Security and Reliability Analysis of Satellite-Terrestrial Multirelay Networks With Imperfect CSI

Tan Nhat Nguyen, Member, IEEE, Dinh-Hieu Tran, Member, IEEE, Trinh Van Chien, Member, IEEE, Van-Duc Phan, Miroslav Voznak, Senior Member, IEEE, and Symeon Chatzinotas, Senior Member, IEEE

Abstract—This article investigates the security and reliability analysis for a novel satellite-terrestrial network. Specifically, a satellite attempts to transmit confidential information to a ground user 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 are deployed to examine a general system model. In this context, the closed-form expressions for the outage probability and intercept probability are derived corresponding to an amplify-and-forward 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 channel state information (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], [2], [3]. Nevertheless, the explosive growth of the number of IoT devices (IoTDs) has brought new challenges to the traditional cellular networks due to its restricted resources, e.g., fixed locations, limited spectrum, and power [4], [5], [6]. Furthermore, IoT devices 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 satellites are being launched to provide global coverage and high throughput supporting the traditional terrestrial communication networks [8], [9], [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], [14], [15], [16], [17], [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], the authors in [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], [17], [18], [19], and [20].

Beyond the indepth analysis of satellite-terrestrial (SatTer) 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 protocols...
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], [24], [25], [26], [27]. The authors in [21] studied the PLS in HSTRN in which a multiantenna satellite tried to communicate with multiantenna relays in the presence of an eavesdropper. Nonorthogonal multiple access (NOMA) and HI were investigated with HSTRN in [23]. Moreover, the authors in [23] studied two security schemes, i.e., 1) colluding; and 2) noncolluding 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, 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 or backscatter-aided terrestrial communications, the authors in [26], [27], and [28] derived the closed-form expression of the secrecy channel capacity, outage probability (OP), and intercept probability (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], [30], [31], [32], [33]. The work in [29] studied the secrecy problem in multibeam 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 SatTer networks with jamming, where dual-hop communications were considered under radio frequency (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 enabled PLS in SatTer 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], [17], [18], [19], [20], [29], [30]. In contrast, there are only a few works on deriving the analytical results for SatTer 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 SatTer networks. In this article, we present an amplify-and-forward (AF)-based SatTer network for secure communication in the presence of an eavesdropper. The main contributions of this work are given as follows.

1) 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.

2) Monte Carlo simulations are performed to verify the correctness of mathematical analyses for various parameter settings. Moreover, the simulations also provide the tradeoff between security and reliability in the considered system model.

3) Insightful discussions on the impact of different key parameters of SatTer networks on its security-reliability tradeoff 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 rest of this article 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. Finally, Section V concludes the article.

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 $n \in \{1, \ldots, N\}$. 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], [37], [38]. To reduce the eavesdropping ability of the illegitimate party, we deploy one friendly jammer J that broadcasts the artificial noise. Notably, the jamming noise is known to the legitimate destination and it can be canceled, while it is unknown to the eavesdropper [31], [41].

1) In this article, 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.

2) 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].
A. Channel Model

In practice, it is difficult to obtain perfect CSI due to channel estimation errors (CEEs). Consequently, channel estimation methods, such as linear minimum mean square error channel estimator [42] are necessary to obtain CSI. Therefore, the channel can be modeled as

\[ \widehat{h}_i = h_i + e_i \]  

(1)

where \( e_i \) with \( i \in \{SR_n, R_nD, R_nE, JE, JR_m, JD\} \) is the CEEs with \( e_i \sim CN(0, \mu^2) \) and \( \widehat{h}_i \) 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. \(^3\) As a result, the channel gains can be represented as \( \gamma_{SR,E} = |h_{SR,E}|^2, \gamma_{SR,D} = |h_{SR,D}|^2 \), etc. are exponential random variables. More specifically, the probability density function (PDF) and cumulative distribution function (CDF) are given, respectively, as [45], [46]

\[ F_X(x) = 1 - \exp(-\lambda x), \]

(2)

\[ f_X(x) = \frac{\partial F_X(x)}{\partial x} = \lambda \exp(-\lambda x) \]

(3)

where \( \lambda \) is the rate parameter of \( X \). Next, we consider a 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 \( \gamma_{SR,n} = |h_{SR,n}|^2 \) between \( S \rightarrow R_n \) is given by [21], [34]

\[ f_{\gamma_{SR,n}}(x) = \alpha_n \exp(-\beta_n x) F_1(m_n; 1; \delta_n x), x \geq 0 \]

(4)

where \( \alpha_n \triangleq \frac{\beta_n}{2 \sigma_n m_n + \Omega_n} \), \( \beta_n \triangleq \frac{\lambda_n}{2 \sigma_n m_n + \Omega_n} \), \( \delta_n \triangleq \frac{\beta_n}{2 \sigma_n m_n + \Omega_n} \), with \( \Omega_n \) and \( 2 \sigma_n \) denote the average power of LOS and multipath components at relay \( R_n \), respectively. Moreover, \( \Omega_n \) implies the fading severity parameter at relay \( R_n \) and \( F_1(\cdot ; \cdot ; \cdot) \) denotes the confluent hypergeometric function of the first kind [48, eq. 9.210.1]. For arbitrary integer-valued fading severity parameters, one can simplify \( F_1(m_n; 1; \delta_n x) \) in (3) to express the PDF of \( \gamma_{SR,n} \) as [49]

\[ f_{\gamma_{SR,n}}(x) = \alpha_n \sum_{k=0}^{m_n-1} \zeta(k)x^k \exp(-\beta_n - \delta_n) x \]

(5)

where the following definition holds

\[ \zeta(k) = \frac{(-1)^k (1 - m_n)k! \delta_n^k}{k!} \]

(6)

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

\[ F_{\gamma_{SR,n}}(x) = \text{Pr} (\gamma_{SR,n} < x) = \int_0^x f_{\gamma_{SR,n}}(x) dx \]

(7)

which can be obtained in closed form as follows:

\[ F_{\gamma_{SR,n}}(x) = 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^{k} \frac{\zeta(k)p!}{k!} \theta_1^{A^1 x^p} \exp(-\theta_1 x) \]

\[ = 1 - \alpha_n \sum_{k=0}^{m_n-1} \sum_{p=0}^{k} \frac{(-1)^p (1 - m_n)k! \delta_n^k}{k!} \theta_1^{A^1 x^p} \exp(-\theta_1 x) \]

(8)

where \( A_1 \triangleq k + 1 - p, \theta_1 \triangleq \beta_n - \delta_n \). 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 \( \zeta(k) \) 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 section, we describe the AF relaying protocol that is used to forward the data from \( S \rightarrow R_n \). Because all GUs work in the half-duplex mode, the signal transmission from \( S \rightarrow D \) through two-time phases [50], [51]. In the first one, \( S \) transmits its data \( x_S \) to the relay \( R_n \). Therefore, the received signal at \( R_n \) can be expressed as

\[ y_{SR,n} = h_{SR,n}x_S + n_{SR,n} = (h_{SR,n} + e_{SR,n})x_S + n_{SR,n} \]

(9)

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

In the second phase, relay \( R_n \) first amplifies received signal \( y_{SR,n} \) with scale parameter \( G \), and then, relays it to the destination \( D \). At the same time, the eavesdropper can detect the transmitted signal from \( R_n \) 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 (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 the signal from \( S \) due to the masking effect or severe fading. Therefore, the eavesdropper monitors only the transmitted signal from relay \( R_n \) [21], [52]. Consequently, the received signal at the destination \( D \) and the eavesdropper \( E \) are given, respectively, as

\[ y_D = (h_{SR,D} + e_{SR,D}) G y_{SR,n} + n_D \]

\[ = (h_{SR,D} + e_{SR,D}) G (h_{SR,n} + e_{SR,n}) x_S + n_{SR,n} + n_D \]

(10)

\[ y_E = (h_{SR,E} + e_{SR,E}) G (h_{SR,n} + e_{SR,n}) x_S + n_{SR,n} \]

\[ + (h_{JE} + e_{JE}) x_J + n_E \]

(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

\[^3\]Channel model considered in this article 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.
Let us denote the second term of the product in (17) as 
\[ x_n = \sum_{k=0}^{m_n-1} \frac{\sum_{p=0}^{k} \alpha_n (-1)^p (1-m_n)}{k! p!} \delta_{\gamma_n}^3 \exp (-\vartheta_1 x) \] 
then we obtain the following result:

\[
F_{\gamma_{SR_n}}(x) = \prod_{n=1}^{N} (1-e^{-x_n}) 
= 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{p=1}^{N} \sum_{t=1}^{n} \prod_{n_1 \neq n_2 \neq \cdots \neq n_t} x_{n_t}. \quad (18)
\]

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

\[
\prod_{n=1}^{N} x_{n_t} = \sum_{k_t=0}^{n_t} \sum_{p_t=0}^{k_t} \cdots \sum_{p_{n_t}=0}^{k_{n_t}-1} \prod_{k=1}^{n_t} \alpha_n \times \frac{(-1)^{k_t} (1-m_{n_t})^t}{k_t! p_t! \vartheta_3^{A_t}} \times A_{2} \exp \left( -\sum_{t=1}^{n_t} \vartheta_3 x \right). \quad (19)
\]

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

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

\[
F_{\gamma_{SR_n}}(x) = 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{\sum_{t=1}^{n_t} A_t = A} \times (-1)^{k_t} (1-m_{n_t})^t \frac{k_t! p_t! \vartheta_3^{A_t}} {k_t! p_t! \vartheta_3^{A_t}} \times A_{2} \exp \left( -\sum_{t=1}^{n_t} \vartheta_3 x \right). \quad (20)
\]

where the summation notation \( \sum^* \) is defined as

\[
\sum^* = \sum_{n_t=1}^{N} \cdots \sum_{n_1=1}^{N} \sum_{k=1}^{m_{n_t}-1} \sum_{p=0}^{k} \sum_{t=1}^{n} \prod_{n_1 \neq n_2 \neq \cdots \neq n_t}. \quad (21)
\]

The preliminary result on the CDF of \( \gamma_{SR_n} \) 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. OP Analysis

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

\[
OP = Pr \left( \gamma_D < \gamma_{th} \right) \quad (22)
\]
where $\gamma_{th} = 2^{C_{th}} - 1$, $C_{th}$ 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

$$
\text{OP} = 1 + \sum_{n=1}^{N} \left( \frac{(-1)^n}{n!} \sum_{t=1}^{n} \frac{2(-1)^t (1 - m_{n_t}) \lambda_{n_t} k_{t} \Psi_{RD}}{k_t p_t t_3^{3 t}} \right) \left( \frac{\gamma_{th}}{\Psi} \right)^{A_2} \exp \left( - \sum_{t=1}^{n} \vartheta_{3} (\gamma_{th} - \lambda_{RD} \gamma_{th}) \right) \right) \times K_{-q+1} \left( 2 \sum_{t=1}^{n} \frac{\vartheta_{3} \lambda_{RD} \Psi_{RD}}{\lambda_{RD} \Psi} \right) (23)
$$

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, e.g., 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. 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] and [54] as follows:

$$
\text{IP} = \Pr \left( \gamma_{E} \geq \gamma_{th} \right) = 1 - \Pr \left( \gamma_{E} < \gamma_{th} \right). (24)
$$

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

$$
\text{IP} = 1 - \Pr \left( \frac{\Psi \vartheta_{SR_{E}} \gamma_{SR_{E}}}{A_{E}} < \gamma_{th} \right)
= 1 - \int_{0}^{\infty} Q \times f_{\gamma_{SR_{E}}}(x) dx
$$

where $Q \triangleq \Pr \left( \frac{\Psi \vartheta_{SR_{E}} \gamma_{SR_{E}}}{A_{E}} < \gamma_{th} \right)$, $A_{E} \triangleq \gamma_{SR_{E}} \Psi_{SR_{E}} \Psi_{th} + \gamma_{JE} \Psi_{th} + \Lambda$, and $\vartheta_{6} \triangleq \frac{\mu_{RE}^2 \Psi_{th} + \Theta \mu_{JE}^2 + \Theta \gamma_{JE} + 1}{\Psi_{E}}$. From (25), $Q$ can be calculated as

$$
Q = \Pr \left( \frac{\Psi \vartheta_{SR_{E}} \gamma_{SR_{E}}}{A_{E}} < \gamma_{th} (\Lambda_{7} + \Lambda_{8}) \right)
= \Pr \left( \frac{\Psi \vartheta_{SR_{E}} \gamma_{SR_{E}}}{\lambda_{E} \Psi} < \gamma_{th} \Lambda_{7} \right)
= \left\{ \begin{array}{ll}
\Pr \left( \vartheta_{SR_{E}} < \frac{\gamma_{th} \Lambda_{7}}{A_{E}} \right), & \text{if } \gamma_{SR_{E}} > \frac{\gamma_{th} \Psi_{E}}{\Psi_{SR_{E}}} \\
1, & \text{if } \gamma_{SR_{E}} \leq \frac{\gamma_{th} \Psi_{E}}{\Psi_{SR_{E}}}
\end{array} \right.
$$

\[ \]
Lemma 2: With using the same approach as (23), the closed-formed expression of $Q$ can be expressed as

$$Q = 1 + 2\sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{k=1}^{\infty} \frac{(-k)^{n-1} (1-m_{n1})_{k1} (\delta_{n1})_{k1} \lambda_{RE}}{k1_p1 \lambda_{RE}}$$

$$\times \exp \left(-\sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} - \lambda_{RE} \Delta_{(x)} \right)$$

$$\times \left(\frac{\bar{A}}{\Psi} \sum_{q=0}^{\infty} \frac{A_k}{q!} \vartheta_2^{A_k-q} \vartheta_1^{q+1} \sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} - \lambda_{RE} \Delta_{(x)} \right)$$

$$\times K_{-q+1} \left(2 \sqrt{\sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} \lambda_{RE} \vartheta_{RE} \vartheta_{6}} \right).$$

(30)

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

$$IP = \sum_{n=1}^{N} \frac{(-1)^{n+1}}{n!} \left(\sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} - \lambda_{RE} \Delta_{(x)} \right)$$

$$\times \sum_{k=1}^{\infty} \frac{(-k)^{n-1} (1-m_{n1})_{k1} (\delta_{n1})_{k1} \lambda_{RE} \lambda_{JE}}{k1_p1 \lambda_{RE}}$$

$$\times \exp \left(\Lambda_{10} - \lambda_{RE} \Lambda_{11} \sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} - \lambda_{RE} \Delta_{(x)} \right)$$

$$\times \left(\frac{\bar{A}}{\Psi} \sum_{q=0}^{\infty} \frac{A_k}{q!} \vartheta_2^{A_k-q} \vartheta_1^{q+1} \sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} - \lambda_{RE} \Delta_{(x)} \right)$$

$$\times G_{3,0}^{1,3} \left(\frac{q_{2}}{4}, -1, w+1, q_{w} \right)$$

(31)

where $\zeta = 2 \sqrt{\sum_{t=1}^{n} \frac{q_{t}}{2} \frac{\vartheta_2}{\vartheta_1} \lambda_{RE} \vartheta_{RE} \vartheta_{6}}$, and $C_{m,n}^{p,q} \left( z \bigg| \frac{a_1, \ldots, a_p}{b_1, \ldots, b_q} \right)$ is the Meijer G-function.

Proof: See Appendix B.

Remark 2: This article 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 SatTer multirelay 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 multifloor 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, $(m,b)$ = $(10.0635,0.0007)$ for heavy shadowing (HS) case and $(5.025,0.279)$ 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-Φ = 5 dB-Ψ = 20 dB-N = 3, and imperfect CSI-Φ = 10 dB-Ψ = 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 OP and IP with HS, 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 heavy 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 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 heavy shadowing (HS) are 0.9783, 0.6742, and 0.2305 corresponding to $\Psi$ values equals 5, 10, and 15 dB, respectively. That is because a better SNR can be obtained at the eavesdropper with higher values of $\Psi$, as shown in (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 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 perfect CSI outperforms imperfect ones.\(^5\)

\(^5\)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 SatTer 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.

In Figs. 6 and 7, we show the influences of CEEs to the outage and intercept performance with heavy and average showing 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 than the higher of CEEs values. For instance, the gap between these schemes are 0.0423, 0.1475, 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 (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 tradeoff 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

This article has studied the physical layer security in terms of security and reliability tradeoff of a satellite AF multirelay 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-formed 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:

\[
\text{OP} = \Pr \left( \frac{\Psi \gamma_{SRa} \gamma_{RD}}{\gamma_{RD} \Psi \vartheta_2 + \gamma_{SRa} \Psi \vartheta_4 + \Xi} < \gamma_{th} \right)
\]

\[
= \Pr \left( \frac{\gamma_{SRa} \Lambda_3}{\Lambda_5} < \gamma_{th} \left( \frac{\gamma_{RD} \Psi \vartheta_2 + \Xi}{\gamma_{SRa} \Psi \vartheta_4 + \Xi} \right) \right)
\]

\[
= \frac{1}{n!} \int_{\gamma_{th}}^{\gamma_{SRa}} f_{\gamma_{SRa}}(x) \, dx + \int_{\gamma_{th}}^{+\infty} F_{\gamma_{SRa}} \left( \frac{\Lambda_3}{\Lambda_5} \right) f_{\gamma_{SRa}}(x) \, dx
\]

(32)

where

\[
\tilde{\gamma}_{th} \triangleq \gamma_{th} (\mu_{RD}^2 \Phi + 1), \quad \vartheta_2 \triangleq (\mu_{RD}^2 \Phi + 1), \quad \Lambda_2 \triangleq [\gamma_{SRa} \Phi \vartheta_4 + \Xi], \quad \Lambda_3 \triangleq [\Phi \Lambda_{RD} - \gamma_{th} \vartheta_2], \quad \Lambda_4 \triangleq [x \Phi \vartheta_2 + \Xi], \quad \text{and} \quad \Lambda_5 \triangleq \Psi [\Phi x - \gamma_{th} \vartheta_4].
\]

By substituting (20) into (32), the OP can be mathematically represented by

\[
\text{OP} = 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{k=0}^{n} \alpha_{n_k} \frac{(-1)^{k_1} (1 - m_{n_k}) k_1 (\delta_{n_k})^{k_1} \lambda_{RD}}{k_1 ! p_1 ! \vartheta_2^{k_1} \Lambda_3}
\]

\[
\times \int_{\gamma_{th}}^{+\infty} \left( \frac{x \vartheta_2 + \Xi}{\Psi [x - \gamma_{th}]} \right)^{m_{n_k}} \sum_{t=1}^{n} p_t \, dx
\]

\[
\times \exp \left( - \sum_{t=1}^{n} \vartheta_3 \left( \frac{\gamma_{th} [x \vartheta_2 + \Xi]}{\Psi [x - \gamma_{th}]} \right) - \lambda_{RD} x \right) \, dx.
\]

(33)

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

\[
\text{OP} = 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{k=0}^{n} \alpha_{n_k} \frac{(-1)^{k_1} (1 - m_{n_k}) k_1 (\delta_{n_k})^{k_1} \lambda_{RD}}{k_1 ! p_1 ! \vartheta_2^{k_1} \Lambda_3}
\]

\[
\times \int_0^{+\infty} \left( \frac{\gamma_{th} (y + \tilde{\gamma}_{th})}{\Psi y} \right)^{m_{n_k}} \sum_{t=1}^{n} p_t \, dy
\]

\[
\times \exp \left( - \sum_{t=1}^{n} \vartheta_3 \left( \frac{\gamma_{th} (y + \tilde{\gamma}_{th})}{\Psi y} \right) - \lambda_{RD} y \right) \, dy.
\]

(34)

where

\[
\tilde{\Xi} = [\gamma_{th} (\mu_{SR}^2 \Psi + 1) + \frac{\psi}{\Psi}].
\]

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

\[
\text{OP} = 1 + \sum_{n=1}^{N} \frac{(-1)^n}{n!} \sum_{k=0}^{n} \alpha_{n_k} \frac{(-1)^{k_1} (1 - m_{n_k}) k_1 (\delta_{n_k})^{k_1} \lambda_{RD}}{k_1 ! p_1 ! \vartheta_2^{k_1} \Lambda_3}
\]

\[
\times \left( \frac{\gamma_{th}}{\Psi} \right)^2 \exp \left( - \sum_{t=1}^{n} \vartheta_3 \left( \frac{\gamma_{th} \vartheta_2}{\Psi} - \lambda_{RD} \gamma_{th} \right) \right)
\]

\[
\times \int_0^{+\infty} \left( \vartheta_2 + \frac{\psi}{\Psi} \right)^{n} \sum_{t=1}^{n} p_t \, dy
\]

\[
\times \exp \left( - \sum_{t=1}^{n} \vartheta_3 \left( \frac{\gamma_{th} \vartheta_2}{\Psi} - \lambda_{RD} y \right) \right) \, dy.
\]

(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

\[
\text{IP} = 2 \sum_{n=1}^{N} \frac{(-1)^{n+1}}{n!} \sum_{k=0}^{n} \alpha_{n_k} \frac{(-1)^{k_1} (1 - m_{n_k}) k_1 (\delta_{n_k})^{k_1} \lambda_{RE} \Lambda_{JE}}{k_1 ! p_1 ! \vartheta_2^{k_1} \Lambda_3}
\]

\[
\times \left( \sum_{t=1}^{n} \vartheta_3 \gamma_{th} \right)^{q+1} \exp \left( - \sum_{t=1}^{n} \vartheta_3 \gamma_{th} \vartheta_2 \right) \Psi \lambda_{RE}.
\]
By substituting (39) and (40) into (36), it yields

\[
\Delta(x) \vartheta_2 + \Omega(x) = \tilde{\gamma}_t \vartheta_2 + \frac{\gamma_t \Theta x}{\Phi} \vartheta_2 + \frac{x \vartheta_2 + \Lambda}{\Phi}
\]

(37)

\[
\exp(-\lambda_{JE} x - \lambda_{RE} \Delta(x))
\]

\[
= \exp(-\lambda_{JE} x - \lambda_{RE} \tilde{\gamma}_t) - \gamma_t \lambda_{RE} \Theta x}{\Phi}
\]

\[
= \exp(-\lambda_{RE} \tilde{\gamma}_t) \exp\left(-x \left[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\Phi}\right]\right)
\]

(38)

Next, by denoting \(t \triangleq \frac{x(\vartheta_2 + 1)}{\Lambda} + 1\), (37) and (38) can be rewritten, respectively, as

\[
\Delta(x) \vartheta_2 + \Omega(x) = t \Lambda,
\]

(39)

\[
\exp(-\lambda_{JE} x - \lambda_{RE} \Delta(x))
\]

\[
= \exp\left(\bar{\Lambda} \left[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\Phi}\right] \frac{\Lambda}{\vartheta_2 \gamma_t}\right)
\]

\[
\times \exp\left(-\left[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\Phi}\right] \frac{t \Lambda}{\vartheta_2 \gamma_t}\right)
\]

(40)

where \(\bar{\Lambda} \triangleq \tilde{\gamma}_t \bar{\vartheta}_2 + \frac{\Lambda}{\vartheta_2} \bar{\vartheta}_2 \triangleq \frac{\bar{\gamma}_t}{\vartheta_2} + 1\). By substituting (39) and (40) into (36), it yields

\[
\text{IP} = 2 \sum_{n=1}^{N} (-1)^{n+1} \left(\frac{\sum_{t=1}^{n} \vartheta_3 \gamma_{th}}{\vartheta_2 \gamma_t \vartheta_2 \gamma_t}\right) \frac{n+1}{n!}
\]

\[
\times \sum_{\alpha_n} (-1)^{k_1} (1 - m_n) \vartheta_3^n \right(l_{n_1})^{k_1} \lambda_{RE} \lambda_{JE}
\]

\[
\times \exp\left(A_{10} \bar{\Lambda} - \lambda_{RE} \tilde{\gamma}_t - \sum_{t=1}^{n} \vartheta_3 \gamma_{th} \bar{\vartheta}_2\right)
\]

\[
\times \left(\frac{\gamma_t}{\Psi}\right) A_2 \sum_{q=0}^{\vartheta_3 \gamma_{th}} \left(\frac{A}{\vartheta_2 \gamma_t}\right) \frac{\vartheta_3 \gamma_{th} \lambda_{RE} t \Lambda}{\vartheta_2 \gamma_t}
\]

\[
\times \int_{1}^{t} (t) \frac{t+1}{t} \exp\left(-A_{10} t \bar{\Lambda}\right)
\]

\[
\times K_{q+1} \left(2 \sqrt{\frac{\sum_{t=1}^{n} \vartheta_3 \gamma_{th} \lambda_{RE} t \Lambda}{\vartheta_2 \gamma_t}}\right) dt
\]

(41)

where \(A_{10} \triangleq \frac{[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\vartheta_2 \gamma_t}] t \Lambda}{\vartheta_2 \gamma_t} + \lambda_{RE} \Delta(x)\). Next, we apply the Maclaurin series as follows:

\[
\exp\left(-\left[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\vartheta_2 \gamma_t}\right] \frac{t \Lambda}{\vartheta_2 \gamma_t}\right)
\]

\[
= \sum_{w=0}^{\infty} (-1)^w \left(\frac{[\lambda_{JE} + \frac{\gamma_t \lambda_{RE} \Theta}{\vartheta_2 \gamma_t}] t \Lambda}{\vartheta_2 \gamma_t}\right)^w
\]

(42)

By substituting (42) into (41), the IP can be recalculated as

\[
\text{IP} = 2 \sum_{n=1}^{N} (-1)^{n+1} \left(\frac{\sum_{t=1}^{n} \vartheta_3 \gamma_{th}}{\vartheta_2 \gamma_t \vartheta_2 \gamma_t}\right) \frac{n+1}{n!}
\]

\[
\times \sum_{\alpha_n} (-1)^{k_1} (1 - m_n) \vartheta_3^n \right(l_{n_1})^{k_1} \lambda_{RE} \lambda_{JE}
\]

\[
\times \exp\left(A_{10} \bar{\Lambda} - \lambda_{RE} \tilde{\gamma}_t - \sum_{t=1}^{n} \vartheta_3 \gamma_{th} \bar{\vartheta}_2\right)
\]

\[
\times \left(\frac{\gamma_t}{\Psi}\right) A_2 \sum_{q=0}^{\vartheta_3 \gamma_{th}} \left(\frac{A}{\vartheta_2 \gamma_t}\right) \frac{\vartheta_3 \gamma_{th} \lambda_{RE} t \Lambda}{\vartheta_2 \gamma_t}
\]

\[
\times \int_{1}^{\infty} (t) \frac{t+1}{t} \exp\left(-A_{10} t \bar{\Lambda}\right)
\]

\[
\times K_{q+1} \left(2 \sqrt{\frac{\sum_{t=1}^{n} \vartheta_3 \gamma_{th} \lambda_{RE} t \Lambda}{\vartheta_2 \gamma_t}}\right) dt
\]

(43)
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, Jan. 2015.

ETSII, “Digital Video Broadcasting (DVB); System Specifications for Satellite services to Handheld devices (SH) below 3 GHz,” Tech. Spec. ETSI TS 102 585 V1.1.1 (2007-07), ETSI, Sophia Antipolis Cedex, France, 2007.

T. N. Nguyen et al., “Outage performance of satellite terrestrial full-duplex relaying networks with co-channel interference,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1478–1482, Jul. 2022.

T. N. Nguyen et al., “Study on new radio (NR) to support non-terrestrial networks,” Tech. Rep., Spec. 38,811, 3GPP, Sophia Antipolis Cedex, France, May 2019.

X. Yue et al., “Outage behaviors of NOMA-based satellite network over shadowed-rician fading channels,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6818–6821, Jun. 2020.

Tan Nhat Nguyen (Member, IEEE) was born in 1986 in Nha Trang City, Vietnam. He received the B.S. degree in electronics from Ho Chi Minh University of Natural Sciences, Ho Chi Minh City, Vietnam, in 2008, the M.S. degree in telecommunications engineering from Vietnam National University, Hanoi, Vietnam, in 2012, and the Ph.D. degree in communications technologies from the Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, Ostrava, Czech Republic, in 2019.

He joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam, as a Lecturer in 2013. His research interests include cooperative communications, cognitive radio, and physical layer security.

Dinh-Hieu Tran (Member, IEEE) was born in 1989 in Vietnam, growing up in Gia Lai. He received the B.E. degree from the Department of Electronics and Telecommunication Engineering, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 2012, the M.S. degree (with honours) in electronics and computer engineering from Hongik University, Seoul, South Korea, in 2017, and the Ph.D. degree from the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg, under the supervision of Prof. Symeon Chatzinotas and Prof. Björn Ottersten.

Trinh Van Chien (Member, IEEE) received the B.S. degree in electronics and telecommunications from the Hanoi University of Science and Technology (HUST), Hanoi, Vietnam, in 2012, the M.S. degree in electrical and computer engineering 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 the University of Luxembourg, Esch-sur-Alzette, Luxembourg. He is currently with the School of Information and Communication Technology, HUST. His research interests include convex optimization problems, machine learning applications for wireless communications, and image and video processing.

Van-Duc Phan was born in 1975 in Long An province, Vietnam. He received the M.S. degree from the Department of Electric, Electrical and Telecommunications Engineering, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, and the Ph.D. degree from the Department of Mechanical and Automation Engineering, Da-Yeh University, Changhua, Taiwan.

His current research interests include sliding mode controls, nonlinear systems and active magnetic bearings, flywheel energy storage systems, power system optimization, optimization algorithms, renewable energies, energy harvesting 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 (Senior Member, IEEE) received the Ph.D. degree in telecommunications from the Faculty of Electrical Engineering and Computer Science, VSB – Technical University of Ostrava, Ostrava, Czech Republic, in 2002, and achieved habilitation in 2009.

He joined as a Full Professor in Electronics and Communications Technologies with the VSB–Technical University of Ostrava, in 2017. He is currently a Principal Investigator with the research project QUANTUMS funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks. He has authored or coauthored more than one hundred articles indexed in SCIE/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 and communication technologies. He has participated in six projects funded by the EU in programs managed directly by European Commission. His research interests include information and communication technology, especially quality of service and experience, network security, wireless networks, and big data analytics.

Dr. Voznak was a General Chair of the 11th IFIP Wireless and Mobile Networking Conference in 2018 and the 24th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications in 2020.

Symeon Chatzinotas (Senior Member, IEEE) was a Visiting Professor with the University of Parma, 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 is currently a Full Professor or Chief Scientist I in satellite communications, and Head of the SIGCOM Research Group with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg. He has authored or coauthored more than 450 technical papers in refereed international journals, conferences, and scientific books. He coordinates research activities in communications and networking, acting as a Principal Investigator in over 20 projects, and is the main representative for 3rd Generation Partnership Project (3GPP), European Telecommunications Standards Institute, and Digital Video Broadcasting.

Prof. Chatzinotas was a corecipient of the 2014 IEEE Distinguished Contributions to Satellite Communications Award and Best Paper Awards at European Association for Signal Processing *Journal on Wireless Communications and Networking*, International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), and International Communications Satellite Systems Conference. He is currently on the Editorial Board of *IEEE Transactions on Communications*, *IEEE Open Journal of Vehicular Technology*, and the *International Journal of Satellite Communications and Networking*. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.