Cooperative Satellite-Terrestrial Networks With Imperfect CSI and Multiple Jammers: Performance Analysis and Deep Learning Evaluation

Tan N. Nguyen, *Member, IEEE*, Trinh Van Chien, *Member, IEEE*, Dinh-Hieu Tran, Bui Vu Minh, Nguyen Chi Ngon, Miroslav Voznak, *Senior Member, IEEE*, and Zhiguo Ding, *Fellow, IEEE*

***Abstract*—This article introduces novel and deep learning approaches for the security analysis of a hybrid satellite-terrestrial cooperative network. More specifically, a satellite transmits information to a ground user through multiple relays in the presence of an eavesdropper. To prevent potential eavesdropping, multiple friendly jammers are employed to disrupt the reception process of the eavesdropper by artificial noise. Within this setting, we then derive the closed-form expressions of the outage probability (OP) and secrecy outage probability (SOP) of the considered system in the presence of imperfect channel state information. Important to mention is the fact that in complex systems (e.g., with multiple jammers, multiple relays, and considering the independent but nonidentically distributed Rician nature of satellite links), analytical approaches may not be effective due to their complex mathematical derivations. As such, we develop a highly effective yet low-complexity deep learning approach to estimate the OP and SOP of the system. Through extensive Monte Carlo simulations, we evaluate the OP and SOP of the system in various settings and demonstrate the effectiveness of the proposed solutions. Interestingly, the proposed deep learning method can achieve comparable performance to that of the analytical approach.**

***Index Terms*—Deep learning, cooperative relay, friendly jamming, physical layer security, satellite communications.**

Received 5 January 2024; revised 26 April 2024 and 22 July 2024; accepted 7 September 2024. This work was supported in part by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries under Grant CZ.10.03.01/00/22_003/0000048, in part by the European Just Transition Fund and by the Ministry of Education, Youth and Sports of the Czech Republic (MEYS CZ) under Grant SP 061/2024 conducted by VSB - Technical University of Ostrava. *(Corresponding author: Bui Vu Minh.)*

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 70000, Vietnam (e-mail: nguyennhattan@tdtu.edu.vn).

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

Dinh-Hieu Tran is with the Interdisciplinary Centre for Security, Reliability and Trust, The University of Luxembourg, 4365 Esch-sur-Alzette, Luxembourg (e-mail: hieu.tran-dinh@uni.lu).

Bui Vu Minh is with the Faculty of Engineering and Technology, Nguyen Tat Thanh University, Ho Chi Minh City 754000, Vietnam (e-mail: bvminh@ntt.edu.vn).

Nguyen Chi Ngon is with the Department of Automation Technology, Can Tho University, Can Tho 900000, Vietnam (e-mail: ncngon@ctu.edu.vn).

Miroslav Voznak is with the VSB - Technical University of Ostrava, 708 33 Ostrava - Poruba, Czech Republic (e-mail: miroslav.voznak@vsb.cz).

I. Introduction

The last decade has witnessed a remarkable development of satellite communication (SatCom) due to its vast coverage and high transmission data [1], [2], [3]. In particular, operating at high altitudes allows satellites to cover a large portion of the Earth's surface and provide communications to a massive number of ground users. As such, SatCom can empower ultra-reliable communications when terrestrial infrastructure is not available due to natural disasters or in unreachable and remote regions [4], [5]. Several major companies, such as SpaceX, Amazon, and OneWeb, have already started to commercialize SatCom to deliver broadband services to ground users anywhere and anytime. With its significant potential, SatCom is expected to play a critical role in future communication systems.

Unfortunately, operating at high altitudes makes SatCom vulnerable to shadow effects and obstacles that can block the line-of-sight links between satellites and terrestrial users, especially in urban environments [6]. To overcome this essential challenge, a new architecture, termed the hybrid satellite-terrestrial relay network (HSTRN) is utilized to harness the advantages of both the nonterrestrial and terrestrial communications [7], [8], [9]. In particular, a typical HSTRN consists of terrestrial relays cooperatively working with satellites to enable satellite coverage available in high-density and nonline-of-sight environments. In recent years, various approaches have been proposed to improve the performance of HSTRN [10], [11], [12], [13], [14], [15]. For example, An et al. [10] considered an HSTRN system with multiple ground users and a relay to facilitate communications from a satellite to the users. To optimize the system performance in terms of outage probability (OP) and ergodic capacity, the authors developed an opportunistic scheduling method to select a desired user to communicate with the relay based on the system's current conditions. Differently, Yan et al. [11] proposed a cooperative nonorthogonal multiple access scheme to further improve the performance of a downlink HSTRN system. In particular, the proposed solution will select a user with better channel conditions to act as a relay node to forward information transmitted from the satellite to other users in the system. To improve the spectral efficiency and efficiently deal with the limited spectrum problem in HSTRN systems, An et al. [12] proposed two content caching approaches, including the most

Zhiguo Ding is with the Khalifa University, Abu Dhabi 127788, UAE, and also with the University of Manchester, M1 9BB Manchester, U.K. (e-mail: zhiguo.ding@ieee.org).

Digital Object Identifier 10.1109/JSYST.2024.3463715

popular content-based scheme and the uniform content-based scheme. Simulation results demonstrated the effectiveness of the proposed solutions.

Although achieving superior performance, the above works and many others in the literature have not taken into account the issue of security in HSTRN systems. In practice, the broadcast nature of wireless links makes SatCom extremely vulnerable to radio security threats, especially eavesdropping attacks. In particular, an eavesdropper can easily intercept the transmitted signals on the target channel. Due to their passive nature, it is very challenging to detect and prevent eavesdropping from "wiretapping" legitimate wireless channels [16]. Consequently, eavesdropping is one of the most dangerous security threats for wireless communication systems, including HSTRN [6], [17]. A common approach to deal with eavesdroppers is using cryptographic techniques to encode information at the transportation and network layers before transmitting over wireless channels [18]. However, encrypting and decrypting information will add computing and resource burdens to wireless devices, which is problematic for power-constrained devices [19]. More importantly, with recent advances in quantum computing, existing cryptography techniques could soon become unreliable while quantum-safe or postquantum cryptography is still under development [20].

A potential solution to effectively mitigate eavesdropping attacks in satellite communication networks is to use artificial noise [21], [22], [23] or friendly jammers that generate interference signals to disrupt the reception processes at eavesdroppers. For instance, Bouabdellah and Bouanani [24] considered a cognitive satellite-terrestrial network in which a secondary user (SU) can transmit information to optical ground stations through the aid of a relay satellite. To defeat eavesdropping attacks, other SUs can act as friendly jammers and broadcast artificial noise that interferes with eavesdroppers, thus improving the system's privacy. Differently, Yin et al. [25] pointed out that co-channel interference caused by the spectrum sharing between terrestrial and satellite networks and the interbeam interference from the frequency reuse among satellites can be leveraged to secure the communications of both the satellite and terrestrial links. To enable that capability, the authors formulated an optimization problem to jointly optimize the beamforming policies of satellites and base stations in the system. To deal with eavesdropping attacks in HSTRN, Li et al. [26] proposed a Stackelberg game to strike a balance between the secure spectrum efficiency and the secure energy efficiency in the presence of an eavesdropper with the support of a friendly jammer.

Nevertheless, there is still a lack of formal analyses of the OP and secrecy outage probability (SOP) for the HSTRN system under eavesdropping attacks in existing studies. As such, in our previous works [6], [27], we formally analyzed the OP and SOP of an HSTRN system with the support of a friendly jammer to deal with eavesdropping attacks. Unfortunately, using only one friendly jammer may not guarantee a high privacy level for the system, particularly if there are multiple eavesdroppers trying to wiretap the transmitted signals and the jammer can be broken or compromised. As such, in this article, we focus on a more important case with multiple friendly jammers that generate artificial noise to defeat eavesdropping in an HSTRN system. Using multiple friendly jammers yields several advantages. In particular, multiple jammers can cover a larger area than a single jammer, resulting in better security coverage for the system. In addition, various jammers can combine their jamming signals, making it more difficult for eavesdroppers to extract useful information from transmitted signals. Finally, with multiple jammers, the security reliability can be significantly enhanced as the failure of a jammer does not make the whole system vulnerable to eavesdropping attacks. Another contribution of this article is to focus on the fact that existing studies fail to handle complex systems (e.g., multiple friendly jammers and multiple relays as considered in this article) due to their mathematical intractability derivations. As such, this article will introduce an effective yet lightweight deep learning-based solution to evaluate the OP and SOP of the system without using complex mathematical operations. The major contributions of this article are highlighted as follows.[1]

1) We consider multiple friendly jammers to defeat eavesdropping attacks in an HSTRN system. Then, closed-form expressions for the OP and SOP given imperfect channel state information (CSI) are derived. To the best of our knowledge, this is the first work that introduces a formal analysis of the OP and SOP for the HSTRN system with multiple jammers in the presence of independent but non-identically distributed (i.n.i.d.) shadow Rician for satellite links.
2) A deep neural network (DNN) model is specifically crafted to forecast the operational OP and SOP performance of the innovative HSTRN system. The study showcases the effectiveness of DNN models in predicting performance within intricate network scenarios, using a low-latency inference process.
3) We perform extensive simulations to evaluate the proposed approaches in various scenarios. Moreover, discussions about the impact of different key parameters on the performance of the HSTRN system, such as the number of relays, the satellite's transmit power, and the transmit power of relays, will be presented.

The rest of this article is organized as follows: Section II introduces the system mode including the channel model and the information transmission process. Sections III and IV show the OP and SOP analyses, respectively. Section V presents the proposed deep learning approach to predict the OP and SOP of the system. Numerical results are discussed in Section VI-B. Finally, Section VII concludes this article.

II. System and Signal Models

This section presents the considered system model together with the data transmission protocol.

A. Channel Model

For practical applications, channel estimation is required to obtain CSI estimates at the destination, by employing the broadcast pilot signals. However, due to limited hardware and finite radio resources for sending pilot signals, channel estimation cannot be carried out perfectly in practice, which leads to non-negligible channel estimation errors (CEEs). In this article, we utilize the minimum mean square error (MMSE) estimation method as in [28], which means that the channel estimate is formulated as follows:

$$\hat{h}_i = h_i + e_i \tag{1}$$

[1]The contributions of our work compared with the previous works are shown in Table I.

where S, R_n with $n \in \{1, \ldots, N\}$, D, E, and J_m with $m \in \{1, \ldots, M\}$ denote source, relay node, destination, eavesdropper, and jammer, respectively; e_i with $i \in (\mathrm{SR}_n, \mathrm{R}_n\mathrm{D}, \mathrm{R}_n\mathrm{E}, \mathrm{JE}, \mathrm{JR}_n, \mathrm{JD})$ is the CEE, distributed as $e_i \sim \mathcal{CN}(0, \mu_i^2)$, $\hat{h}_i$ is the estimated channel of h_i.[2]

1) Channel Model Between Terrestrial Nodes: In this article, we provide a statistical analysis of fading channels in each hop. We assume that the channels between any two nodes in terrestrial links can be modeled as block Rayleigh fading. This means that the channel coefficients remain constant within a transmission block but vary independently across different blocks. Since the channels exhibit Rayleigh fading, we focus on the squared amplitudes of the channel gains, such as

$$\gamma_{\mathrm{R}_n\mathrm{E}} = |h_{\mathrm{R}_n\mathrm{E}}|^2, \gamma_{\mathrm{R}_n\mathrm{D}} = |h_{\mathrm{R}_n\mathrm{D}}|^2. \quad (2)$$

The squared amplitudes of the channel gains can be modeled as exponential random variables (RVs), with corresponding probability density function (PDF) and cumulative distribution function (CDF) given by the following equations, respectively:

$$F_X(x) = 1 - \exp(-\lambda x) \quad (3)$$

$$f_X(x) = \frac{\partial F_X(x)}{\partial x} = \lambda \exp(-\lambda x). \quad (4)$$

where λ is the mean of the exponential RV X. Next, for the satellite links, we consider the Shadowed-Rician fading model [10]. Thereby, the PDF of the squared amplitude of the channel coefficient $\gamma_{\mathrm{SR}_n} = |h_{\mathrm{SR}_n}|^2$ between the satellite and the nth relay is given by [7], [8] as follows:

$$f_{\gamma_{\mathrm{SR}_n}}(x) = \alpha_n \exp(-\beta_n x)\, {}_1F_1(m_n; 1; \delta_n x), x \geqslant 0 \quad (5)$$

where the following definitions hold:

$$\alpha_n = \beta_n \left(\frac{2b_n m_n}{2b_n m_n + \Omega_n}\right)^{m_n} \quad (6)$$

$$\beta_n = \frac{1}{2b_n} \quad (7)$$

$$\delta_n = \frac{\beta_n \Omega_n}{2b_n m_n + \Omega_n} \quad (8)$$

with Ω_n and $2b_n$ being the average power of LOS and multipath components at the nth relay, respectively. Herein, m_n is the fading severity parameter at the nth relay and ${}_1F_1(.;.;.)$ is the first-kind confluent hypergeometric function [29, eq.9.210.1]. With any integer-valued fading severity parameters, one can simplify ${}_1F_1(m_n; 1; \delta_n x)$ in (4) to express the PDF of γ_{SR_n} by utilizing the similar methodology in [30] as follows:

$$f_{\gamma_{\mathrm{SR}_n}}(x) = \alpha_n \sum_{k=0}^{m_n-1} \zeta_n(k) x^k \exp(-(\beta_n - \delta_n)x) \quad (9)$$

where $\zeta_n(k)$ is defined as

$$\zeta_n(k) = \frac{(-1)^k (1-m_n)_k \delta_n^k}{(k!)^2} \quad (10)$$

[2]In this article, we assume that there is no communication link between S and E. The considered phenomenon corresponds to the large obstacles between S and E. Furthermore, in order to receive the signals from a satellite, it requires a specific hardware configuration to eavesdrop information from S due to the typical architecture of the space communication. Multiple friendly jammers considered in this paper are easy to deploy in practice since the noncoherent joint transmission protocol is exploited.

with $(\cdot)_k$ being the Pochhammer symbol [29, p. xliii]. After that, the corresponding CDF is given by

$$F_{\gamma_{\mathrm{SR}_n}}(x) = \Pr(\gamma_{\mathrm{SR}_n} < x) = \int_0^x f_{\gamma_{\mathrm{SR}_n}}(x) dx \quad (11)$$

which can be obtained after using of [29, Eq. 3.351.1] as follows:

$$\begin{aligned} F_{\gamma_{\mathrm{SR}_n}}(x) &= 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^{k} \frac{\zeta_n(k) k!}{p!} (\beta_n - \delta_n)^{-(k+1-p)} \\ &\quad \times x^p \exp(-(\beta_n - \delta_n)x) \\ &= 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^{k} \frac{(-1)^k (1-m_n)_k \delta_n^k}{k! p!} \\ &\quad \times (\beta_n - \delta_n)^{-(k+1-p)} x^p \exp(-(\beta_n - \delta_n)x). \end{aligned}$$

In the considered model, following the previous works [7], [31], the relays are the fixed-location stations, which are located to have the free-space distance to the satellite such as on the roof of high buildings. In contrast, the eavesdropper E is just mobile device operating similar to the destination. Therefore, it can not receive the signal directly from the satellite due to obstacles. The hardware configuration for the relays is assumed to be the typical configuration of the earth station in the satellite communication systems [32].

B. Information Transmission

This section focuses on the DF relaying protocol in which the relay first decodes the received signal and then forwards it to the destination. Because the relay nodes work in a full-duplex mode, the signal transmission from the satellite to the destination with the help of the relay requires a one-time phase. First, satellite S transmits its signal x_s to the relay R_n. Hence, the received signal at R_n can be thus given by

$$y_{\mathrm{R}_n} = \widehat{h}_{\mathrm{SR}_n} x_{\mathrm{S}} + n_{\mathrm{R}_n} = (h_{\mathrm{SR}_n} + e_{\mathrm{SR}_n}) x_{\mathrm{S}} + n_{\mathrm{R}_n} \quad (12)$$

where x_{S} and x_{R_n} are the energy symbol with $\mathrm{E}\{|x_{\mathrm{S}}|^2\} = P_{\mathrm{S}}$ and $\mathrm{E}\{|x_{\mathrm{R}_n}|^2\} = P_{\mathrm{R}_n}$. Here, $\mathrm{E}\{\cdot\}$ is the expectation operation and n_{R_n} is the zero-mean additive white Gaussian noise (AWGN) with variance N_0 at the nth relay. After relaying the nth received the signal from satellite, it will decode this signal and then forward it to D. Meanwhile, the eavesdroppers track the signal transmitted from the relay and try to eavesdrop the information. The cooperative jamming technique is employed to diminish the quality of the eavesdropping link, where multiple friendly jammers (J_n) are employed to continuously generate artificial noises for eavesdroppers. Furthermore, the relays and destination have to cooperate with the jammers to cancel the interference in the received signals. Considering the masking effect, it becomes extremely challenging for eavesdroppers to directly intercept the signal from the source. Therefore, we assume that the eavesdroppers only monitor the transmitted signal from the relay for potential attacks, which aligns with the common approach adopted in the literature [7], [33], [34]. Hence, the received signal at the destination and eavesdropper can be expressed, respectively, as follows:

$$y_{\mathrm{D}} = (h_{\mathrm{R}_n\mathrm{D}} + e_{\mathrm{R}_n\mathrm{D}}) x_{\mathrm{R}_n} + n_{\mathrm{D}} \quad (13)$$

$$y_{\mathrm{E}} = \left(h_{\mathrm{R}_n\mathrm{E}} + e_{\mathrm{R}_n\mathrm{E}}\right) x_{\mathrm{R}_n} + \sum_{k=1}^{M} \left(h_{\mathrm{J}_k\mathrm{E}} + e_{\mathrm{J}_k\mathrm{E}}\right) x_{\mathrm{J}_k} + n_{\mathrm{E}} \quad (14)$$

where n_{D} and n_{E} are the zero mean AWGN with variance N_0 at the destination and the eavesdropper, respectively; x_{J_k} is the transmit signal at J_k and satisfied $\mathrm{E}\{|x_{\mathrm{J}_k}|^2\} = P_{\mathrm{J}_k}$. To facilitate the performance analysis, we assume that all CEEs at each at each S-R_n or R_n-D or R_n-E, etc., links are the same such as $\mu^2_{\mathrm{SR}_1} = \mu^2_{\mathrm{SR}_2} = \ldots = \mu^2_{\mathrm{SR}_n} = \mu^2_{\mathrm{SR}}, \forall n \in (1, 2, \ldots, N)$, etc. Moreover, we also assume that all jammers have the same transmit power P_{J} and all CEEs in $\mathrm{J}_k\mathrm{E}, k \in (1, \ldots, M)$, links are equal.[3] From (12)–(14), the signal-to-noise ratio (SNR) at the nth relay, destination and eavesdropper can be expressed, respectively, as follows:

$$\gamma_{\mathrm{R}_n} = \frac{\gamma_{\mathrm{SR}_n} P_{\mathrm{S}}}{\mu^2_{\mathrm{SR}} P_{\mathrm{S}} + \mathrm{N}_0} = \frac{\gamma_{\mathrm{SR}_n} \Psi}{\mu^2_{\mathrm{SR}} \Psi + 1} \quad (15)$$

$$\gamma_{\mathrm{D}} = \frac{\Phi \gamma_{\mathrm{R}_n\mathrm{D}}}{\mu^2_{\mathrm{RD}} \Phi + 1} \quad (16)$$

$$\gamma_{\mathrm{E}} = \frac{\Phi \gamma_{\mathrm{R}_n\mathrm{E}}}{\mu^2_{\mathrm{RE}} \Phi + \Theta\left(\gamma_{\mathrm{JE}} + M\mu^2_{\mathrm{JE}}\right) + 1} \quad (17)$$

where $\Psi = P_{\mathrm{S}}/N_0$, $\Phi = P_{\mathrm{R}}/N_0$, $\Theta = P_{\mathrm{J}}/N_0$, and $\gamma_{\mathrm{JE}} = \sum_{k=1}^{M} |h_{\mathrm{J}_k\mathrm{E}}|^2$.

Remark 1: This article applies the partial relay selection (PRS) method. Specifically, we introduce a sub-optimal relay selection protocol that involves selecting the best relay as follows:

$$a = \underbrace{\mathrm{argmax}}_{n=1,2,\ldots,N} \{\gamma_{\mathrm{SR}_n}\} \Leftrightarrow \gamma_{\mathrm{SR}_a} = \underbrace{\max}_{n=1,2,\ldots,N} \{\gamma_{\mathrm{SR}_n}\} \quad (18)$$

where a denotes the index of the best relay.

We assume that the links from *S* to the *N* relays nodes are n.i.i.d Rician. Bankey and Upadhyay [7] and Bhatnagar and Arti [8] considered the i.i.d channel with the same parameter between *S* and *N* relays. In contrast, this work investigates a more generalized i.i.d scenario where *S* will transmit its information to each relay with different parameters such as a, β, σ, m, etc. Hence, the CDF of γ_{SR_a} can be computed as follows:

$$F_{\gamma_{\mathrm{SR}_a}}(x) = \Pr\left(\underbrace{\max}_{n=1,2,\ldots,N} \{\gamma_{\mathrm{SR}_n}\} < x\right) = \prod_{n=1}^{N} F_{\gamma_{\mathrm{SR}_n}}(x) \quad (19)$$

By substituting (12) into (19), we obtain the following result:

$$F_{\gamma_{\mathrm{SR}_a}}(x) = \prod_{n=1}^{N}\Bigg(1 - \alpha_n \sum_{k=0}^{m_n-1}\sum_{p=0}^{k} \frac{(-1)^k (1-m_n)_k (\delta_n)^k}{k!p!} (\beta_n - \delta_n)^{-(k+1-p)} \times x^p \exp\left(-(\beta_n - \delta_n)x\right)\Bigg). \quad (20)$$

In order to obtain a compact expression, let us set

$$x_n = \alpha_n \sum_{k=0}^{m_n-1}\sum_{p=0}^{k} \frac{(-1)^k (1-m_n)_k (\delta_n)^k}{k!p!} (\beta_n - \delta_n)^{-(k+1-p)} \times x^p \exp\left(-(\beta_n - \delta_n)x\right). \quad (21)$$

Then (20) is reformulated as follows:

$$F_{\gamma_{\mathrm{SR}_a}}(x) = \prod_{n=1}^{N}(1 - x_n) = 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \underbrace{\sum_{l_1=1}^{N} \ldots \sum_{l_n=1}^{N}}_{l_1 \neq l_2 \ldots \neq l_n} \prod_{t=1}^{n} x_{n_t}. \quad (22)$$

We note that in (22), x_{n_t} can be expanded as

$$\prod_{t=1}^{n} x_{n_t} = \sum_{k_1=0}^{m_{n_t}-1}\sum_{p_1=0}^{k_1} \cdots \sum_{k_n=0}^{m_{n_t}-1}\sum_{p_n=0}^{k_n}\prod_{t=1}^{n}\alpha_{n_t} \frac{(-1)^{k_t}(1-m_{n_t})_{k_t}(\delta_{n_t})^{k_t}}{k_t! p_t!} (\beta_{n_t} - \delta_{n_t})^{-(k_t+1-p_t)} x^{\sum_{t=1}^{n} p_t} \exp\left(-\sum_{t=1}^{n}(\beta_{n_t} - \delta_{n_t})x\right). \quad (23)$$

Based on (22) and (23), $F_{\gamma_{\mathrm{SR}_a}}(x)$ can be expressed by

$$F_{\gamma_{\mathrm{SR}_a}}(x) = 1 + \sum_{n=1}^{N}\frac{(-1)^n}{n!}\sum^{*}\alpha_{n_t}\frac{(-1)^{k_t}(1-m_{n_t})_{k_t}(\delta_{n_t})^{k_t}}{k_t!p_t!} (\beta_{n_t} - \delta_{n_t})^{-(k_t+1-p_t)} x^{\sum_{t=1}^{n} p_t}\exp\left(-\sum_{t=1}^{n}(\beta_{n_t} - \delta_{n_t})x\right)$$

where $\sum^{*} = \underbrace{\sum_{l_1=1}^{N} \ldots \sum_{l_n=1}^{N}}_{l_1 \neq l_2 \ldots \neq l_n} \sum_{k_1=0}^{m_{n_t}-1}\sum_{p_1=0}^{k_1} \cdots \sum_{k_n=0}^{m_{n_t}-1} \sum_{p_n=0}^{k_n}\prod_{t=1}^{n}$.

Remark 2: Since γ_{JE} is a summation of M i.i.d. exponential RVs, its PDF can be given by [35] as follows:

$$f_{\gamma_{\mathrm{JE}}}(x) = \frac{(\lambda_{\mathrm{JE}})^M}{(M-1)!} x^{M-1} \exp(-\lambda_{\mathrm{JE}} x) \quad (24)$$

where λ_{JE} is the mean of RV γ_{JE}.

III. OP Analysis

With the DF scheme, the OP of system can be defined as

$$\mathrm{OP} = \Pr\left(\gamma_{\mathrm{DF}} < \gamma_{\mathrm{th}}\right) = \Pr\left(\min\left(\gamma_{\mathrm{R}_a}, \gamma_{\mathrm{D}}\right) < \gamma_{\mathrm{th}}\right) \quad (25)$$

where $\gamma_{\mathrm{th}} = 2^{2C_{\mathrm{th}}} - 1$ is the predefined threshold of system and C_{th} is the target rate. Based on (15), (16), and (18), the OP can be rewritten as follows:

$$\begin{aligned}\mathrm{OP} &= \Pr\left(\min\left(\Theta_1, \Theta_2\right) < \gamma_{\mathrm{th}}\right) \\ &= 1 - \underbrace{\Pr\left(\Theta_1 \geqslant \gamma_{\mathrm{th}}\right)}_{\mathrm{P}_1}\underbrace{\Pr\left(\Theta_2 \geqslant \gamma_{\mathrm{th}}\right)}_{\mathrm{P}_2}.\end{aligned} \quad (26)$$

[3] Another way to attack E is by utilizing artificial noise. Different from our framework, Rs can generate such artificial noise. Besides, the power consumption of the jammers can be reduced by optimizing the difference between the distance from the jammers to the eavesdropper and to the legitimate receiver. This extension has the potential for future work.

where

$$\Theta_1 \triangleq \frac{\Psi\gamma_{\mathrm{SR}_a}}{\mu_{\mathrm{SR}}^2\Psi+1} \quad (27)$$

$$\Theta_2 \triangleq \frac{\Phi\gamma_{\mathrm{R}_a\mathrm{D}}}{\mu_{\mathrm{RD}}^2\Phi+1}. \quad (28)$$

In order to investigate the OP, we now compute P_1 as follows:

$$\mathrm{P}_1 = \Pr\left(\Theta_1 \geqslant \gamma_{\mathrm{th}}\right) = 1 - F_{\gamma_{\mathrm{SR}_a}}\left(\frac{\gamma_{\mathrm{th}}\Theta_1}{\Psi}\right). \quad (29)$$

By applying (24), (29) can be recalculated as follows:

$$\mathrm{P}_1 = \sum_{n=1}^{N}\frac{(-1)^{n+1}}{n!}\sum\nolimits^{*}\alpha_{n_t}\frac{(-1)^{k_t}\left(1-m_{n_t}\right)_{k_t}\left(\delta_{n_t}\right)^{k_t}}{k_t!p_t!\left(\beta_{n_t}-\delta_{n_t}\right)^{(k_t+1-p_t)}} \times\left(\Delta\gamma_{\mathrm{th}}\right)^{\sum_{t=1}^{n}p_t}\exp\left(-\gamma_{\mathrm{th}}\tilde{\Delta}\right) \quad (30)$$

where

$$\Delta = \frac{\left(\mu_{\mathrm{SR}}^2\Psi+1\right)}{\Psi} \quad (31)$$

$$\tilde{\Delta} = \sum_{t=1}^{n}\left(\beta_{n_t}-\delta_{n_t}\right)\Delta. \quad (32)$$

We now compute P2 in (26) as follows:

$$\begin{aligned}\mathrm{P}_2 &= \Pr\left(\frac{\Phi\gamma_{\mathrm{R}_a\mathrm{D}}}{\mu_{\mathrm{RD}}^2\Phi+1} \geq \gamma_{\mathrm{th}}\right)\\ &= 1-\Pr\left(\gamma_{\mathrm{R}_a\mathrm{D}} < \frac{\gamma_{\mathrm{th}}\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}\right)\\ &= \exp\left(-\gamma_{\mathrm{th}}\tilde{\lambda}_{\mathrm{RD}}\right)\end{aligned}$$

where

$$\tilde{\lambda}_{\mathrm{RD}} \triangleq \frac{\lambda_{\mathrm{RD}}\left(\mu_{\mathrm{RD}}^2\Phi+1\right)}{\Phi}. \quad (33)$$

By substituting (23) and (24) into (20), the following theorem can be obtained.

Theorem 1: The OP of the considered communication scenario can be expressed as follows:

$$\mathrm{OP} = 1 - \begin{Bmatrix} 1-\sum_{n=1}^{N}\frac{(-1)^{n+1}}{n!}\sum\nolimits^{*}\alpha_{n_t}\frac{(-1)^{k_t}\left(1-m_{n_t}\right)_{k_t}\left(\delta_{n_t}\right)^{k_t}}{k_t!p_t!\left(\beta_{n_t}-\delta_{n_t}\right)^{(k_t+1-p_t)}}\\ \left(\Delta\gamma_{\mathrm{th}}\right)^{\sum_{t=1}^{n}p_t}\exp\left(-\gamma_{\mathrm{th}}\tilde{\Delta}\right)\end{Bmatrix} \times\exp\left(-\gamma_{\mathrm{th}}\tilde{\lambda}_{\mathrm{RD}}\right).$$

IV. SOP Analysis

Within the field of physical layer security, as discussed in prior research, such as [36], the focus lies on exploring the feasibility of transmitting confidential messages at a positive rate, known as the secrecy rate. The objective is to maintain the eavesdropper's ignorance when the channel between the source and legitimate destination is superior to the channel between the source and eavesdropper. Furthermore, a greater disparity in channel strengths between these two channels leads to higher achieved secrecy rates. The secrecy rate can be defined as follows:

$$C_{\mathrm{sec}} = \max\left(C_{\mathrm{DF}} - C_{\mathrm{E}}, 0\right) \quad (34)$$

where the achievable data rates of the DF system and at the eavesdropper E are, respectively, defined as follows:

$$C_{\mathrm{DF}} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{DF}}\right) \text{ and } C_{\mathrm{E}} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}^{\mathrm{DF}}\right) \quad (35)$$

with $\gamma_{\mathrm{E}}^{\mathrm{DF}} = \min(\gamma_{\mathrm{R}_a}, \gamma_{\mathrm{E}})$. To ensure the confidentiality of the message, it is crucial to maintain the secrecy rate above a certain threshold. A secrecy outage occurs when the achievable secrecy rate falls below this threshold. Mathematically, a secrecy outage can be defined as follows:

$$\begin{aligned}\mathrm{SOP} &= \Pr\left(C_{\mathrm{sec}} < C_{\mathrm{th}}\right) = \Pr\left(\frac{1+\gamma_{\mathrm{DF}}}{1+\gamma_{\mathrm{E}}^{\mathrm{DF}}} < 2^{2C_{\mathrm{th}}}\right)\\ &\approx \Pr\left(\frac{\gamma_{\mathrm{DF}}}{\gamma_{\mathrm{E}}^{\mathrm{DF}}} < 2^{2C_{\mathrm{th}}}\right). \quad (36)\end{aligned}$$

Plugging (16) and (17) into (36), the SOP can be further expressed as follows:

$$\begin{aligned}&\mathrm{SOP}\\ &= \Pr\left(\min\left(\Theta_1,\Theta_2\right) < \tilde{\gamma}_{\mathrm{th}}\min\left(\Theta_1,\Theta_3\right)\right)\\ &= \int_0^\infty \Pr\left(\min\left(y,\Theta_2\right) < \tilde{\gamma}_{\mathrm{th}}\min\left(y,\Theta_3\right)\right) f_{\gamma_{\mathrm{R}_a}}(y)dy\\ &= \int_0^\infty \underbrace{\Pr\left(\Lambda_1 < \tilde{\gamma}_{\mathrm{th}}\Lambda_2\right)}_{\Upsilon}\times f_{\Theta_1}(y)dy\end{aligned}$$

where

$$\tilde{\gamma}_{\mathrm{th}} \triangleq 2^{2C_{\mathrm{th}}}, \quad (37)$$

$$\Lambda_1 \triangleq \min\left(y,\Theta_2\right) \quad (38)$$

$$\Lambda_2 \triangleq \min\left(y,\Theta_3\right) \quad (39)$$

$$\Theta_3 \triangleq \frac{\Phi\gamma_{\mathrm{R}_a\mathrm{E}}}{\mu_{\mathrm{RE}}^2\Phi+\Theta\left(\gamma_{\mathrm{JE}}+M\mu_{\mathrm{JE}}^2\right)+1}. \quad (40)$$

First, Υ in (37) can be expressed as follows:

$$\Upsilon = \Pr\left(\Lambda_1 < \tilde{\gamma}_{\mathrm{th}}\Lambda_2\right) = \int_0^\infty F_{\Lambda_1}\left(\tilde{\gamma}_{\mathrm{th}}z\right)\times f_{\Lambda_2}(z)dz. \quad (41)$$

From (41), the CDF $F_{\Lambda_1}(\tilde{\gamma}_{\mathrm{th}}y)$ can be calculated as follows:

$$\begin{aligned}F_{\Lambda_1}\left(\tilde{\gamma}_{\mathrm{th}}y\right) &= \Pr\left(\min\left(y,\Phi_2\right) < \tilde{\gamma}_{\mathrm{th}}z\right)\\ &= 1-\Pr\left(\Phi_2 \geq \tilde{\gamma}_{\mathrm{th}}z\right)\Pr\left(y \geq \tilde{\gamma}_{\mathrm{th}}z\right)\\ &= \begin{cases}1-\exp\left(-\frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{\mathrm{th}}z\left(\mu_{\mathrm{RD}}^2\Phi+1\right)}{\Phi}\right), & z \leq \frac{y}{\tilde{\gamma}_{\mathrm{th}}}\\ 1, & z > \frac{y}{\tilde{\gamma}_{\mathrm{th}}}.\end{cases} \quad (42)\end{aligned}$$

By substituting (42) into (41), it yields

$$\Upsilon = \int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\left\{1-\exp\left(-\frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{\mathrm{th}}z\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}\right)\right\}\times f_{\Lambda_2}(z)dz + \int_{\frac{y}{\tilde{\gamma}_{th}}}^{\infty} f_{\Lambda_2}(z)dz. \quad (43)$$

Next, the CDF $F_{\Lambda_2}(z)$ can be given by the following:

$$\begin{aligned}&F_{\Lambda_2}(z)\\ &= \Pr\left(\min\left(y,\frac{\Phi\gamma_{\mathrm{R}_a\mathrm{E}}}{\mu_{\mathrm{RE}}^2\Phi+\Theta\left(\gamma_{\mathrm{JE}}+M\mu_{\mathrm{JE}}^2\right)+1}\right) < z\right)\\ &= 1-\Pr\left(\frac{\Phi\gamma_{\mathrm{R}_a\mathrm{E}}}{\mu_{\mathrm{RE}}^2\Phi+\Theta\left(\gamma_{\mathrm{JE}}+M\mu_{\mathrm{JE}}^2\right)+1} \geq z\right)\Pr\left(y \geq z\right)\end{aligned}$$

$$= \begin{cases} \underbrace{\Pr\left(\frac{\Phi\gamma_{\mathrm{R}_a\mathrm{E}}}{\mu_{\mathrm{RE}}^2\Phi+\Theta\left(\gamma_{\mathrm{JE}}+M\mu_{\mathrm{JE}}^2\right)+1}<z\right)}_{\Xi}, & \text{if } z\le y \\ 1 & \text{if } z>y. \end{cases} \quad (44)$$

Then, Ξ in (44) can be formulated as follows:

$$\Xi = \Pr\left(\frac{\Phi\gamma_{\mathrm{R}_a\mathrm{E}}}{\mu_{\mathrm{RE}}^2\Phi+\Theta\left(\gamma_{\mathrm{JE}}+M\mu_{\mathrm{JE}}^2\right)+1}<z\right) = \int_0^\infty F_{\gamma_{\mathrm{R}_a\mathrm{E}}}\left\{\frac{z\left[\mu_{\mathrm{RE}}^2\Phi+\Theta\left(x+M\mu_{\mathrm{JE}}^2\right)+1\right]}{\Phi}\right\} \times f_{\gamma_{\mathrm{JE}}}(x)dx. \quad (45)$$

By substituting (24) into (45), we have

$$\Xi = 1-\frac{(\lambda_{\mathrm{JE}})^M}{(M-1)!} \times \exp(-z\kappa)\times\int_0^\infty x^{M-1}\exp\left(-x\left[\frac{z\Theta\lambda_{\mathrm{RE}}}{\Phi}+\lambda_{\mathrm{JE}}\right]\right)dx \quad (46)$$

where

$$\kappa \triangleq \frac{\lambda_{\mathrm{RE}}\left(\mu_{\mathrm{RE}}^2\Phi+\Theta M\mu_{\mathrm{JE}}^2+1\right)}{\Phi}. \quad (47)$$

By adopting [37, Eq. 3.381.4], Ξ is reformulated as follows:

$$\Xi = 1-\left(z\tilde{\lambda}+1\right)^{-M}\times\exp(-z\kappa) \quad (48)$$

where

$$\tilde{\lambda} = \frac{\Theta\lambda_{\mathrm{RE}}}{\Phi\lambda_{\mathrm{JE}}}. \quad (49)$$

Then, by substituting (48) into (44), we have

$$F_{\Lambda_2}(z) = \begin{cases} 1-\left(z\tilde{\lambda}+1\right)^{-M}\times\exp(-z\kappa), & \text{if } z\le y \\ 1 & \text{if } z>y \end{cases} \quad (50)$$

In order to obtain (50), we calculate PDF $f_{\Lambda_2}(z)$ as follows:

$$f_{\Lambda_2}(z) = \begin{cases} e^{-z\kappa}\left(\tilde{\lambda}z+1\right)^{-M-1}\left(\kappa\tilde{\lambda}z+M\tilde{\lambda}+\kappa\right), & \text{if } z\le y \\ 0 & \text{if } z>y \end{cases} \quad (51)$$

Based on (51), (43) can be rewritten as follows:

$$\Upsilon = \int_0^{\frac{y}{\tilde{\gamma}_{th}}}\left\{1-\exp\left(-\frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{\mathrm{th}}z\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}\right)\right\} \times f_{\Lambda_2}(z)dz+\int_{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}^\infty f_{\Lambda_2}(z)dz = 1-\int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\exp\left(-\frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{\mathrm{th}}z\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}\right)\times f_{\Lambda_2}(z)dz. \quad (52)$$

By applying (51) and (52), Υ is recalculated as follows:

$$\Upsilon = 1-\int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\exp\left(-\frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{\mathrm{th}}z\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}\right) \times\exp(-z\kappa)\left(\tilde{\lambda}z+1\right)^{-M-1}\left(\kappa\tilde{\lambda}z+M\tilde{\lambda}+\kappa\right)dz$$
$$= 1-\left(M\tilde{\lambda}+\kappa\right)\int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\left(\tilde{\lambda}z+1\right)^{-M-1}\exp(-z\tilde{\kappa})dz - \int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\kappa\tilde{\lambda}z\left(\tilde{\lambda}z+1\right)^{-M-1}\exp(-z\tilde{\kappa})dz \quad (53)$$

where

$$\tilde{\kappa} = \frac{\lambda_{\mathrm{RD}}\tilde{\gamma}_{th}\left[\mu_{\mathrm{RD}}^2\Phi+1\right]}{\Phi}+\kappa. \quad (54)$$

By applying Maclaurin series, i.e., $\exp(-z\tilde{\kappa}) = \sum_{q\ge0}\frac{(-\tilde{\kappa})^q z^q}{q!}$, (54) can be reformulated as follows:

$$\Upsilon = 1-\left(M\tilde{\lambda}+\kappa\right)\int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\left(\tilde{\lambda}z+1\right)^{-M-1}\exp(-z\tilde{\kappa})dz - \sum_{q\ge0}\frac{(-\tilde{\kappa})^q}{q!}\int_0^{\frac{y}{\tilde{\gamma}_{\mathrm{th}}}}\kappa\tilde{\lambda}z^{q+1}\left(\tilde{\lambda}z+1\right)^{-M-1}dz. \quad (55)$$

With the help of [37, Eq. 3.197.8], Υ can be expressed as follows:

$$\Upsilon = 1-\sum_{q\ge0}\frac{\left(M\tilde{\lambda}+\kappa\right)(-\tilde{\kappa})^q}{q!}\left(\frac{y}{\tilde{\gamma}_{\mathrm{th}}}\right)^{q+1}\mathrm{B}(1,q+1)\,{}_2F_1\left(M+1,q+1;q+2;-\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\mathrm{th}}}\right) - \sum_{q\ge0}\frac{(-\tilde{\kappa})^q\tilde{\lambda}\kappa}{q!}\left(\frac{y}{\tilde{\gamma}_{\mathrm{th}}}\right)^{q+2}\mathrm{B}(1,q+2)\,{}_2F_1\left(M+1,q+2;q+3;-\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\mathrm{th}}}\right) \quad (56)$$

where ${}_2F_1(\alpha,\beta;\gamma;z)$ is the first kind of Gauss hypergeometric function and $\mathrm{B}(x,y)$ is the Beta function. Next, based on (24), we obtain

$$f_{\gamma_{\mathrm{R}_a}}(y) = \sum^{**}\left(\sum_{t=1}^n p_t\right)\left(\frac{1}{\psi}\right)^{\sum_{t=1}^n p_t} y^{\sum_{t=1}^n p_t-1} \times\exp\left(-\sum_{t=1}^n\frac{(\beta_{n_t}-\delta_{n_t})}{\psi}y\right) - \sum^{**}\left(\sum_{t=1}^n(\beta_{n_t}-\delta_{n_t})\right)\left(\frac{1}{\psi}\right)^{\sum_{t=1}^n p_t+1} y^{\sum_{t=1}^n p_t} \times\exp\left(-\sum_{t=1}^n\frac{(\beta_{n_t}-\delta_{n_t})}{\psi}y\right) \quad (57)$$

where

$$\sum^{**} = \sum_{n=1}^N\frac{(-1)^n}{n!}\sum^{*}\alpha_{n_t}\frac{(-1)^{k_t}(1-m_{n_t})_{k_t}(\delta_{n_t})^{k_t}}{k_t!p_t!(\beta_{n_t}-\delta_{n_t})^{(k_t+1-p_t)}} \quad (58)$$

$$\psi = \frac{\Psi}{\mu_{\mathrm{SR}}^2\Psi+1}. \quad (59)$$

By replacing (57) and (62) into (37), the following theorem can be obtained:

Theorem 2: The SOP of the considered communication scenario can be expressed as follows:

$$\mathrm{SOP} = 1-\Upsilon_3+\Upsilon_4-\Upsilon_5+\Upsilon_6 \quad (60)$$

where

$$\Upsilon_3 =$$

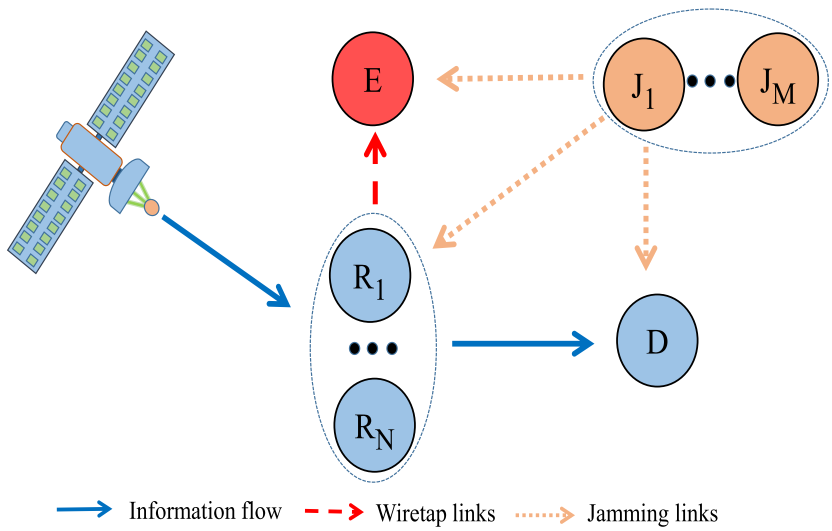


Fig. 1. Integrated satellite-terrestrial system model.

$$\sum^{**} p_{\text{sum}} \sum_{q=0}^{\infty} \frac{\left(M\tilde{\lambda}+\kappa\right)\left(-\tilde{\kappa}\right)^{q}\left(q+1\right)\mathrm{B}\left(1,q+1\right)}{M!q!(\tilde{\gamma}_{\text{th}})^{2-p_{\text{sum}}}\left(\tilde{\lambda}_{\text{sum}}\right)^{\hat{p}_{\text{sum}}+1}\left(\tilde{\lambda}\right)^{\hat{p}_{\text{sum}}-1}} \times E\left(M+1;q+1:\hat{p}_{\text{sum}}+1;q+2:\tilde{\lambda}_{\text{sum}}\right), \tag{61}$$

$$\Upsilon_4 = \sum^{**}\left(\hat{\kappa}-\kappa\right) \sum_{q=0}^{\infty} \frac{\left(M\tilde{\lambda}+\kappa\right)\left(-\tilde{\kappa}\right)^{q}\left(q+1\right)\mathrm{B}\left(1,q+1\right)}{M!q!(\tilde{\gamma}_{\text{th}})^{1-p_{\text{sum}}}\left(\tilde{\lambda}_{\text{sum}}\right)^{\hat{p}_{\text{sum}}+2}\left(\tilde{\lambda}\right)^{\hat{p}_{\text{sum}}}} \times E\left(M+1;q+1:\hat{p}_{\text{sum}}+1;q+2:\tilde{\lambda}_{\text{sum}}\right) \tag{62}$$

$$\Upsilon_5 = \sum^{**} p_{\text{sum}} \sum_{q=0}^{\infty} \frac{\left(-\tilde{\kappa}\right)^{q}\tilde{\lambda}\kappa\left(q+2\right)\mathrm{B}\left(1,q+2\right)}{M!q!(\tilde{\gamma}_{\text{th}})^{2-p_{\text{sum}}}\left(\tilde{\lambda}_{\text{sum}}\right)^{\hat{p}_{\text{sum}}+2}\left(\tilde{\lambda}\right)^{\hat{p}_{\text{sum}}}} \times E\left(M+1;q+2:\hat{p}_{\text{sum}}+1;q+3:\tilde{\lambda}_{\text{sum}}\right) \tag{63}$$

$$\Upsilon_6 = \sum^{**}\left(\hat{\kappa}-\kappa\right) \sum_{q=0}^{\infty} \frac{\left(-\tilde{\kappa}\right)^{q}\tilde{\lambda}\kappa\left(q+2\right)\mathrm{B}\left(1,q+2\right)}{M!q!(\tilde{\gamma}_{\text{th}})^{1-p_{\text{sum}}}\left(\tilde{\lambda}_{\text{sum}}\right)^{\hat{p}_{\text{sum}}+3}\left(\tilde{\lambda}\right)^{\hat{p}_{\text{sum}}+1}} \times E\left(M+1;q+2:\hat{p}_{\text{sum}}+1;q+3:\tilde{\lambda}_{\text{sum}}\right). \tag{64}$$

Remark 3: The analytical results obtained for the OP in Theorem 1 and for the SOP in Theorem 2 are independent of the small-scale fading coefficients, which can operate over multiple time slots whenever the channel statistics remain unchanged. Regarding the system design, it is of interest to consider multiple colluding eavesdropper nodes Es. Nonetheless, it is not possible to compute the analytical performance in closed form due to the complicated expressions. This potential extension should be left for future work.

V. Performance Prediction With DNN

This section designs a DNN to train and predict performance of our considered communication system.

A. DNN Descripttion

In this section, we propose a DNN model to evaluate OP and SOP, particularly given the fact that the system model is complex and employing mathematical derivation methods is challenging. The DNN model offers a viable alternative as it is data-driven. This section presents the design of the DNN model, which comprises an input layer, several hidden layers, and an output layer, as depicted in Fig. 1. In addition, the input layer comprises 10 neurons corresponding to the 10 parameters listed in Table I. The relationship between the input and output data is primarily determined by the multiple hidden layers. To accurately calculate this relationship, each link in every hidden neuron possesses unique weights and biases. For enhanced computational efficiency, each hidden neuron also incorporates a nonlinear activation function. Specifically, the rectified linear unit (ReLU) serves as the nonlinear activation function employed at each hidden layer, and it is formally defined as follows:

$$\text{ReLU}(x) = \max\left\{x, 0\right\}. \tag{65}$$

Given that the regression problem involves predicting numerical values without any additional transformation, the output layer does not require an activation function. To establish connectivity between the activation of the jth neuron in the ith layer and the activation in the $(i-1)$th layer within a fully connected layer, the following expression is considered:

$$n_j^i = \text{ReLU}\left(\sum_{z=1}^{Ne} m_{jz}^i n_z^{i-1} + u_j^i\right) \tag{66}$$

where N_e is the number of neuron for the $(i-1)$th layer, u_j^i and m_{jz}^i are the scalar bias for ith layer and the weight connecting of the zth neuron at the $(i-1)$th layer, respectively. Furthermore, considering that the objective of the regression problem is to estimate an output value without any additional conversions, the output layer, consisting of a single neuron, employs the linear activation function to provide the predicted value of OP/SOP.

B. Generating the Traning Data

In Fig. 2, we examine the accuracy of the DNN model in evaluating OP/SOP. The sample data are generated over a certain

TABLE I
OUR CONTRIBUTIONS COMPARED TO THE PREVIOUS WORKS

	Physical layer security (PLS)	Amplify-and-forward (AF)	Decode-and- forward (DF)	Imperfect CSI	DNN
Our work	x		x	x	x
[8]	x	x			
[13]		x			
[14]			x		
[15]		x			
[25]				x	

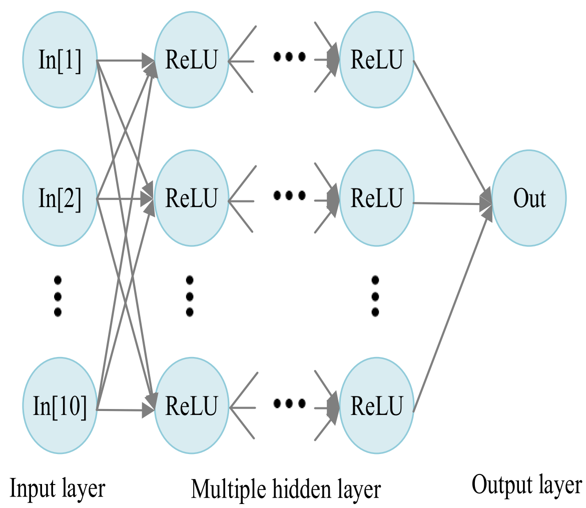


Fig. 2. Proposed DNN model for OP and SOP prediction.

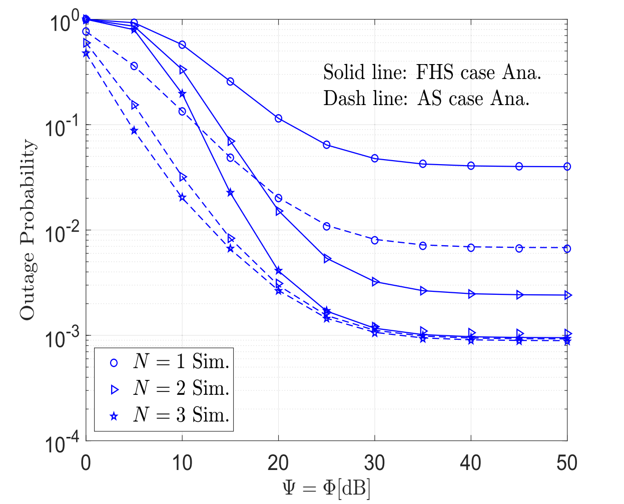


Fig. 3. OP versus $\Phi = \Psi$ when $N \in \{1, 2, 3\}$ under FHS and AS scenarios.

period, with 80% allocated for training, 10% of the data are allocated for validation, and another 10% is reserved for testing purposes. Subsequently, the estimation accuracy of the DNN model is measured by using the mean square error (MSE), i.e.,

$$\mathrm{MSE} = \frac{1}{\mathrm{D_{train}}} \sum_{\mathrm{a}=1}^{\mathrm{D_{train}}} (\mathrm{In}\,[\mathrm{n}] - \mathrm{Out}\,[\mathrm{n}])^2. \quad (67)$$

Furthermore, the root MSE (RMSE) is employed to determine the disparity between the actual and predicted OP/SOP values across the entire test set, defined as $\mathrm{RMSE} = \sqrt{\mathrm{MSE}}$. In addition, the optimal weights and biases for each connection are determined using the Adam optimizer.

VI. PERFORMANCE ANALYSIS

In this section, we first discuss the parameter setting in our Monte Carlo simulations. Then, the OP and SOP of the system are verified and evaluated under different scenarios. Finally, the OP and SOP evaluation of the proposed deep learning approach is highlighted.

A. Parameter Setting

To obtain reliable results of the OP and SOP, all simulations are performed with 10^6 independent trials. The channels between the satellite and relays follow the shadows-Rician fading channel model [38]. The channel between two arbitrary nodes in the terrestrial network follows Rayleigh fading. Unless otherwise stated, the number of relays N is 2 and the number of friendly jammers M is 5. The target rate C_{th} is set as 0.5bps/Hz. Θ and μ^2 are set at 10 dB and 0.005, respectively. The distance from each relay to the ground user d_{RD} and to the eavesdropper d_{RE} are 0.5 and 2 m, respectively. The distances between each jammer and the eavesdropper d_{JE} is 1 m. The pathloss exponent is set at 2.5. In DNN model, the numbers of neurons in the hidden layers are one hundred and 28. In addition, the activation function of the hidden layers is relu. To train the proposed DNN, Adam optimizer is used. The learning rate is set at 10^{-3}.

B. Numerical Results

1) OP and SOP Analysis: In Fig. 3, we show the OP of the considered system under the FHS and AS scenarios with the number of relays varied from 1 to 3. It can be observed from the figure that when Φ and Ψ increase from 0 to 50 dB, the OP of the system decreases. This is stemmed from the fact that when Φ and Ψ increase, the transmit powers of the relays and the satellite are also increased as $\Phi = \frac{P_R}{N_0}$ and $\Psi = \frac{P_S}{N_0}$, respectively. With stronger signals from the satellite and relays, it is easier for the ground user to decode the transmitted information. It is worth noting that with more relays, the OP of the system can be decreased as the probability of choosing a good channel from a relay to the ground user becomes higher. Finally, under the AS scenario, the OP of the system is lower than that of the FHS scenario. For instance, at $\Phi = \Psi = 25$ dB and $N = 2$, the OP under the AS scenario is around 0.0017 while the OP under the FHS scenario is around 0.0054. This stems from the fact that the FHS effect affects the satellite link more seriously than the AS effect.

In Fig. 4, we evaluate the SOP of the system obtained by simulation and our analytical expressions under the FHS and AS cases with $\Phi = 20$ dB. Clearly, when Ψ is increased from 0 to 50 dB, the SOP is decreased. This is because the increased transmit power of the source (represented as Ψ) facilitates easier

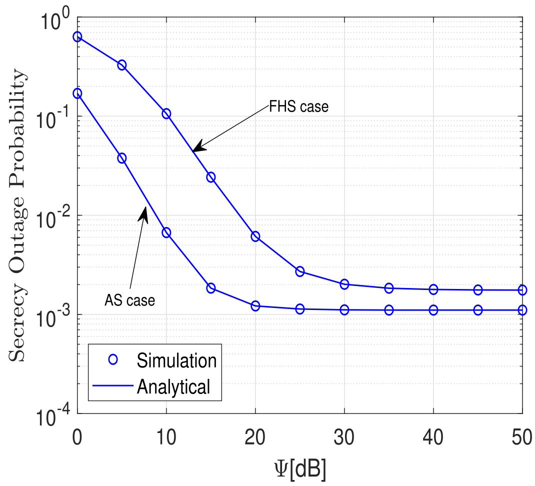


Fig. 4. SOP versus Ψ under FHS and AS scenarios.

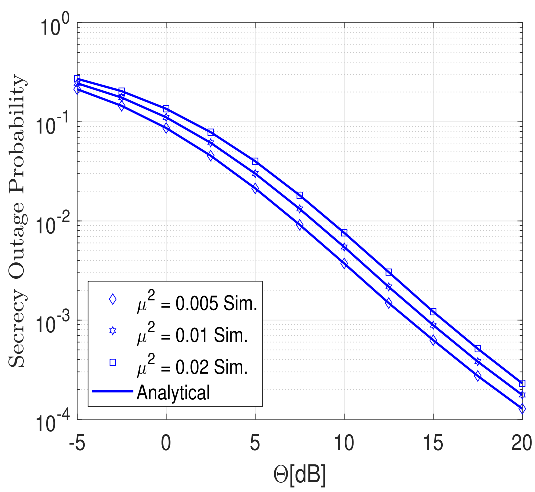


Fig. 5. SOP versus Θ with $\Phi = \Psi = 10$ dB and $\mu^2 \in \{0.005, 0.01, 0.02\}$.

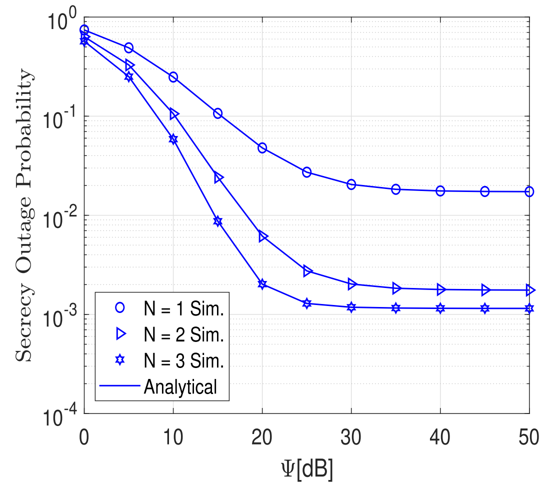


Fig. 6. SOP versus Ψ with $\Phi = 20$ dB and $\mathrm{N} \in \{1, 2, 3\}$.

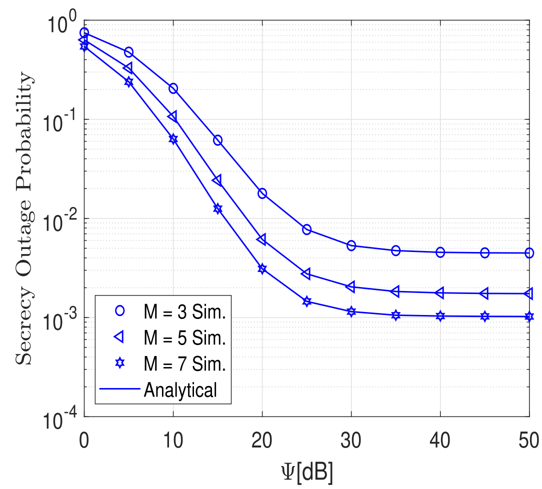


Fig. 7. SOP versus Ψ with $\Phi = 20$ dB and $M \in \{3, 5, 7\}$.

signal decoding at the receiver. More importantly, the simulation results are similar to our analytical results, demonstrating the accuracy of our SOP derivations. Again, the SOP under the AS effect is lower than that under the FHS effect.

In Fig. 5, we vary Θ from -5 to 20 dB and show the SOP performance under different values of μ^2. As shown in the figure, the SOP decreases when we increase Θ. This is because, with a higher value of Θ, the jammers can generate stronger jamming signals to better prevent the eavesdropper from wiretapping the channel. It is worth noting that when μ^2 is increased, the SOP of the system is also increased. For example, at $\Theta = 10$ dB, the SOP values are 0.0037, 0.0055, and 0.0076 with $\mu^2 = 0.005$, $\mu^2 = 0.01$, and $\mu^2 = 0.02$, respectively. It is anticipated that the SNR experienced by eavesdroppers will noticeably deteriorate when jammers increase their transmit power. However, the relay and destination can still effectively decipher the received signal by collaborating with the jammers to eliminate interference.

In Fig. 6, we evaluate the SOP performance of the system with different numbers of relays. It can be observed from the figure that with more relays in the system, the SOP is decreased. For instance, at $\Psi = 25$ dB, the SOP values are 0.0272 with 1 relay, 0.0027 with 2 relays, and 0.0013 with 3 relays. The reason is that with more relays, it is easier to find a good channel to communicate with the ground user. Again, our analytical results are comparable with the simulation results, and thus demonstrating the accuracy of the SOP analysis presented in Section IV.

In Fig. 7, we vary Ψ from 0 to 50 dB and evaluate the SOP performance with different numbers of friendly jammers. As can be seen in the figure, the SOP decreases when we employ more jammers in the systems. For example, at $\Psi = 30$ dB, the SOP values are 0.0053, 0.0020, and 0.0011 with $M = 3, M = 5$, and $M = 7$, respectively. This stems from the fact that with more jammers, significant disruption at the eavesdropper is introduced to improve the privacy level of the system. Besides, Fig. 8 shows the SOP as a function of μ_{JE}^2 with the different parameter settings. The results suggest that the imperfection of the channel estimates obtained for the jammers increase, the network has better the SOP.

2) Deep Learning Analysis: In this section, we perform our proposed deep-learning approach and obtain the estimated OP and SOP for the system. Specifically, we first evaluate the OP performance with $\mu^2 = 0.005$ and $\mu^2 = 0.01$ when varying Φ and Ψ from 0 to 50 dB, as shown in Fig. 9. Clearly , when Φ and Ψ increase, the OP of the system is decreased as the transmit powers of the satellite and relays are increased, resulting in stronger received signals at the ground user. As can be observed from the figure, our proposed deep learning approach can obtain

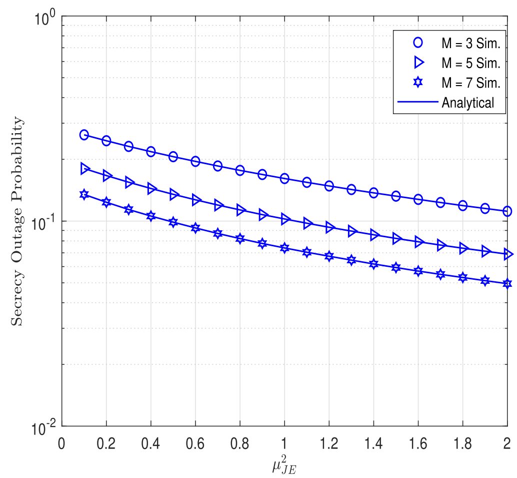


Fig. 8. SOP versus μ^2_{JE} with $\Psi = \Phi = 40$ dB and $M \in \{3, 5, 7\}$.

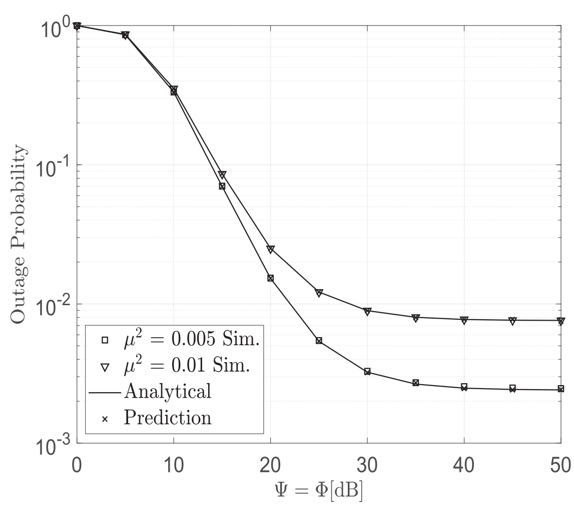


Fig. 9. OP versus $\Phi = \Psi$ with $\mu^2 \in \{0.005, 0.01\}$.

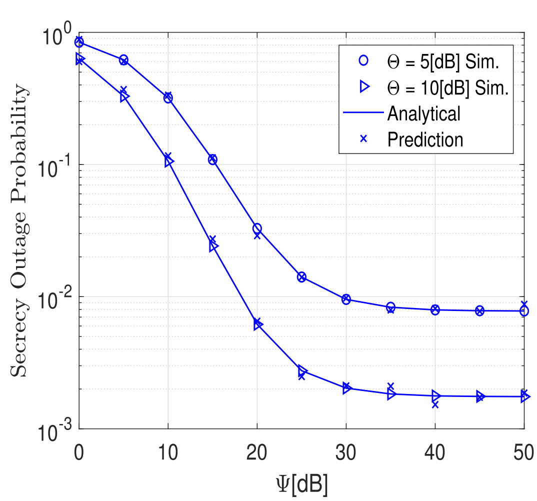


Fig. 10. SOP versus Ψ with $\Phi = 20$ dB and $\Theta \in \{5, 10\}$.

similar performance to that of the simulation and analytical methods, validating the feasibility to use DDNs to learn from raw data.

We then vary Ψ and observe the SOP performance of the proposed deep learning method with $\Theta = 5$ dB and $\Theta = 10$ dB, as illustrated in Fig. 10. As can be observed from the figure, the SOP is reduced when we increase Θ. This is because Θ is defined as the ratio of the jamming power and the variance of Gaussian noise. As such, a higher value of Θ leads to a higher transmit power of the jammers, resulting in a better security level for the system. Again, our proposed deep learning method can achieve a performance similar to that of the simulation and analytical methods while avoiding complex mathematical derivations. As the theme of the data-driven approach, we have demonstrated that deep learning can predict the solution with high accuracy toward real-time resource allocation as neural networks are implemented in hardware.

VII. Conclusion

This article presented a comprehensive investigation into the security analysis of a satellite relay network. The network consists of a single satellite, multiple relays, and a single destination, while also considering the presence of an eavesdropper. To counter the eavesdropper's impact, the network incorporates multiple jammers that generate artificial noise. The analysis focuses on deriving closed-form expressions for the OP and SOP of the system, where nonidentical Shadowed Rician and Rayleigh fading models were applied to the first and second hop, respectively. These analytical results were further validated through simulations and an innovative machine-learning prediction approach. By leveraging the obtained OP and SOP outcomes, the article investigated the security aspects of the proposed system and recommended appropriate system parameters for real-world scenarios. Specifically, the authors suggested adjusting the satellite transmit power, relay transmit power, and jammers transmit power to mitigate the eavesdropper's influence effectively.

Appendix A: Proof of Theorem 2

From (2), $\Upsilon_3, \Upsilon_4, \Upsilon_5, \Upsilon_6$ can be given as, respectively:

$$\Upsilon_3 = \sum^{**} \left(\sum_{t=1}^{n} p_t \right) \sum_{q \geq 0} \frac{\left(M\tilde{\lambda} + \kappa\right) (-\tilde{\kappa})^q \mathrm{B}\left(1, q+1\right)}{q! (\tilde{\gamma}_{\mathrm{th}})^{q+1} \psi^{\sum_{t=1}^{n} p_t}} \times \int_0^\infty y^{q + \sum_{t=1}^{n} p_t} \exp\left(- \sum_{t=1}^{n} \frac{(\beta_{n_t} - \delta_{n_t})}{\psi} y \right) {}_2F_1\left(M+1, q+1; q+2; -\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\mathrm{th}}} \right) dy, \tag{A.1}$$

$$\Upsilon_4 = \sum^{**} \left(\sum_{t=1}^{n} (\beta_{n_t} - \delta_{n_t}) \right) \times \sum_{q \geq 0} \frac{\left(M\tilde{\lambda} + \kappa\right) (-\tilde{\kappa})^q \mathrm{B}\left(1, q+1\right)}{q! (\tilde{\gamma}_{\mathrm{th}})^{q+1} \psi^{\sum_{t=1}^{n} p_t + 1}}$$

$$\times \int_0^\infty y^{q+1+\sum_{t=1}^n p_t} \exp\left(-\sum_{t=1}^n \frac{(\beta_{n_t}-\delta_{n_t})}{\psi} y\right)$$
$${}_2F_1\left(M+1, q+1; q+2; -\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\text{th}}}\right) dy, \quad \text{(A.2)}$$
$$\Upsilon_5 = \sum^{**}\left(\sum_{t=1}^n p_t\right)\sum_{q\ge 0}\frac{(-\tilde{\kappa})^q \tilde{\lambda}\kappa \mathrm{B}(1, q+2)}{q!(\tilde{\gamma}_{\text{th}})^{q+2}\psi^{\sum_{t=1}^n p_t}}$$
$$\times \int_0^\infty y^{q+1+\sum_{t=1}^n p_t} \exp\left(-\sum_{t=1}^n \frac{(\beta_{n_t}-\delta_{n_t})}{\psi} y\right)$$
$${}_2F_1\left(M+1, q+2; q+3; -\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\text{th}}}\right) dy, \quad \text{(A.3)}$$
$$\Upsilon_6 = \sum^{**}\left(\sum_{t=1}^n (\beta_{n_t}-\delta_{n_t})\right)$$
$$\times \sum_{q\ge 0}\frac{(-\tilde{\kappa})^q \tilde{\lambda}\kappa \mathrm{B}(1, q+2)}{q!(\tilde{\gamma}_{\text{th}})^{q+2}\psi^{\sum_{t=1}^n p_t+1}}$$
$$\times \int_0^\infty y^{q+2+\sum_{t=1}^n p_t} \exp\left(-\sum_{t=1}^n \frac{(\beta_{n_t}-\delta_{n_t})}{\psi} y\right)$$
$$\times {}_2F_1\left(M+1, q+2; q+3; -\frac{y\tilde{\lambda}}{\tilde{\gamma}_{\text{th}}}\right) dy. \quad \text{(A.4)}$$

Let us define $z = \frac{y\tilde{\lambda}}{\tilde{\gamma}_{th}}$ and [37, Eq. 7.522.1] and denote $p_{\text{sum}} \triangleq \sum_{t=1}^n p_t$, $\hat{p}_{\text{sum}} = q + p_{\text{sum}}$, $\hat{\kappa} = \kappa + \sum_{t=1}^n (\beta_{n_t} - \delta_{n_t})$, $\tilde{\lambda}_{\text{sum}} \triangleq \sum_{t=1}^n (\beta_{n_t} - \delta_{n_t}) \frac{\tilde{\gamma}_{\text{th}}}{\tilde{\lambda}}$, and $E(p; \alpha_r : q; \varphi_s : x)$ is the MacRobert function. Finally, we can obtain $\Upsilon_3, \Upsilon_4, \Upsilon_5, \Upsilon_6$ as shown in the theorem.

REFERENCES

[1] O. Kodheli et al., “Satellite communications in the new space era: A survey and future challenges,” *IEEE Commun. Surv. Tut.*, vol. 23, no. 1, pp. 70–109, Jan.–Mar. 2021.

[2] T. Van Chien, E. Lagunas, T. M. Hoang, S. Chatzinotas, B. Ottersten, and L. Hanzo, “Space-terrestrial cooperation over spatially correlated channels relying on imperfect channel estimates: Uplink performance analysis and optimization,” *IEEE Trans. Commun.*, vol. 71, no. 2, pp. 773–791, Feb. 2023.

[3] M. M. Azari et al., “Evolution of non-terrestrial networks from 5G to 6G: A survey,” *IEEE Commun. Surv. Tut.*, vol. 24, no. 4, pp. 2633–2672, Oct.–Dec. 2022.

[4] G. Geraci, D. Lopez-Perez, M. Benzaghta, and S. Chatzinotas, “Integrating terrestrial and non-terrestrial networks: 3D opportunities and challenges,” *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 42–48, Apr. 2023.

[5] 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 Trans. Commun.*, vol. 70, no. 10, pp. 6918–6937, Oct. 2022.

[6] 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 Syst. J.*, vol. 17, no. 2, pp. 2824–2835, Jun. 2023.

[7] 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, Mar. 2019.

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

[9] B. Evans et al., “Integration of satellite and terrestrial systems in future multimedia communications,” *IEEE Wireless Commun.*, vol. 12, no. 5, pp. 72–80, Oct. 2005.

[10] K. An, M. Lin, and T. Liang, “On the performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling,” *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1722–1725, Oct. 2015.

[11] X. Yan, H. Xiao, K. An, G. Zheng, and W. Tao, “Hybrid satellite terrestrial relay networks with cooperative non-orthogonal multiple access,” *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 978–981, May 2018.

[12] K. An, Y. Li, X. Yan, and T. Liang, “On the performance of cache-enabled hybrid satellite-terrestrial relay networks,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1506–1509, Oct. 2019.

[13] K. An and T. Liang, “Hybrid satellite-terrestrial relay networks with adaptive transmission,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12448–12452, Dec. 2019.

[14] Z. Zhao, G. Xu, N. Zhang, and Q. Zhang, “Performance analysis of the hybrid satellite-terrestrial relay network with opportunistic scheduling over generalized fading channels,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2914–2924, Mar. 2022.

[15] Z. Lin et al., “Refracting RIS-aided hybrid satellite-terrestrial relay networks: Joint beamforming design and optimization,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 4, pp. 3717–3724, Aug. 2022.

[16] N. Van Huynh, N. Q. Hieu, N. H. Chu, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, “Defeating eavesdroppers with ambient backscatter communications,” in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2023, pp. 1–6.

[17] T. N. Nguyen et al., “Physical layer security in AF-based cooperative SWIPT sensor networks,” *IEEE Sensors J.*, vol. 23, no. 1, pp. 689–705, Jan. 2023.

[18] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018.

[19] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, “On secure wireless communications for IoT under eavesdropper collusion,” *IEEE Trans. Automat. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[20] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[21] S. Liu, X. Zhu, H. Chen, and Z. Han, “Secure communication for integrated satellite-terrestrial backhaul networks: Focus on up-link secrecy capacity based on artificial noise,” *IEEE Wireless Commun. Lett.*, vol. 12, no. 8, pp. 1369–1373, Aug. 2023.

[22] J. Wang, Y. Xiao, T. Li, and C. P. Chen, “A jamming aware artificial potential field method to counter GPS jamming for unmanned surface ship path planning,” *IEEE Syst. J.*, vol. 17, no. 3, pp. 4555–4566, Sep. 2023.

[23] F. Fourati and M.-S. Alouini, “Artificial intelligence for satellite communication: A review,” *Intell. Converged Netw.*, vol. 2, no. 3, pp. 213–243, 2021.

[24] M. Bouabdellah and F. El 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, Dec. 2021.

[25] Z. Yin, N. Cheng, T. H. Luan, Y. Hui, and W. Wang, “Green interference based symbiotic security in integrated satellite-terrestrial communications,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9962–9973, Nov. 2022.

[26] X. Li et al., “Secure spectrum-energy efficiency tradeoff based on Stackelberg game in a two-way relay cognitive satellite terrestrial network,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 8, pp. 1679–1683, Aug. 2022.

[27] T. N. Nguyen et al., “Security-reliability trade-offs for satellite-terrestrial relay networks with a friendly jammer and imperfect CSI,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 5, pp. 7004–7019, Oct. 2023.

[28] X. Li et al., “Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments,” *IEEE Access*, vol. 7, pp. 102644–102661, 2019.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. San Diego: Academic Press, 2014.

[30] 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, Feb. 2016.

[31] V. Bankey and P. K. Upadhyay, “Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes,” in *Proc. IEEE 85th Veh. Technol. Conf.*, 2017, pp. 1–5.

[32] B. Elbert, *The Satellite Communication Ground Segment and Earth Station Handbook* (Artech House Space Technology and Applications Series), 2nd ed. Norwood, MA, USA: Artech House Publishers, 2014.

[33] 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, 2018.

[34] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[35] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, “Secrecy performance analysis with relay selection methods under impact of co-channel interference,” *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, 2015.

[36] D.-H. Ha, T. N. Nguyen, M. H. 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. 187165–187181, 2020.

[37] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products - Seventh Edition*. New York, NY, USA: Elsevier, 2007.

[38] K. An et al., “Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference,” *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4390–4404, Nov. 2015.

Tan N. Nguyen (Member, IEEE) was born at Nha Trang City, Vietnam, in 1986. He received the B.S. and M.S. degrees in electronics and telecommunications engineering from Ho Chi Minh University of Natural Sciences, a member of Vietnam National University, Ho Chi Minh City, Vietnam, in 2008 and 2012, respectively. He received the Ph.D. degree in computer science, communication technology and applied mathematics from VSB Technical University of Ostrava, Czech Republic, in 2019. He is currently working toward the Ph.D. degree in electrical engineering with VSB Technical University of Ostrava, Czech Republic.

In 2013, he joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam and have been working as Lecturer since then. His major interests are cooperative communications, cognitive radio, and physical layer security.

Trinh Van Chien (Member, IEEE) received the B.S. degree in electronics and telecommunications from Hanoi University of Science and Technology (HUST), Hanoi, Vietnam, in 2012, the M.S. degree in electrical and computer enginneering from Sungkyunkwan University, Seoul, South Korea, in 2014, and the Ph.D. degree in communication systems from Linköping University, Linköping, Sweden, in 2020.

He was a Research Associate with University of Luxembourg. He is currently with the School of Information and Communication Technology (SoICT), HUST, Vietnam. His interest lies in convex optimization problems and machine learning applications for wireless communications and image & video processing.

Dr. Chien was an IEEE Wireless Communications Letters exemplary reviewer for 2016, 2017 and 2021. He was a recipient of the award of scientific excellence in the first year of the 5G wireless project funded by European Union Horizon’s 2020.

Dinh-Hieu Tran was born and grew up in Gia Lai, Vietnam, 1989. He received the B.E. degree from Electronics and Telecommunication Engineering Department, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 2012, the M.Sc degree in electronics and computer engineering from Hongik University, Seoul, South Korea, in 2017, and the Ph.D. degree in telecommunications engineering from the Interdiscipline Reliability and Trust (SnT) research center, the University of Luxembourg, Esch-sur-Alzette, Luxembourg, in December 2021, under the supervision of Prof. Symeon Chatzinotas and Prof. Björn Ottersten.

His major interests include UAV, satellite, IoT, mobile edge computing, caching, B5G for wireless communication networks.

Dr. Tranwas a recipient of the Hongik Rector Award for his excellence during his master’s study at Hongik University, in 2016. He was a co-recipient of the IS3C 2016 best paper award. In 2021, he was nominated for the Best Ph.D. Thesis Award at the University of Luxembourg.

Bui Vu Minh was born on March 02, 1991, in Dong Nai, Vietnam. He received the graduate degree in electrical and electronic engineering from Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam, in 2015, and the master’s degree in electrical engineering from Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam, in 2019

End of 2014, he joined the Faculty of Engineering and Technology, Nguyen Tat Thanh University as Laboratory-Practice management, until in 2017 he was a Lecturer. His major research interests are wireless networks, robot, artificial neural networks, and power electronics.

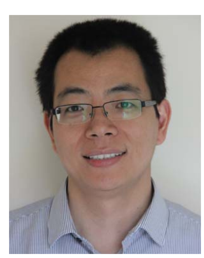
Nguyen Chi Ngon received the bachelor’s and master’s degrees in electronic engineering from Can Tho University, Can Tho, Vietnam, and the Vietnam National University, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 1996 and 2001, respectively.

Since 1996, he has worked with the Can Tho University. Currently, he is an Associate Professor in automation with the Department of Automation Technology, and a Vice Chairman of Can Tho University Board of Trustee. He is also a National-Distinguished Lecturer and a Secretary of the national council for professorships in Electrical-Electronics and Automation. His research interests are AI applications, intelligent control, medical control, pattern recognition, classifications, computer vision and agricultural automation.

Prof. Ngon was a recipient of Ph.D. award by the University of Rostock, Germany, in 2007.

Miroslav Voznak (Senior Member, IEEE) was born in 1971. He received the Ph.D. degree in telecommunications from the VSB, Technical University of Ostrava, Ostrava, Czech Republic, in 2002.

He is currently a Professor of electronics and communication technologies with the Department of Telecommunications, VSB, Technical University of Ostrava, and a Foreign Professor with Ton Duc Thang University, Ho Chi Minh City, Vietnam. He is a coauthor of more than one hundred articles in journals indexed in the SCIE database. His research interests include IP telephony, wireless networks, network security, and Big Data analytics.



Zhiguo Ding (Fellow, IEEE) received the B.Eng. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2000, and the Ph.D. degree from Imperial College London, London, U.K., in 2005.

He is currently a Professor in communications with Khalifa University, and has also been affiliated with the University of Manchester and Princeton University. His research interests are 6G networks, multiple access, energy harvesting networks and statistical signal processing.

Dr. Ding was an Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and was an Editor for IEEE WIRELESS COMMUNICATION LETTERS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATION LETTERS from 2013 to 2016. He recently received the EU Marie Curie Fellowship 2012–2014, the Top IEEE TVT Editor 2017, IEEE Heinrich Hertz Award 2018, IEEE Jack Neubauer Memorial Award 2018, IEEE Best Signal Processing Letter Award 2018, Friedrich Wilhelm Bessel Research Award 2020, and IEEE SPCC Technical Recognition Award 2021. He is a Fellow of the IEEE, a Distinguished Lecturer of IEEE ComSoc, and a Web of Science Highly Cited Researcher in two categories 2022.