EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

On the Security and Reliability Trade-off of the Satellite Terrestrial Networks with Fountain Codes and Friendly Jamming

Nguyen Quang Sang[1], Nguyen Van Hien[2,*], Tran Trung Duy[2], Nguyen Luong Nhat[2], Lam-Thanh Tu[3]

[1]Science and Technology Application for Sustainable Development Research Group, Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam; sang.nguyen@ut.edu.vn
[2]Posts and Telecommunications Institute of Technology, Vietnam; hiennv@ptit.edu.vn, duytt@ptit.edu.vn, nhatnl@ptit.edu.vn
[3]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam; tulamthanh@tdtu.edu.vn

Abstract

The performance of the satellite-terrestrial network with Fountain Codes (FCs) is conducted in the present work. More precisely, the air-to-ground link is modeled according to the shadow-Rician distribution to capture the strong line-of-sight (LOS) path as well as the impact of the shadowing. As a result, we employ the directional beamforming at both the satellite and relay to mitigate such an ultra-long transmission distance. We investigate the trade-off between the reliability and security aspects. Particularly, we derive the outage probability (OP) and intercept probability (IP) in the closed-form expressions. To further facilitate the security of the considered networks, the friendly jamming scheme is deployed as well. Finally, simulation results based on the Monte-Carlo method are given to corroborate the exactness of the developed mathematical framework and to identify key parameters such as antenna gain, and transmit power that have a big impact on the considered networks.

Received on 20 October 2023; accepted on 03 December 2023; published on 07 December 2023

Keywords: Fountain Codes, Intercept Probability, Outage Probability, Satellite-Terrestrial Communications

doi:10.4108/eetinis.v10i4.4192

1. Introduction

Satellite communications have been considered one of the key technologies for the sixth generation of cellular networks (6G) [1]. Particularly, by virtual a strong line-of-sight (LOS) link, the air-to-ground link rarely suffers from fading and/or shadowing. Additionally, another advantage of satellite communications is that it is able to cover a wide range of geography such as mountainous and ocean areas. As a result, satellite communications have gained lots of attention from both academia and industry. However, the main drawback of satellite-based services is that they require a high-cost hardware. It, as a consequence, is not suitable for low-cost devices such as end devices in long-range (LoRa) networks and/or sensors in remote areas. To fully exploit the benefits of the satellite-based services, the relaying technique is generally combined to form the satellite-terrestrial networks to serve low-cost terminals [2].

Fountain Codes (FCs), on the other hand, is one of the most effective codes to significantly ameliorate the performance of the wireless networks [3]. More precisely, the messages are divided into unlimited of encoded packets or Fountain packets. These packets seamlessly transmit to all users. On the receiver side, they only need to collect a sufficient number of encoded packets to decode the transmitted messages. It, thus, is very suitable for serving multicast and/or broadcast networks where re-transmission a huge

*Corresponding author: Nguyen Van Hien
Email: hiennv@ptit.edu.vn

number of packets will become the bottleneck of the whole networks [4]. As a result, in the present paper, we investigate the satellite-terrestrial communications employing FCs. More specifically, we study two aspects of such networks, reliability and security via two essential metrics namely, outage probability (OP) and intercept probability (IP). Before summarizing the core contributions and novelties of the considered networks. We shortly provide the state-of-the-art of the satellite-terrestrial networks as well as the FC-based communications in the sequel.

The performance of the satellite-terrestrial networks, relaying networks, and Fountain codes-based networks were broadly addressed in [5–19]. More precisely, Guo and other authors in [5] studied the performance of the two-way satellite-high altitude platform (HAP)-terrestrial networks with non-orthogonal multiple access (NOMA). They derived the outage probability and ergodic capacity of the considered networks. However, they do not take the FCs and friendly jamming into account. The work in [6] also investigated the satellite-terrestrial networks with NOMA networks. They, nevertheless, concentrated on the maximization of the achievable rate while we focused on the trade-off between reliability and security. The joint bandwidth and power allocation maximization problem in multi-user unmanned aerial vehicle (UAV)-aided two-way relaying networks were comprehensively solved in [7]. Nguyen and his colleagues in [8] addressed the reliability and security trade-off in satellite-terrestrial networks. Nonetheless, the FCs do not apply in their work. The performance of the integrated free space optical (FSO)/ radio frequency (RF) in satellite-terrestrial networks was conducted in [9]. On the other hand, the performance of the multi-hop with Fountain codes was given in [10] but the authors do not examine the satellite communications. The performance of the broadcast networks in cognitive radio networks (CRNs) with transmit and receive diversity techniques was examined in [11–13]. More precisely, they derived the cumulative distribution function (CDF), probability density function (PDF), and the average number of required time slots to broadcast a message to an arbitrary number of secondary receivers (SRs) in the closed-form expressions. Additionally, they also propose an effective power allocation to simultaneously satisfy the quality-of-service (QoS) of the primary networks (PNs) and the reliability of the secondary networks (SNs). Besides, the all-inclusive survey on the cooperative relaying networks applying to physical layer security (PLS) was given in [14]. The end-to-end (e2e) OP and IP of the integration of energy harvesting (EH) in multi-hop networks under three cooperative jamming schemes was studied in [15]. The trade-off of reliability and security in simultaneous wireless information and power transfer (SWIPT)-enabled in NOMA full-duplex relaying networks was performed in [16]. They found that increasing the transmit power of the source node will be beneficial for reliability. It, nonetheless, also scaled up the intercept probability. A special issue focused on PLS in satellite-based communications was published by Trung and others in [17]. The secrecy outage probability (SOP) and the secrecy capacity of the CRNs under Nakagami-m distribution were calculated in [18]. The closest work to the current manuscript was our previous work which was given in [19]. Nevertheless, we did not take the jamming techniques as well as directional beamforming into consideration. Furthermore, the previous work solely concentrated on reliability, the present work, on the other hand, studies both the security and reliability aspects. The summarized contributions and novelties of the present work are given below

- We consider the shadow-rician distribution of the satellite-terrestrial link to take into consideration of the strong LOS link as well as the impact of the shadowing. Moreover, the friendly jamming scheme is considered to improve the security aspect of the networks. Furthermore, the FCs are employed to further ameliorate the spectral efficiency (SE) of the networks.
- We also consider the directional beamforming at the satellite and relay to overcome the ultra-long transmission distance and to boost the reliability and security of the networks.
- We derive both the OP and IP in the closed-form expression. Additionally, we also compute the success probability in decoding a packet at both destination and eavesdropper.
- We corroborate the accuracy of the developed mathematical framework with computer-based simulation results based on the Monte-Carlo methods.
- We point out some key metrics that can either significantly facilitate the system performance or have a big impact on the two considered metrics.

The organization of the current paper is given as follows: The system model is provided in Section 2 while the OP and IP analyses are given in Secion 3. Section 4 supplies simulation results and the conclusion is conducted in Section 5.

2. System model

Let us consider a satellite-terrestrial system as shown in Fig. 1. Here, the satellite denotes by S and transmits information to the ground terminal denoted by D with the help of a relay R. Additionally, the considered

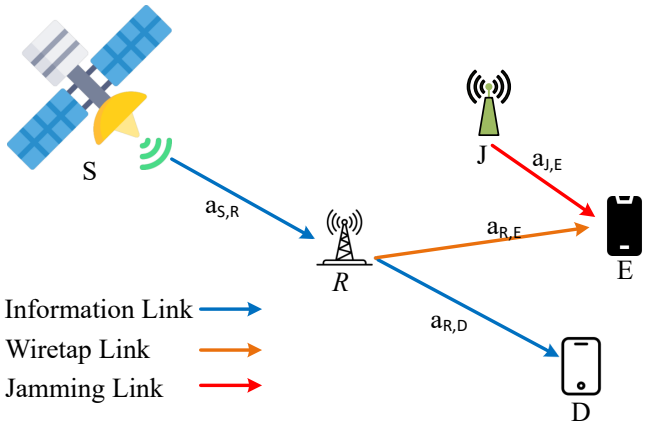

Figure 1. The considered satellite-terrestrial system model.

networks also comprises an active eavesdropper[1]. All nodes are equipped with a single antenna. The extension to multiple antennae is left for future work. To facilitate the security of the considered networks, a friendly jammer denoted by J is utilized which broadcasts artificial noises (ANs) toward the eavesdropper.

The whole transmission from the satellite to the destination is taken place in two phases. In the first phase, the satellite sends their signals to the relay. It is noted that both the destination and eavesdropper are not able to decode the satellite signals owing to low-cost device. At the end of the first phase, the relay decodes source information, it, then, re-encodes and forwards to the destination. Such signal processing is classified as decode-and-forward (DF) protocol.

2.1. Channel modeling

All transmission links are subjected to both small-scale fading and large-scale path-loss. However, the channel coefficient of the small-scale fading is different between air-to-ground channel and ground-to-ground channels. Particularly, the small-scale fading is defined as follows:

Air-to-ground modeling. The channel coefficient of the satellite-terrestrial link is modeled according to the shadow-Rician distribution. The probability density function of the channel gain from S to R denoted by $\left|a_{S,R}\right|^2$ is given below [23]

$$f_{\left|a_{S,R}\right|^2}(x) = \omega \sum_{v=0}^{m-1} \theta(v)\, x^v \exp\left(-(\vartheta-\rho)\, x\right), \quad (1)$$

where $\omega = \vartheta\left(\frac{2pm}{2pm+q}\right)^m$, $\rho = \frac{\vartheta q}{2pm+q}$, $\theta(v) = \frac{(-1)^v (1-m)_k \rho^k}{(v!)^2}$, and $\vartheta = \frac{1}{2p}$; p and q are the average power of the LOS and non-LOS (NLOS) components. $(x)_v = \prod_{k=0}^{v-1}(x-k)$ is the Pochhammer symbol [24, p. xliii] and $m \in \mathbb{N}$ is the fading severity of the $\left|a_{S,R}\right|^2$. The cumulative distribution function of the $\left|a_{S,R}\right|^2$ is computed as [25]

$$F_{\left|a_{S,R}\right|^2}(x) = 1 - \omega \sum_{v=0}^{m-1} \sum_{i=0}^{v} \frac{(-1)^v (1-m)_v \rho^v}{v!\, i!\, (\vartheta-\rho)^{(v+1-i)}} x^i \times \exp\left(-(\vartheta-\rho)\, x\right). \quad (2)$$

Ground-to-ground modeling. The small-scale fading of all transmission links between ground terminals are subjected to the Rayleigh fading. The channel gain denoted by $\left|a_{s,o}\right|^2$, $s \in \{R, J\}$, $o \in \{D, E\}$, as a consequence, follows by an exponential distribution with scale parameter $\Omega_{s,o}$. Mathematical speaking, the CDF, and PDF of the channel gain from node s to node o denoted by $F_{\left|a_{s,o}\right|^2}(x)$ and $f_{\left|a_{s,o}\right|^2}(x)$ are formulated as [26]

$$F_{\left|a_{s,o}\right|^2}(x) = 1 - \exp\left(-\frac{x}{\Omega_{s,o}}\right)$$
$$f_{\left|a_{s,o}\right|^2}(x) = \frac{1}{\Omega_{s,o}} \exp\left(-\frac{x}{\Omega_{s,o}}\right). \quad (3)$$

Here we assume that the channel coefficient remains stable for the whole transmission and varies independently between transmissions.

2.2. Large-scale path-loss

The large-scale path-loss from the transmitter to receiver denoted by O_{s^+,o^+} is formulated as follows [27]:

$$O_{s^+,o^+} = W_0 d^{\lambda}_{s^+,o^+}, \quad (4)$$

where $o^+ \in \{R, D, E\}$, $s^+ \in \{S, R, J\}$, $\lambda \in [2, 8]$ is the path-loss exponent, $W_0 = \left(\frac{4\pi d_0 f_c}{c}\right)^2$ is the path-loss constant at the reference distance d_0 and is computed according to the free space path-loss model [28], f_c (in Hz) is the carrier frequency, and $c = 3 \times 10^8$ (in meter per second) is the speed of light. Without loss of generality, d_0 is set to 1 meter, e.g., $d_0 = 1$ m.

2.3. Antenna gain modeling

In the present work, directional beamforming is considered. In particular, to compensate the severe large-scale path-loss owing to long transmission distance from the satellite to the relay, directional antenna is employed at both the satellite and relay. Let us denote G_S, G_R are antenna gain at the satellite and

[1] To obtain the channel state information (CSI) of the eavesdropper, several methods can be deployed, e.g., the energy ratio detectors, pilot signals, and support vector machines (SVM), etc. [20–22].

the relay, it is formulated as follows:

$$G_{s^-}(\chi) = \begin{cases} G^{s^-}_{\max} & |\chi| \le \varphi_{s^-} \\ G^{s^-}_{\min} & \varphi_{s^-} < |\chi| \le \pi \end{cases}, \quad s^- \in \{S, R\}, \tag{5}$$

where $G^{s^-}_{\max}$ and $G^{s^-}_{\min}$ are the beamforming gain of the main and side lobe of $s^- \in \{S, R\}$, respectively. $\chi \in [-\pi, \pi)$ is the angle of the boresight direction, φ_{s^-} is the beamwidth of the main lobe of the s^- antenna.

The destination, jammer, and eavesdropper, on the other hand, are equipped with a single omnidirectional antenna with antenna gain G_{o^+}, $o^+ \in \{J, D, E\}$ [29].

2.4. Received signals

The whole transmission is taken place in two phases. In the first phase, the satellite will steer its signals toward the relay and the relay also adjusts its antenna toward the satellite. The received signals at relay are then computed as follows:

$$\begin{aligned} y_R =& \sqrt{\frac{P_S G_S G_R}{O_{S,R}}} a_{S,R} x_S + n_R \\ =& \sqrt{\frac{P_S G^S_{\max} G^R_{\max}}{O_{S,R}}} a_{S,R} x_S + n_R, \end{aligned} \tag{6}$$

where P_S is the transmit power of the satellite, n_R is the additive white Gaussian noise (AWGN) at the relay, and x_S is the transmitted signals sent by S. At relay it will decode, re-encode, and forward the source signals to the destination. The received signals at the destination is then given as

$$\begin{aligned} y_D =& \sqrt{\frac{P_R G_D G_R}{O_{R,D}}} a_{R,D} x_R + n_D \\ =& \sqrt{\frac{P_R G_D G^R_{\max}}{O_{R,D}}} a_{R,D} x_R + n_D. \end{aligned} \tag{7}$$

Here n_D is the AWGN noise at the destination, P_R is the transmit power of the relay, and x_R is the transmitted signals sent by R. Besides, due to the broadcast nature of the wireless networks, the eavesdropper also receives signals from the relay and is calculated as

$$y_E = \sqrt{\frac{P_R G_E G_R}{O_{R,E}}} a_{R,E} x_R + \sqrt{\frac{P_J G_E G_J}{O_{J,E}}} a_{J,E} x_J + n_E. \tag{8}$$

Here n_E is the AWGN noise at the eavesdropper, x_J is the AN signals sent by the jammer, and P_J is the transmit power of the jammer. Here the second term in (8) is artificial interference created by the jammer toward the eavesdropper to limit the wiretap probability of the eavesdropper.

2.5. Signal-to-noise-ratio (SNR) at receivers

From (6), (7), and (8) the signal-to-noise-ratio (SNR) at the o^+, $o^+ \in \{R, D, E\}$, receiver denoted by Υ_{o^+}, is given as

$$\begin{aligned} \Upsilon_R =& \frac{P_S G^S_{\max} G^R_{\max} \left|a_{S,R}\right|^2}{O_{S,R}\sigma^2_R} \\ \Upsilon_D =& \frac{P_R G_D G^R_{\max} \left|a_{R,D}\right|^2}{O_{R,D}\sigma^2_D} \\ \Upsilon_E =& \frac{\frac{P_R G_E G^R_{\min} \left|a_{R,E}\right|^2}{O_{R,E}}}{\frac{P_J G_J G_E \left|a_{J,E}\right|^2}{O_{J,E}} + \sigma^2_E}, \end{aligned} \tag{9}$$

where $\sigma^2_{o^+} = \sigma^2 = -174 + \mathrm{NF} + 10\log_{10}(\mathrm{Bw})$ is the noise variance of the o^+ receiver, NF (in dB) is the noise figure of the receiver, Bw (in Hz) is the transmission bandwidth. Here we assume that $\mathbb{E}\left\{|x_S|^2\right\} = \mathbb{E}\left\{|x_R|^2\right\} = \mathbb{E}\left\{\left|x_J\right|^2\right\} = 1$; $\mathbb{E}\{.\}$ is the expectation operator. From (9), the end-to-end SNR at D and E denoted by $\Upsilon^R_{\mathrm{e2e}}$ and $\Upsilon^E_{\mathrm{e2e}}$ are formulated as

$$\begin{aligned} \Upsilon^D_{\mathrm{e2e}} =& \min\{\Upsilon_R, \Upsilon_D\} \\ \Upsilon^E_{\mathrm{e2e}} =& \min\{\Upsilon_R, \Upsilon_E\}. \end{aligned} \tag{10}$$

2.6. Performance metrics

In the present paper, we investigate both the security and reliability aspects of the considered satellite-terrestrial networks with FCs. Particularly, for the reliability perspectives, we study a vital metric namely, outage probability. On the other hand, from the security point of view, the intercept probability is considered which measures the probability that the eavesdropper is able to wiretap the secure information from the satellite to the destination. Let us denote X and Y as the number of successfully received packets at the destination and eavesdropper out of N transmitted packets by the satellite, the OP and IP are then defined as follows:

$$\begin{aligned} \mathrm{OP}(n) =& F_X(n, N) = \Pr(X < n), \\ \mathrm{IP}(n) =& \overline{F}_Y(n, N) = \Pr(Y \ge n). \end{aligned} \tag{11}$$

Here, $\Pr\{.\}$ is the probability operator and $\overline{F}_X(x) = 1 - F_X(x)$ is the complementary CDF (CCDF) of the RV X. The successful probability of receiving a packet at D and E, on the other hand, refers to the probability that the end-to-end SNR at destination and eavesdropper are greater than a targeted threshold. Mathematical speaking, it is formulated as

$$\begin{aligned} P_{\mathrm{suc}}(\Theta) =& \Pr\{\log_2(1 + \min(\Upsilon_R, \Upsilon_D)) \ge \Theta\} \\ P_{\mathrm{eve}}(\Theta) =& \Pr\{\log_2(1 + \min(\Upsilon_R, \Upsilon_E)) \ge \Theta\}. \end{aligned} \tag{12}$$

3. Outage Probability and Intercept Probability Analyses

In this section, we are going to derive the OP and IP of the considered networks. Before studying OP and IP, let us first provide the following Lemma which are useful to compute the IP of the considered networks.

Lemma 1. Given X and Y are two exponential random variables (RVs) with scale parameters Ξ_X and Ξ_Y and three real positive numbers, i.e., $a, b, c \in \mathbb{R}^+$, the CDF and PDF of the following RV $Z = \frac{aX}{bY+c}$ are given as follows:

$$F_Z(z) = 1 - \exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-1} \tag{13}$$

$$f_Z(z) = \exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-1}\left(\frac{c}{a\Xi_X} + \left(z + \frac{a\Xi_X}{b\Xi_Y}\right)^{-1}\right).$$

Proof. The proof is given in Appendix A. □

Next, we are going to derive the successful probability to receive a packet at the destination, P_{suc}. In particular, P_{suc} is given by (14) at the top of the next page.

Proof. Let us begin the definition of the CCDF of the e2e SNR at D as follows:

$$\begin{aligned}\overline{F}_{\Upsilon^D_{\text{e2e}}}(\Theta) =& P_{suc}(\Theta) = \Pr\left\{\Upsilon^D_{\text{e2e}} = \min\{\Upsilon_R, \Upsilon_D\} \geq \Theta\right\}\\ =& \Pr\{\min\{\Upsilon_R, \Upsilon_D\} > \Theta\}\\ =& \Pr\{\Upsilon_R > \Theta, \Upsilon_D > \Theta\}\\ =& \Pr\left\{\Upsilon_R = \frac{P_S G^S_{\max} G^R_{\max}}{O_{S,R}\sigma^2_R}\left|a_{S,R}\right|^2 > \Theta\right\}\\ &\times \Pr\left\{\Upsilon_D = \frac{P_R G^R_{\max}}{O_{R,D}\sigma^2_D}\left|a_{R,D}\right|^2 > \Theta\right\} \qquad (15)\\ =& \overline{F}_{|a_{S,R}|^2}\left(\frac{\Theta\sigma^2 O_{S,R}}{P_S G^S_{\max} G^R_{\max}}\right)\overline{F}_{|a_{R,D}|^2}\left(\frac{\Theta\sigma^2 O_{R,D}}{P_R G^R_{\max}}\right).\end{aligned}$$

Here the fifth equation is achieved owing to the uncorrelated between Υ_D and Υ_R. Here, we assume that $G_D = 1$ and the relay steers its main beam toward the destination. Finally, by substituting the CCDF of the $\left|a_{S,R}\right|^2$ and $\left|a_{R,D}\right|^2$ given by (2) and (3), we obtain (14). We close the proof here. □

Having obtained the P_{suc}, we are going to derive the OP of the legitimate link.

The outage probability refers to the event that the number of error-free packets received at the destination is less than n packets out of N total packets sent by S. Mathematical speaking, it is computed as

$$\begin{aligned}\text{OP}(n) =& \sum_{k=0}^{n-1}\binom{N}{k}(P_{\text{suc}}(\Theta))^k(1 - P_{\text{suc}}(\Theta))^{N-k}.\\ =& 1 - \mathcal{I}_{P_{\text{suc}}}(n, N-n+1).\end{aligned} \tag{16}$$

Here (16) is attained because RV X in (11) undergoes the binomial distribution with the success probability P_{suc}. Here $\mathcal{I}_{P_{\text{suc}}}(.,.)$ is the regularized incomplete beta function [24, (8.392)], $\binom{\cdot}{\cdot}$ is the binomial coefficient.

Proof. Since RV X is defined as the number of successfully received packets at the destination out of N transmitted by the satellite. It, as a consequence, follows by a binomial distribution with success probability P_{suc}. □

Similarly, the IP defines as the probability that the eavesdropper can decode the secure message sent by the satellite to the destination. Here we assume that the eavesdropper has prior information on the generator matrix of the FCs at the satellite thus, it is able to decode the message if it collects at least n packets without error. Mathematically, it is calculated as follows:

$$\begin{aligned}\text{IP}(n) =& \sum_{k=n}^{N}\binom{N}{k}(P_{\text{eve}}(\Theta))^k(1 - P_{\text{eve}}(\Theta))^{N-k}.\\ =& \mathcal{I}_{P_{\text{eve}}}(n, N-n+1),\end{aligned} \tag{17}$$

where P_{eve} is the probability that E successfully decodes a packet and is computed as follows:

$$\begin{aligned}P_{\text{eve}}(\Theta) =& \overline{F}_{\Upsilon^E_{\text{e2e}}}(\Theta) = \Pr\left\{\Upsilon^E_{\text{e2e}} = \min\{\Upsilon_R, \Upsilon_E\} \geq \Theta\right\}\\ =& \Pr\{\Upsilon_R > \Theta\}\Pr\{\Upsilon_E > \Theta\}\\ =& \overline{F}_{|a_{S,R}|^2}\left(\frac{\Theta\sigma^2 O_{S,R}}{P_S G^S_{\max} G^R_{\max}}\right)\overline{F}_{\Upsilon_E}(\Theta).\end{aligned} \tag{18}$$

The explicit equation of (18) is given in (19) at the top of the next page.

Proof. Eq. (17) is immediately obtained by following the similar steps as (16). Regarding the (19), it is attained by substituting the CCDF of $\left|a_{S,R}\right|^2$ and the help of Lemma 1. We terminate the proof here. □

Remark 1. Here we assume that eavesdropper has a prior information about the FCs. If eavesdropper does not have any information about FC, it then needs to collect correctly all N packets in order to decode the secure message from the satellite. As a result, it will reduce the intercept probability of the eavesdropper.

4. Numerical results

In this section, simulation results based on Monte-Carlo method are given to corroborate the exactitude of the derived mathematical framework as well as to reveal the influences of some key parameters such as the transmit power of the satellite, the jammer, the relay, and the antenna gain at the satellite and so on. Without loss of generality, following set of parameters

$$P_{suc}(\Theta) = \varpi \exp\left(-\frac{\Theta\sigma^2 O_{R,D}}{P_R G^R_{\max}\Omega_{R,D}}\right)\sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\Theta\sigma^2 O_{S,R}}{P_S G^S_{\max}G^R_{\max}}\right)^i \exp\left(-\frac{\Theta\sigma^2 O_{S,R}(\vartheta-\rho)}{P_S G^S_{\max}G^R_{\max}}\right). \quad (14)$$

$$P_{\text{eve}}(\Theta) = \varpi \exp\left(-\frac{\Theta\sigma_E^2 O_{R,E}}{P_R\Omega_{R,E}}\right)\left(1+\Theta\frac{P_J O_{R,E}\Omega_{J,E}}{P_R O_{J,E}\Omega_{R,E}}\right)^{-1} \times \sum_{v=0}^{m-1}\sum_{i=0}^{v}\frac{(-1)^v(1-m)_v\rho^v}{v!i!(\vartheta-\rho)^{(v+1-i)}}\left(\frac{\Theta\sigma^2 O_{S,R}}{P_S G^S_{\max}G^R_{\max}}\right)^i \exp\left(-\frac{\Theta\sigma^2 O_{S,R}(\vartheta-\rho)}{P_S G^S_{\max}G^R_{\max}}\right). \quad (19)$$

are deployed throughout this section: $N = 10$ packets, $n = 4$ packets, $P_S = 20$ dBm, $P_R = P_J = 15$ dBm, Bw = 500 kHz, NF = 6 dB, $\lambda = 3.5$, $f_c = 2.1$ GHz, $d_{S,R} = 2000$ km, $d_{R,D} = 300$ m, $d_{R,E} = 200$ m, $d_{J,E} = 150$ m, $G^S_{\max} = 30$ dB, $G^R_{\max} = 5$ dB, $G^R_{\min} = 0$ dB, $\Theta = 0.1$, $\Omega_{R,D} = 2.1$, $\Omega_{R,E} = 1.3$, $\Omega_{J,E} = 2.9$.

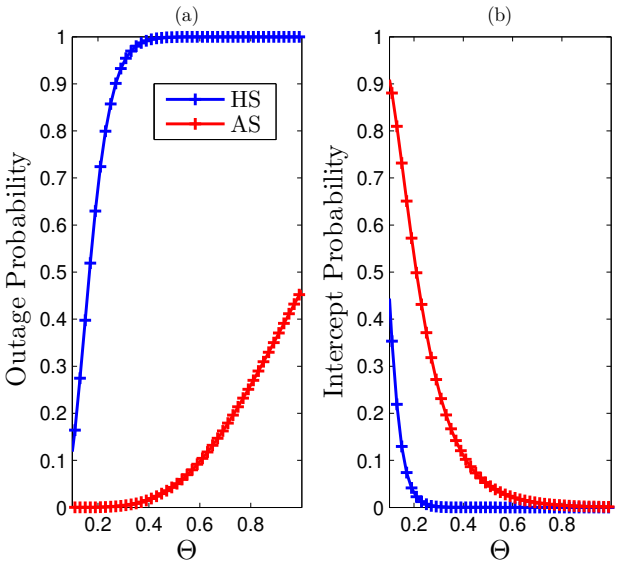

Figure 2. OP(a) and IP(b) vs. Θ. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

Fig. 2 stretches the performance of the OP and IP with respect to (w.r.t.) the Θ. It is no doubt that increasing Θ will monotonically increase OP and decrease the IP. This can be effortlessly explained by directly inspecting the definition of the P_{suc} and P_{eve} and the property of the regularized incomplete beta function. We also observe a good agreement between the derived mathematical framework and computed-based simulation results. The curves denoted by HS signify that the system undergoes the heavy shadowing scenario with the triple parameters $(m = 1, p = 0.0635, q = 0.0007)$ while curves denoted by AS means that the system suffers from average shadowing with parameters $(m = 5, p = 0.3, q = 0.279)$. It is certain that the OP under HS will approach one quicker than another because of the deep fade scenario. Besides, if HS is harmful for the reliability aspect, it is beneficial for the security as the intercept probability will quickly approach zero.

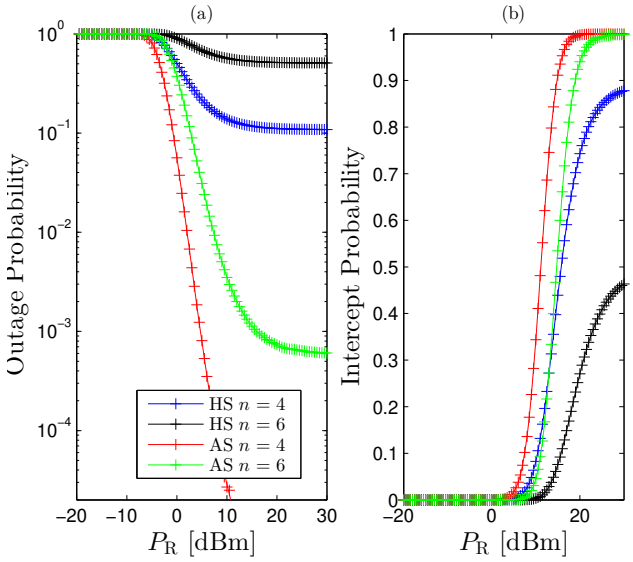

Figure 3. OP(a) and IP(b) vs. P_R [dBm] with different values of n. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

The influences of the relay transmit power on the performance of the OP and IP are given in Fig. 3. We observe again that the curves from mathematical framework and simulation results are undistinguished with each other. We see that increasing P_R will be helpful for both destination and eavesdropper. In particular, the OP is a decrease function while the IP simply scales up with the increase of P_R. Moreover, escalating the number of decoded packets will lead

to higher outage probability but smaller intercept probability. Additionally, under the AS scenario the OP achieves less than 10^{-4} with $P_R = 10$ dBm for case $n = 4$ while under the HS circumstance the best performance is only 10^{-1}. Finally, there exists a lower bound for the OP and an upper bound for the IP. The rationale behind this phenomenon is that although the SNR of the second hop keeps improving by raising the P_R, the e2e SNR is constrained by the first hop which is independent of P_R. As a result, a bound is appeared for both metrics.

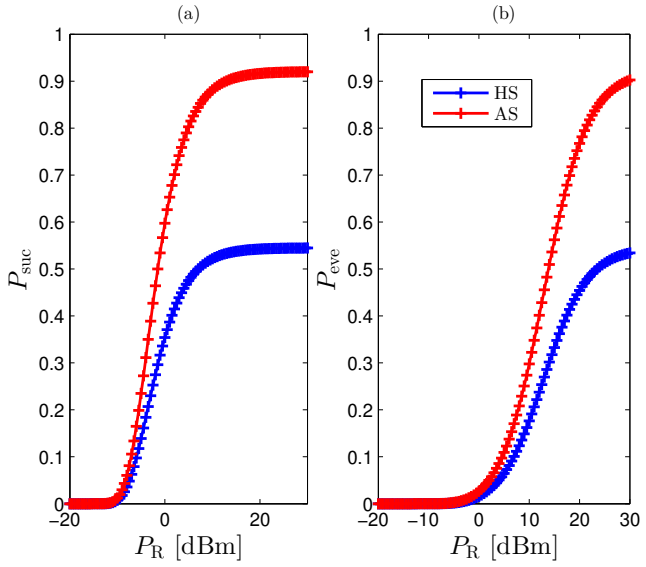

Figure 4. P_{suc}(a) and P_{eve}(b) vs. P_R [dBm] with different values of n. Solid lines are plotted by (14) and (19). Markers are plotted by the Monte-Carlo method.

Fig. 4 illustrates the performance of the P_{suc}(a) and P_{eve}(b) regarding the P_R. Unlike OP and IP which have a contrary behavior, both P_{suc} and P_{eve} are simply ameliorating with the increase of P_R. Again, the heavy shadowing has severe effects on the success probability to decode a packet of both the destination and eavesdropper. Particularly, the best performance of both P_{suc} and P_{eve} is only above 0.5 while the upper limit of two considered metrics under AS scenario is over 0.9. We see that the curves computed by (14) and (19) align with the Monte-Carlo simulations.

The impact of the number of required packets to decode the message on the performance of the outage probability and intercept probability is given in Fig. 5. It is obvious that fixing N and keeps increasing n will let the OP approach one since the probability to successfully decode a large number of packet is, of course, getting smaller. We see that enhancing the directivity gain at the satellite will dramatically improve the OP, e.g., the OP under the heavy shadowing with $G^S_{\max} = 20$ dB is equal to 1 unless $n = 1$ while the

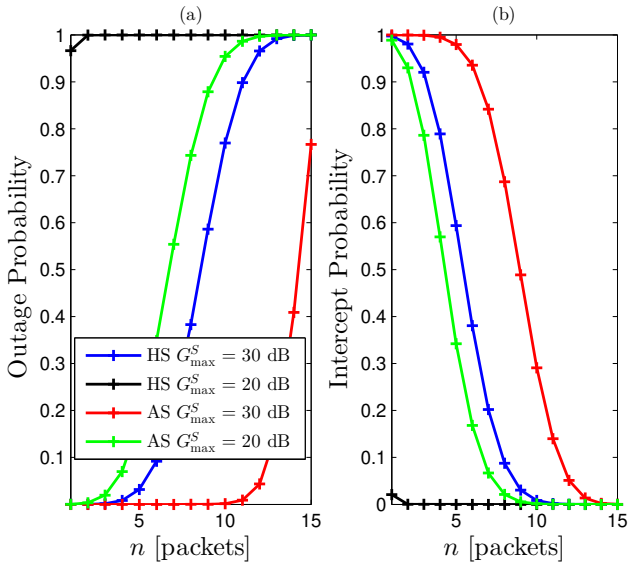

Figure 5. OP(a) and IP(b) vs. n packets with various values of $G^S_{\max}$, $N = 15$. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

OP under the same fading condition with $G^S_{\max} = 30$ dB only accesses 1 when $n = N = 15$. For the IP, decreasing $G^S_{\max}$ is beneficial.

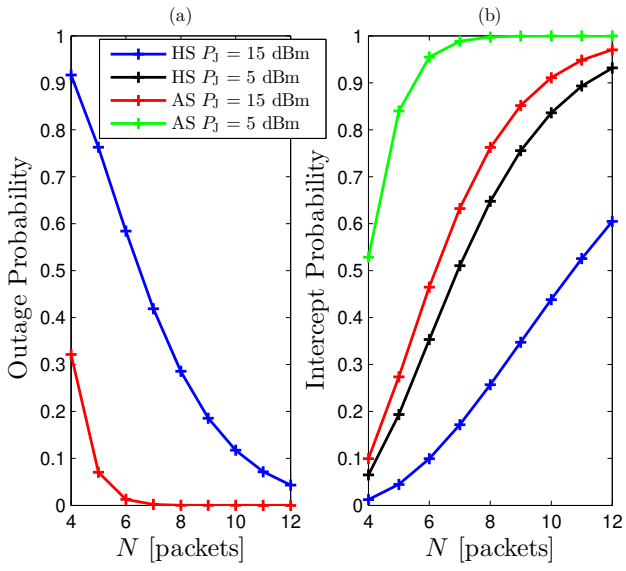

Figure 6. OP(a) and IP(b) vs. N packets with several values of P_J, $n = 4$. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

Fig. 6 studies the behaviors of OP and IP regarding N packets with different values of P_J. It should be noted that there is no effects of P_J on the OP thanks to the friendly jamming scheme. Nonetheless, augmenting the

P_J will be helpful for combating the eavesdropper. More precisely, under the average shadowing scenario, when P_J goes from 5 to 15 dBm, the IP declines two-fold from above 0.9 to under 0.5 with $N = 5$ packets. Additionally, increasing the P_J also overcomes the negative impact of the heavy shadowing as the gap between IP with P_J = 15 dBm under average shadowing and the IP with P_J = 5 dB under heavy shadowing is always less than 0.1 regardless of N. As for the OP, the OP under the AS case goes to zero faster, i.e., $N = 7$ packets.

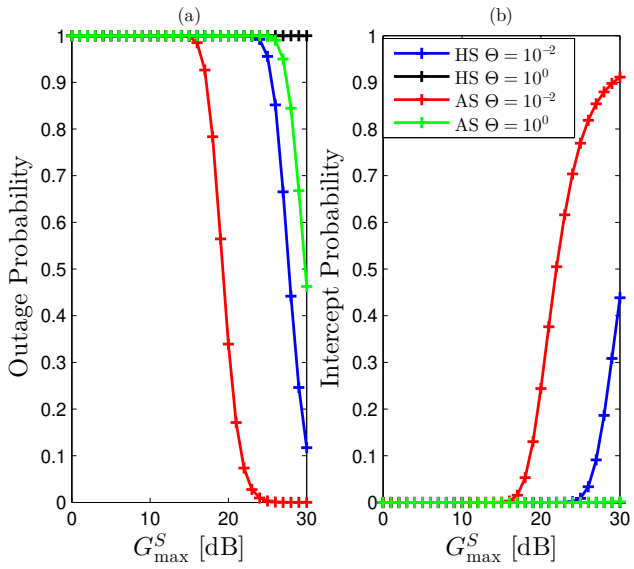

Figure 7. OP(a) and IP(b) vs. $G^S_{\max}$ packets with several values of Θ. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

Fig. 7 depicts the influences of the directional beamforming on the performance of the OP and IP. Particularly, the OP and IP are plotted as a function of the main beamforming gain of the satellite's antenna. We observe that increasing $G^S_{\max}$ is an effective approach to mitigate the long transmission distance from the satellite to ground terminals. Nonetheless, it also poses a higher risk in security since the IP is a proportional function with $G^S_{\max}$ too. Additionally, this figure also confirms our findings in Fig. 2 that enhancing the predefined threshold will degrade the system performance. More precisely, the OP under heavily shadowing with $\Theta = 1$ is always one under the current setup.

The impact of the transmission distance from the satellite to the relay is given in Fig. 8. Specifically, the transmission distance spans from low earth orbit (LEO) (from 150 - 2000 km) to medium earth orbit (MEO) (2000 - 35786 km) and geostationary equatorial orbit (GEO) (35786 km). We see that our proposed system works well in the range of LEO and parts of

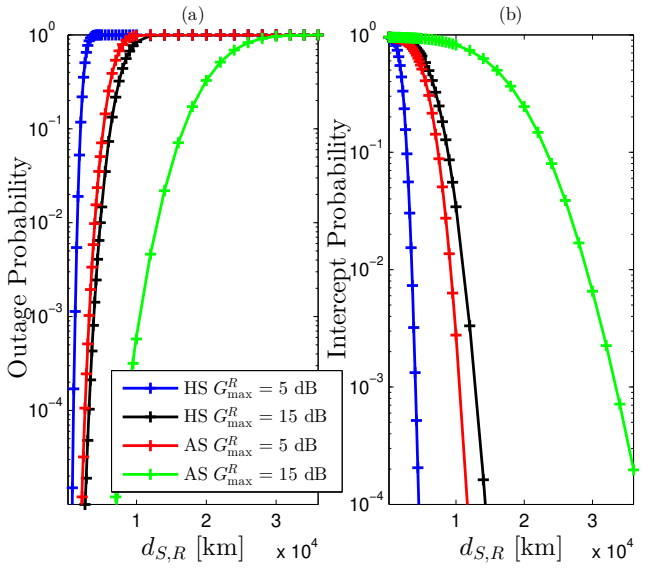

Figure 8. OP(a) and IP(b) vs. $d_{S,R}$ packets with different values of $G^R_{\max}$. Solid lines are plotted by (16) and (17). Markers are plotted by the Monte-Carlo method.

the MEO provided that the directional gain at relay is sufficiently large. More precisely, the OP under the heavy shadowing is equal to 10^{-2} with the transmission distance around 5000 km. For the average shadowing we even achieve up to 12000 km with the same threshold. From Figs. 7 and 8, we conclude that by increasing the directional gain at both the satellite and the relay, we can straightforwardly transmit signals at GEO altitude and under the heavy shadowing scenario.

5. Conclusion

The reliability and security trade-off of satellite-terrestrial communications utilizing Fountain codes were comprehensively studied in this manuscript. Particularly, the transmission link from the satellite to the ground terminal underwent the shadow-rician distribution in order to capture the strong LOS as well as the obstacle from the air-to-ground channel. Additionally, to mitigate the large-scale path-loss, the directional beamforming was deployed at both the satellite and relay to enhance the air-to-ground link. We unveiled that by increasing the antennae gain at the satellite and/or the relay, we were able to transmit at the altitude of GEO. We also found that increasing the jammer's transmit power is beneficial in terms of security but there is no impact on the systems' reliability. The paper can be developed in various ways. One of the promising ways is to consider stochastic geometry (SG) to capture the randomness of wireless networks. Second, integrating the energy-harvesting and reconfigurable intelligent surfaces into

the considered networks will dramatically enhance the whole systems' performance . Third, the covert communications and LoRa networks are interested in studying to enhance security in different ways and to cover the Internet of Things (IoTs) networks. Finally, taking advantage of the data-driven approach like deep learning is also a bright extension.

Acknowledgement. This research is funded by Posts and Telecommunications Institute of Technology under grant number 12-2023-HV-VT2.

References

[1] Duong, T.Q., Nguyen, L.D., Bui, T.T., Pham, K.D. and Karagiannidis, G.K. (2023) Machine learning-aided real-time optimized multibeam for 6g integrated satellite-terrestrial networks: Global coverage for mobile services. *IEEE Network* **37**(2): 86–93. doi:10.1109/mnet.003.2200275, URL https://doi.org/10.1109/mnet.003.2200275.

[2] Duong, T.Q., da Costa, D.B., Elkashlan, M. and Bao, V.N.Q. (2012) Cognitive amplify-and-forward relay networks over nakagami-m fading. *IEEE Transactions on Vehicular Technology* **61**(5): 2368–2374. doi:10.1109/tvt.2012.2192509, URL https://doi.org/10.1109/tvt.2012.2192509.

[3] Duy, T., Khan, L., Binh, N. and Nhat, N. (2021) Intercept probability analysis of cooperative cognitive networks using fountain codes and cooperative jamming. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **8**(26): 168229. doi:10.4108/eai.26-1-2021.168229, URL https://doi.org/10.4108/eai.26-1-2021.168229.

[4] Douglass, N.P., Langel, J., Moore, W.J., Ng, L., Dudukovich, R.M. and Mal-Sarkar, S. (2023) Application of fountain code to high-rate delay tolerant networks. *IEEE Access* : 1–1doi:10.1109/access.2023.3315659, URL https://doi.org/10.1109/access.2023.3315659.

[5] Guo, K., Shuai, H., Li, X., Yang, L., Tsiftsis, T.A., Nallanathan, A. and Wu, M. (2023) Two-way satellite-HAP-terrestrial networks with non-orthogonal multiple access. *IEEE Transactions on Vehicular Technology* : 1–15doi:10.1109/tvt.2023.3307457, URL https://doi.org/10.1109/tvt.2023.3307457.

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

[7] Sheng, Z., Tuan, H.D., Duong, T.Q. and Hanzo, L. (2021) UAV-aided two-way multi-user relaying. *IEEE Transactions on Communications* **69**(1): 246–260. doi:10.1109/tcomm.2020.3030679, URL https://doi.org/10.1109/tcomm.2020.3030679.

[8] Nguyen, T.N., Chien, T.V., Tran, D.H., Phan, V.D., Voznak, M., Chatzinotas, S., Ding, Z. *et al.* (2023) Security-reliability trade-offs for satellite-terrestrial relay networks with a friendly jammer and imperfect CSI. *IEEE Transactions on Aerospace and Electronic Systems* : 1–16doi:10.1109/taes.2023.3282934, URL https://doi.org/10.1109/taes.2023.3282934.

[9] Li, X., Li, Y., Song, X., Shao, L. and Li, H. (2023) RIS assisted UAV for weather-dependent satellite terrestrial integrated network with hybrid FSO/RF systems. *IEEE Photonics Journal* : 1–16doi:10.1109/jphot.2023.3314664, URL https://doi.org/10.1109/jphot.2023.3314664.

[10] Hung, D., Duy, T. and Trinh, D. (2019) Security-reliability analysis of multi-hop LEACH protocol with fountain codes and cooperative jamming. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **6**(18): 157120. doi:10.4108/eai.28-3-2019.157120, URL https://doi.org/10.4108/eai.28-3-2019.157120.

[11] Tu, L.T., Nguyen, T.N., Duy, T.T., Tran, P.T., Voznak, M. and Aravanis, A.I. (2022) Broadcasting in cognitive radio networks: A fountain codes approach. *IEEE Transactions on Vehicular Technology* **71**(10): 11289–11294. doi:10.1109/TVT.2022.3188969.

[12] Ngoc, L.N., Tu, L.T., Tan, N., Nguyen, P.L. and Nguyen, Q.S. (2022) Performance on cognitive broadcasting networks employing fountain codes and maximal ratio transmission. *Radioengineering* **Vol 32**. doi:10.13164/re.2023.0001.

[13] Tu, L.T., Nguyen, T.N., Tran, P.T., Duy, T.T. and Nguyen, Q.S. (2023) Performance statistics of broadcasting networks with receiver diversity and fountain codes. *Journal of Information and Telecommunication* : 1–17doi:10.1080/24751839.2023.2225254, URL https://doi.org/10.1080/24751839.2023.2225254.

[14] Jameel, F., Wyne, S., Kaddoum, G. and Duong, T.Q. (2019) A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Communications Surveys & Tutorials* **21**(3): 2734–2771. doi:10.1109/comst.2018.2865607, URL https://doi.org/10.1109/comst.2018.2865607.

[15] Anh, N., Minh, N., Duy, T., Hanh, T. and Hai, H. (2021) Reliability-security analysis for harvest-to-jam based multi-hop cluster MIMO networks using cooperative jamming methods under impact of hardware impairments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **8**(28): 170963. doi:10.4108/eai.17-9-2021.170963, URL https://doi.org/10.4108/eai.17-9-2021.170963.

[16] Nguyen, Q.S., Nguyen, T.N. and Tu, L.T. (2023) On the security and reliability performance of SWIPT-enabled full-duplex relaying in the non-orthogonal multiple access networks. *Journal of Information and Telecommunication* : 1–15doi:10.1080/24751839.2023.2218046, URL https://doi.org/10.1080/24751839.2023.2218046.

[17] Wu, Y., Duong, T.Q. and Swindlehurst, A.L. (2019) Safeguarding 5g-and-beyond networks with physical layer security. *IEEE Wireless Communications* **26**(5): 4–5. doi:10.1109/mwc.2019.8883122, URL https://doi.org/10.1109/mwc.2019.8883122.

[18] Nguyen, N.P., Tu, L.T., Duong, T.Q. and Nallanathan, A. (2017) Secure communications in cognitive underlay networks over nakagami-m channel. *Physical Communication* **25**: 610–618. doi:https://doi.org/10.1016/j.phycom.2016.05.003.

[19] Toan, N.V., Duy, T.T., Son, P.N., Hung, D.T., Sang, N.Q. and Tu, L.T. (2023) Outage performance of hybrid satellite-terrestrial relaying networks with rateless codes in co-channel interference environment. In *2023 International Conference on System Science and Engineering (ICSSE)* (IEEE). doi:10.1109/icsse58758.2023.10227228, URL https://doi.org/10.1109/icsse58758.2023.10227228.

[20] Kapetanovic, D., Zheng, G., Wong, K.K. and Ottersten, B. (2013) Detection of pilot contamination attack using random training and massive MIMO. In *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (IEEE). doi:10.1109/pimrc.2013.6666096, URL https://doi.org/10.1109/pimrc.2013.6666096.

[21] Xiong, Q., Liang, Y.C., Li, K.H. and Gong, Y. (2015) An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems. *IEEE Transactions on Information Forensics and Security* **10**(5): 932–940. doi:10.1109/tifs.2015.2392564, URL https://doi.org/10.1109/tifs.2015.2392564.

[22] Hoang, T.M., Duong, T.Q., Tuan, H.D., Lambotharan, S. and Hanzo, L. (2021) Physical layer security: Detection of active eavesdropping attacks by support vector machines. *IEEE Access* **9**: 31595–31607. doi:10.1109/access.2021.3059648, URL https://doi.org/10.1109/access.2021.3059648.

[23] Nguyen, T.N., Tu, L.T., Tran, D.H., Phan, V.D., Voznak, M., Chatzinotas, S. and Ding, Z. (2022) Outage performance of satellite terrestrial full-duplex relaying networks with co-channel interference. *IEEE Wireless Communications Letters* **11**(7): 1478–1482. doi:10.1109/LWC.2022.3175734.

[24] Gradshteyn, I.S. and Ryzhik, I.M. (2007) *Table of integrals, series, and products* (Elsevier/Academic Press, Amsterdam), seventh ed.

[25] Nguyen, T.N., Tu, L.T., Fazio, P., Chien, T.V., Le, C.V., Binh, H.T.T. and Voznak, M. (2023) On the dilemma of reliability or security in unmanned aerial vehicle communications assisted by energy harvesting relaying. *IEEE Journal on Selected Areas in Communications* : 1–1doi:10.1109/jsac.2023.3322756, URL https://doi.org/10.1109/jsac.2023.3322756.

[26] Tu, L.T., Phan, V.D., Nguyen, T.N., Tran, P.T., Duy, T.T., Nguyen, Q.S., Nguyen, N.T. *et al.* (2023) Performance analysis of multihop full-duplex NOMA systems with imperfect interference cancellation and near-field path-loss. *Sensors* **23**(1): 524. doi:10.3390/s23010524, URL https://doi.org/10.3390/s23010524.

[27] Di Renzo, M., Zappone, A., Tu, L.T. and Debbah, M. (2019) Spectral-energy efficiency pareto front in cellular networks: A stochastic geometry framework. *IEEE Wireless Communications Letters* **8**(2): 424–427. doi:10.1109/LWC.2018.2874642.

[28] Goldsmith, A. (2005) *Wireless Communications* (Cambridge University Press). doi:10.1017/cbo9780511841224, URL https://doi.org/10.1017/cbo9780511841224.

[29] Tu, L.T. and Di Renzo, M. (2017) Analysis of millimeter wave cellular networks with simultaneous wireless information and power transfer. In *2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*: 39–43. doi:10.1109/SIGTELCOM.2017.7849792.

About the authors ...

Nguyen Quang Sang (Email: sang.nguyen@ut.edu.vn) received the B.E. degree from Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam, in 2010, the M.E. degree from Ho Chi Minh City University of Technology, Ho Chi Minh City, in 2013, and the Ph.D. degree in electrical engineering from the University of Ulsan, Ulsan, South Korea, in 2017. From January 2017 to June 2017, he was a Postdoctoral Research Fellow with Queen's University Belfast, Belfast, U.K. From June 2017 until May 2021, he has been a Lecturer at Duy Tan University, Ho Chi Minh City. Since May 2021, He is currently the Dean of the Faculty of Electrical and Electronics Telecommunications Engineering at Ho Chi Minh City University of Transport. His major research interests are cooperative communication, cognitive radio network, physical layer security, energy harvesting, and non-orthogonal multiple access, Artificial intelligence.

Nguyen Van Hien (Corresponding author) (Email: hiennv@ptit.edu.vn) received Master degree in Telecommunications Engineering from Posts and Telecommunications Institute of Technology in 2022. Currently, he is working at the Department of Telecommunications 2 - Posts and Telecommunications Institute of Technology, Ho Chi Minh City campus. His major research interests are IoT networks, cooperative communications, multi-hop relay networks, energy harvesting for wireless communications, physical layer security.

Tran Trung Duy (Email: duytt@ptit.edu.vn) received the Ph.D degree in electrical engineering from University of Ulsan, South Korea in 2013. In 2013, he joined Posts and Telecommunications Institute of Technology, Ho Chi Minh city campus (PTIT-HCM), as a lecturer. From 2022, he is an associate Professor of Wireless Communications at PTIT-HCM. His major research interests are cooperative communications, cooperative multi-hop, cognitive radio, physical-layer security, energy harvesting, hardware impairments and Fountain codes.

Nguyen Luong Nhat (Email: nhatnl@ptit.edu.vn) received Ph.D degree in 1997 in Moscow, Russia. Currently, he is serving as Head of the Department of Electronics Engineering 2 at Posts and Telecommunications Institute of Technology, Ho Chi Minh City campus. His major research interests are image and signal processing, artificial intelligence and information security.

Lam-Thanh Tu (Email: tulamthanh@tdtu.edu.vn) received the Ph.D. degree from the University of Paris Sud, Paris-Saclay University, France, in 2018. From 2022, he has been with the Faculty of Electrical and Electronics Engineering, at Ton Duc Thang University, Vietnam. His research interests include stochastic geometry, LoRa networks, reconfigurable intelligent surfaces, covert communications, and artificial intelligence applications for wireless communications.

Appendix A. Proof of (13)

This section provides detail derivation of (13). Particularly, we are going to derive the CDF, and PDF of RV X. Let us commence with the definition of the CDF as follows:

$$\begin{aligned} F_Z(z) &= \Pr\left\{\frac{aX}{bY+c} \le z\right\} = \int_{y=0}^{\infty} \left(1 - \exp\left(-\frac{z(by+c)}{a\Xi_X}\right)\right) f_Y(y)\, dy \\ &= 1 - \frac{1}{\Xi_Y}\exp\left(-\frac{zc}{a\Xi_X}\right) \int_{y=0}^{\infty} \exp\left(-y\frac{zb}{a\Xi_X} - y\frac{1}{\Xi_Y}\right) dy \\ &= 1 - \exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-1}, \end{aligned} \tag{A.1}$$

where the second equation is held by substituting the CDF of the exponential RV and the last equation is attained by computing the integration. Regarding the PDF, it can be straightforwardly computed by taking the first-order derivative as follows:

$$\begin{aligned} f_Z(z) = \frac{dF_Z(z)}{dz} &= \frac{c}{a\Xi_X}\exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-1} \\ &\quad + \frac{b\Xi_Y}{a\Xi_X}\exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-2} \\ &= \exp\left(-\frac{zc}{a\Xi_X}\right)\left(1 + z\frac{b\Xi_Y}{a\Xi_X}\right)^{-1}\left(\frac{c}{a\Xi_X} + \left(z + \frac{a\Xi_X}{b\Xi_Y}\right)^{-1}\right). \end{aligned} \tag{A.2}$$

We finish the proof here.