University, South Korea. He obtained a PhD at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, under the supervision of Prof. Symeon Chatzinotas and Prof. Björn Ottersten. His research interests include UAVs, IoTs, mobile edge computing, caching, backscatter, B5G for wireless communication networks. He is a recipient of the IS3C 2016 best paper award.

**Trinh Van Chien** (S'16-M'20) received the B.S. degree in Electronics and Telecommunications from Hanoi University of Science and Technology (HUST), Vietnam, in 2012. He then received the M.S. degree in Electrical and Computer Engineering from Sungkyunkwan University (SKKU), Korea, in 2014 and the Ph.D. degree in Communication Systems from Linköping University (LiU), Sweden, in 2020. He was a research associate at University of Luxembourg. He is now with the School of Information and Communication Technology (SoICT), Hanoi University of Science and Technology (HUST), Vietnam. His interest lies in convex optimization problems and machine learning applications for wireless communications and image & video processing. He was an IEEE wireless communications letters exemplary reviewer for 2016, 2017 and 2021. He also received the award of scientific excellence in the first year of the 5Gwireless project funded by European Union Horizon's 2020.

**Van-Duc Phan** (duc.pv@vlu.edu.vn) was born in 1975 in Long An province, Vietnam. He received his MS degree from the Department of Electric, Electrical and Telecommunications Engineering at Ho Chi Minh City University of Transport in Vietnam and then in 201 a PhD from the Department of Mechanical and Automation Engineering, Da-Yeh University, Taiwan. His current research interests are sliding mode controls, non-linear systems and active magnetic bearings, flywheel energy storage systems, power system optimization, optimization algorithms, renewable energies, energy harvesting (EH) enabled cooperative networks, optical property improvement, lighting performance of white LEDs, energy efficiency LED driver integrated circuits, novel radio access technologies, and physical security in communications networks.

**Miroslav Voznak** (M'09-SM'16) received his PhD in telecommunications in 2002 from the Faculty of Electrical Engineering and Computer Science at VSB – Technical University of Ostrava, and achieved habilitation in 2009. He was appointed Full Professor in Electronics and Communications Technologies in 2017. His research interests generally focus on ICT, especially quality of service and experience, network security, wireless networks, and big data analytics. He has authored and co-authored over one hundred articles indexed in SCI/SCIE journals. According to the Stanford University study released in 2020, he is one of the World's Top 2% of scientists in Networking & Telecommunications and Information & Communications Technologies. He served as a general chair of the 11<sup>th</sup> IFIP Wireless and Mobile Networking Conference in 2018 and the 24<sup>th</sup> IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications in 2020. He participated in six projects funded by EU in programs managed directly by European Commission. Currently, he is a principal investigator in the research project QUANTUM5 funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks.

**Symeon Chatzinotas** (S'06-M'09-SM'13) is currently Full Professor / Chief Scientist I in Satellite Communications and Head of the SIGCOM Research Group at SnT, University of Luxembourg. He coordinates research activities in communications and networking, acting as a PI in over 20 projects and is the main representative for 3GPP, ETSI, DVB. In the past, he worked as a Visiting Professor at the University of Parma, Italy, lecturing on 5G Wireless Networks. He was involved in numerous R&D projects for NCSR Demokritos, CERTH Hellas and CCSR, University of Surrey. He was co-recipient of the 2014 IEEE Distinguished Contributions to Satellite Communications Award and Best Paper Awards at EURASIP JWCN, CROWNCOM, ICSSC. He has (co-)authored more than 450 technical papers in refereed international journals, conferences and scientific books. He is currently on the editorial board of the IEEE Transactions on Communications, IEEE Open Journal of Vehicular Technology, and the International Journal of Satellite Communications and Networking.