Security-Reliability Tradeoffs for Dual-Hop Satellite Communication Systems with AF Relaying Protocol

Yeqiu Xiao[1,2], Jin Liu[1,2], and Shuangrui Zhao[3,4]
[1] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, 710048, China
[2] Shaanxi Key Laboratory for Network Computing and Security Technology, Xi'an, 710048, China
[3] School of Computer Science and Technology, Xidian University, Xi'an, 710071, China
[4] Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, 710071, China

Satellite communication systems serve as an indispensable component of heterogeneous wireless networks in the next generation era for providing various critical civil and military applications. However, due to the broadcast nature and full accessibility of the wireless medium, such systems exist serious security threats. As an effort to address this issue, this paper, for the first time, investigates secure communication in a dual-hop communication system consisting of a satellite working as an amplified-and-forward relay. We first provide the theoretical modeling to analyze the fundamental system metrics in terms of secrecy outage probability and connection outage probability. By using the modeling, we then study the security-reliability tradeoffs and propose to transmit power schemes depending on the search algorithm. We further analyze asymptotic expressions of outage performance, which was further utilized to simplify the transmit power schemes. Simulation results show the validation of the proposed secure transmission model and design schemes of transmit power. Results also illustrate that transmit power schemes based on asymptotic analysis effectively achieve the optimal performance for the relay satellite communication system.

***Index Terms*—Dual-hop satellite communication, physical layer security, secrecy outage probability, connection outage probability, security-reliability tradeoffs**

I. Introduction

Satellite communication has been widely adopted in civil and military applications because of its global availability and seamless connectivity. However, due to the broadcast nature of the wireless medium, satellite communication systems are vulnerable to eavesdropping attacks by unauthorized receivers. Traditionally, the security of satellite communication is guaranteed by cryptographic-based approaches, which could be broken as the opponent's computing capability improves greatly. Fortunately, transmission security of satellite communication can also be protected by physical layer security (PLS) technologies, which exploit different properties of wireless propagation channels [1]. The concept of physical layer security was pioneered by Wyner for the degraded wiretap channel model in [2], and later, it has been regarded as a complement of cryptography to achieve perfect secrecy from the information-theoretic perspective [3]. Therefore, serving as a critical issue, PLS for satellite communication systems has already attracted much attention.

Recently, researchers have been devoted to the study of physical-layer secure communications under different satellite systems, such as land fixed satellite systems and land mobile satellite systems. In particular, the authors in [4] first introduced PLS to satellite communication systems, where the effects of precipitation are considered. In [5] and [6], authors studied PLS in land fixed satellite communication systems and provided beamforming design to achieve systems' secrecy requirements. In [7], authors investigated secrecy performance for satellite communication systems based on Shadowed-rician fading models, a popular model for land mobile satellite channels. In [8], authors discussed the PLS performance and relay selection strategies in hybrid satellite-terrestrial relay networks. In [9]–[11], the authors studied security-reliability tradeoffs for wireless communications based on two different outage probabilities, namely secrecy outage probability (SOP) and connection outage probability (COP). Literature [12] and [13] gave kind discussions for overview of PLS in satellite communication systems.

It is worth noting that all aforementioned works focused on the one-hop or terrestrial-relay satellite communication systems. However, in practice, satellites always work as relays to support remote communications between terrestrial earth stations or users [14]. To the best of our knowledge, there are only a few works focusing on the secure communication and security-reliability tradeoffs, where a satellite acts as a relay. Miridakis *et al.* [15] investigated several transmission metrics performance for the digital communication system assisted with an amplify-and-forward (AF) satellite. Guo *et al.* [16] analyzed the COP of a dual-hop communication system with a decode-and-forward (DF) satellite relay. Xu *et al.* [17] developed a power allocation policy to optimize the secrecy capacity for a satellite communication system surrounding by a ground eavesdropper, where the satellite relay works in the DF protocol. Further, Xu *et al.* studied PLS for a hybrid satellite-terrestrial communication network [18], where signals are successively forwarded by the satellite and terrestrial relays.

It is notable from the above literature review that security-reliability tradeoffs in satellite relay communication systems have not been fully explored yet.

A. Novelty and Contributions

Motivated by the above observations, in this paper, we investigate for the first time tradeoffs between security and

Manuscript received December 19, 2021; revised June 10, 2022. Corresponding author: Shuangrui Zhao (email: zhaoshuangrui@xidian.edu.cn).

reliability for a dual-hop AF relaying satellite communication system, where the terrestrial source transmits signals to the destination with a satellite relay. We provide a comprehensive analysis for both SOP and COP. The main contributions of this paper are three-fold:

- A theoretical framework is defined for physical layer security in the dual-hop satellite communication system using the AF relaying protocol. In contrast to existing secrecy-reliability works on the dual-hop satellite communication systems, we consider signal transmission from a terrestrial source to a terrestrial destination assisted by a satellite relay as well as the coexistence of satellite and terrestrial eavesdroppers.
- To analyze the security and reliability of the dual-hop satellite communication, we provide closed-form expressions of both SOP and COP. Then, we formulate the security-reliability tradeoff problems for the established dual-hop satellite communication system, where the problem can be transformed into two constrained optimization based on [19].
- Aiming at the balance of security and reliability requirements, we design the transmit power for the satellite communication systems by solving the formulated nonlinear and nonconvex optimization problems. Approximations of optimal transmit power at the source and relay are given out in closed-form expressions, which can directly provide similar performance as the optimal one that the system can achieve.

B. Organization and Notations

The organization of this paper is as follows. Section II introduces the system models and performance metrics. In Section III, connection outage probability and secrecy outage probability are analyzed for the dual-hop satellite system and security-reliability tradeoff problems are formulated by them. Section IV discusses the proposed tradeoff problems and designs the transmit power to achieve optimal performance. We present the numerical simulation results in Section V and conclude the paper in Section VI.

Throughout this paper, we use the following notations. Let $|\cdot|$ and $\mathbb{E}[\cdot]$ denote the absolute value and the expectation operator, respectively. The functions $\Gamma(\cdot,\cdot)$ and $\gamma(\cdot,\cdot)$ are the upper incomplete gamma function and the lower incomplete gamma function. Moreover, $f_X(\cdot)$, $F_X(\cdot)$ and $\bar{F}_X(\cdot)$ stand for the probability density function, cumulative distribution function and complementary cumulative distribution function of random variable X, respectively. Finally, the notation $\mathcal{CN}(\mu,\sigma^2)$ denotes the complex Gaussian distribution with mean μ as well as variance σ^2.

II. Preliminaries

A. System Model

As shown in Fig. 1, we consider a dual-hop satellite communication system consisting of a terrestrial source S, a terrestrial destination D and a satellite relay R as well as a satellite eavesdropper E_1 and a terrestrial eavesdropper E_2.

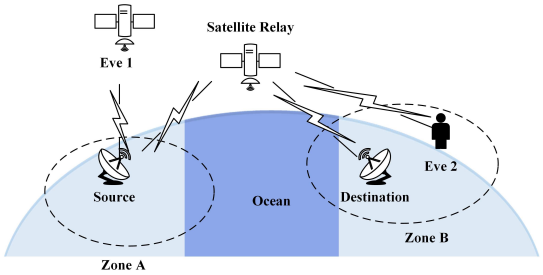


Fig. 1: System Model

Each node is equipped with a single antenna. We assume that the system works in a half-duplex mode and there is no direct link between S and D due to the long distance between them. Thus, the source has to transmit signals to the destination via the help of the node R, which experiences two phases. Specifically, in the first phase, the node S transmits signals to R, while the satellite eavesdropper E_1 overhears the process. During the second phase, the node R transmits post-processing signals to D, which operates in an amplify-and-forward (AF) scheme. In addition, the node E_2 surrounding D attempts to decode signals transmitted from the satellite relay in the second phase.

B. Channel Model

We consider a Shadowed-Rician (SR) fading channel model [20], where different channels suffer non-identical SR fading. The channel coefficient between nodes A and B is denoted as h_{AB}, where the subscript AB can be SR, SE_1, RD and RE_2. Hence, h_{SR}, h_{SE_1}, h_{RD} and h_{RE_2} correspond to these four channles from the node S to the node R, from the node S to the node E_1, from the node R to the node D and from the node R to the node E_2, respectively. $|h_{AB}|^2$ denotes the corresponding channel gain, whose probability density function (PDF) is given by [20]

$$f_{|h_{AB}|^2}(x) = \alpha_{AB} \exp\left(-\beta_{AB} x\right) {}_1F_1\left(m_{AB}, 1; c_{AB} x\right), \quad (1)$$

where $\alpha_{AB} \triangleq \frac{1}{2b_{AB}} \left(\frac{2b_{AB} m_{AB}}{2b_{AB} m_{AB} + \Omega_{AB}}\right)^{m_{AB}}$, $\beta_{AB} \triangleq \frac{1}{2b_{AB}}$, and $c_{AB} \triangleq \frac{\Omega_{AB}}{2b_{AB}(2b_{AB} m_{AB} + \Omega_{AB})}$. Moreover, m_{AB} is the fading severity parameter, Ω_{AB} represents the average power of the line-of-sight component for the link, and $2b_{AB}$ denotes the average power of the scatter. ${}_1F_1(.,.;.)$ represents the Kummer confluent hypergeometric function. It is notable that m_{AB} is set to integer values in the rest of this paper for analytical tractability like the analysis in [15].

C. Signal Model

The communication between the terrestrial source and the destination is established in two transmission phases. In the first phase, S transmits its signal to the relay with power P_S. The received signals at R and E_1 are given, respectively, as

$$y_{SR} = \sqrt{P_S} h_{SR} x + n_R, \quad (2)$$

$$y_{SE_1} = \sqrt{P_S} h_{SE_1} x + n_{E_1}, \quad (3)$$

where x is the transmit signal satisfying $\mathbb{E}\left(|x|^2\right) = 1$. $n_R \sim \mathcal{CN}\left(0, \sigma_R^2\right)$ and $n_{E_1} \sim \mathcal{CN}\left(0, \sigma_{E_1}^2\right)$ are additive white Gaussian noise (AWGN) variables at R and E_1, respectively. Thus, the signal noise ratio (SNR) at R and E_1 can be given as $\gamma_R = P_S|h_{SR}|^2/\sigma_R^2$ and $\gamma_{E_1} = P_S|h_{SE_1}|^2/\sigma_{E_1}^2$.

In the second phase, the satellite relay amplifies and forwards its received signals to the terrestrial destination. Correspondingly, the signals at D and E_2 are expressed, respectively, as

$$y_{RD} = G\sqrt{P_S P_R}h_{SR}h_{RD}x + (G\sqrt{P_R}n_R h_{RD} + n_D), \quad (4)$$

and

$$y_{RE_2} = G\sqrt{P_S P_R}h_{SR}h_{RE_2}x + (G\sqrt{P_R}n_R h_{RE_2} + n_{E_2}), \quad (5)$$

where P_R is the transmit power at R. n_D and n_{E_2} represent AWGN at D and E_2 with variance σ_D^2 and $\sigma_{E_2}^2$, respectively. Moreover, G is a gain factor, which can be determined as [21, eq.(7)]

$$G^2 \triangleq \frac{1}{P_S|h_{SR}|^2 + \sigma_R^2}. \quad (6)$$

Based on (4) and (5), the SNR at D and E_2 can be obtained, respectively, as

$$\gamma_D = \frac{\frac{P_S|h_{SR}|^2}{\sigma_R^2}\frac{P_R|h_{RD}|^2}{\sigma_D^2}}{\frac{P_R|h_{RD}|^2}{\sigma_D^2} + \frac{1}{G^2\sigma_R^2}} = \frac{\gamma_R\gamma_{D'}}{\gamma_R + \gamma_{D'} + 1}, \quad (7)$$

and

$$\gamma_{E_2} = \frac{\frac{P_S|h_{SR}|^2}{\sigma_R^2}\frac{P_R|h_{RE_2}|^2}{\sigma_{E_2}^2}}{\frac{P_R|h_{RE_2}|^2}{\sigma_{E_2}^2} + \frac{1}{G^2\sigma_R^2}} = \frac{\gamma_R\gamma_{E_2'}}{\gamma_R + \gamma_{E_2'} + 1}, \quad (8)$$

where $\gamma_{D'} = P_R|h_{RD}|^2/\sigma_D^2$ and $\gamma_{E_2'} = P_R|h_{RE_2}|^2/\sigma_{E_2}^2$.

D. Performance Metrics

The performance metrics, connection outage probability (COP) and secrecy outage probability (SOP), are used to quantify the reliability and security of the satellite communication system, respectively. COP and SOP are defined as follows:

1) Connection outage probability

The event of connection outage happens when the instantaneous achievable rate of the legitimate channel is less than a required rate of transmitted codewords R_t, such that the receiver can not correctly decode the message. The probability that a connection outage event happens is called connection outage probability. Under the AF scheme, the satellite relay does not decode its received signals. Therefore, COP of the satellite communication depends on the transmission in the second phase [22], which is given by

$$P_{co} \triangleq \mathbb{P}(\log_2(1+\gamma_D) \leq R_t) = \mathbb{P}(\gamma_D \leq \lambda_c). \quad (9)$$

where $\lambda_c = 2^{R_t} - 1$.

2) Secrecy outage probability

The event of secrecy outage occurs when the instantaneous achievable rate of one or more eavesdroppers' channels is above the difference between the rate of transmitted codewords R_t and the required rate of the confidential messages R_s, such that at least one of the eavesdroppers can decode the message. Secrecy outage probability is defined as the probability that a secrecy outage event occurs. For the dual-hop satellite communication system, SOP relies on both the transmission in the first phase and the second phase. Therefore, SOP under the AF scheme can be formulated as

$$\begin{aligned} P_{so} &\triangleq \mathbb{P}\left(\bigcup_{B\in\{E_1, E_2'\}} \{\log_2(1+\gamma_B) \geq R_t - R_s\}\right) \\ &= 1 - \mathbb{P}(\gamma_{E_1} < \lambda_e)\mathbb{P}(\gamma_{E_2'} < \lambda_e), \end{aligned} \quad (10)$$

where $\lambda_e \triangleq 2^{R_t - R_s} - 1$.

III. Performance Evaluation and Problem Formulation

Here, we analyze respective connection outage probability (COP) and secrecy outage probability (SOP) for the dual-hop satellite communication system operating amplify-and-forward (AF) manner.

A. Outage Performance Evaluation

Recall (1), the probability density function (PDF) of Shadowed-Rician channel gain. Utilizing [23, Eq. (07.20.02.0001.01)], the PDF of the signal-to-ratio (SNR) at the receiver B can be written as

$$f_{\gamma_B}(x) = \sum_{k=0}^{m_{AB}-1} \frac{\alpha_{AB}\Theta_{AB}(k)}{k!^2\bar{\gamma}_B^{k+1}} x^k \exp\left(-\frac{\Delta_{AB}}{\bar{\gamma}_B}x\right), \quad (11)$$

where $A \in \{S\}$ with $B \in \{R, E_1\}$ or $A \in \{R\}$ with $B \in \{D', E_2'\}$. Moreover, $\bar{\gamma}_B \triangleq \frac{P_S}{\sigma_B^2}$ for the first hop, $\bar{\gamma}_B \triangleq \frac{P_R}{\sigma_B^2}$ for the second hop, $\Delta_{AB} \triangleq \beta_{AB} - c_{AB}$ and $\Theta_{AB}(k) \triangleq (1-m_{AB})_k (-c_{AB})^k$. Then, the cumulative distribution function (CDF) and the complementary cumulative distribution function (CCDF) of γ_B can be derived, respectively, by

$$F_{\gamma_B}(x) = \sum_{k=0}^{m_{AB}-1} \frac{\alpha_{AB}\Theta_{AB}(k)}{k!^2\Delta_{AB}^{k+1}} \gamma\left(k+1, \frac{\Delta_{AB}}{\bar{\gamma}_B}x\right), \quad (12)$$

and

$$\bar{F}_{\gamma_B}(x) = \sum_{k=0}^{m_{AB}-1} \frac{\alpha_{AB}\Theta_{AB}(k)}{k!^2\Delta_{AB}^{k+1}} \Gamma\left(k+1, \frac{\Delta_{AB}}{\bar{\gamma}_B}x\right). \quad (13)$$

Lemma 1: When the satellite relay operates an amplified-and-forward scheme, the COP and SOP of the dual-hop satellite communication are given as (14) and (15), respectively, where $K_v(.)$ is the modified Bessel functions of the second kind with order v.

Proof: The proof is presented in Appendix A. ■

$$P_{co} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{m_{RD}-1} \frac{\alpha_{SR}\Theta_{SR}(k)}{\Delta_{SR}^{k+1}} \frac{\alpha_{RD}\Theta_{RD}(l)}{\Delta_{RD}^{l+1}} \sum_{p=0}^{k}\sum_{r=0}^{p}\sum_{s=0}^{l} \frac{2}{l!p!} \binom{p}{r} \binom{l}{s} \left(\frac{\Delta_{SR}}{\bar{\gamma}_R}\right)^{\frac{2p+s-r+1}{2}} \left(\frac{\Delta_{RD}}{\bar{\gamma}_{D'}}\right)^{\frac{2l-s+r+1}{2}} \times \lambda_c^{p+l-s-r}(\lambda_c^2+\lambda_c)^{\frac{s+r+1}{2}} \exp\left(-\frac{\Delta_{SR}}{\bar{\gamma}_R}\lambda_c - \frac{\Delta_{RD}}{\bar{\gamma}_{D'}}\lambda_c\right) K_{s-r+1}\left(2\sqrt{\frac{\Delta_{SR}}{\bar{\gamma}_R}\frac{\Delta_{RD}}{\bar{\gamma}_{D'}}(\lambda_c^2+\lambda_c)}\right) \quad (14)$$

$$P_{so} = \sum_{t=0}^{m_{SE_1}-1} \frac{\alpha_{SE_1}\Theta_{SE_1}(t)}{t!^2\Delta_{SE_1}^{t+1}}\Gamma\left(t+1, \frac{\Delta_{SE_1}}{\bar{\gamma}_{E_1}}\lambda_e\right) + \sum_{k=0}^{m_{SR}-1}\sum_{t=0}^{m_{SE_1}-1}\sum_{l=0}^{m_{RE_2}-1} \frac{\alpha_{SR}\Theta_{SR}(k)}{\Delta_{SR}^{k+1}} \frac{\alpha_{SE_1}\Theta_{SE_1}(t)}{\Delta_{SE_1}^{t+1}} \frac{\alpha_{RE_2}\Theta_{RE_2}(l)}{\Delta_{RE_2}^{l+1}} \times \sum_{p=0}^{k}\sum_{r=0}^{p}\sum_{s=0}^{l} \frac{2}{t!^2 l! p!} \binom{p}{r} \binom{l}{s} \left(\frac{\Delta_{SR}}{\bar{\gamma}_R}\right)^{\frac{2p+s-r+1}{2}} \left(\frac{\Delta_{RE_2}}{\bar{\gamma}_{E_2'}}\right)^{\frac{2l-s+r+1}{2}} \lambda_e^{p+l-s-r}(\lambda_e^2+\lambda_e)^{\frac{s+r+1}{2}} \times \exp\left(-\frac{\Delta_{SR}}{\bar{\gamma}_R}\lambda_e - \frac{\Delta_{RE_2}}{\bar{\gamma}_{E_2'}}\lambda_e\right)\gamma\left(t+1, \frac{\Delta_{SE_1}}{\bar{\gamma}_{E_1}}\lambda_e\right) K_{s-r+1}\left(2\sqrt{\frac{\Delta_{SR}}{\bar{\gamma}_R}\frac{\Delta_{RE_2}}{\bar{\gamma}_{E_2'}}(\lambda_e^2+\lambda_e)}\right) \quad (15)$$

B. Security-Reliability Tradeoff Problem Formulation

For a given dual-hop satellite communication system, parameters λ_c and λ_e are usually predetermined, but parameters P_S and P_R are controllable and can be changed. Note that $\Theta_{AB}(k) > 0$ due to [23, Eq. (06.10.02.0003.01)] and $\Delta_{AB} = \frac{m_{AB}}{2b_{AB}m_{AB}+\Omega_{AB}} > 0$. We utilize Leibniz integral rule to give the partial derivative of (14) and (15) with respect to P_S and P_R as

$$\frac{\partial P_{co}}{\partial P_S} = -\int_0^{+\infty} \frac{g_c(x)}{P_S} f_{\gamma_R}(g_c(x)) f_{\gamma_{D'}}(\lambda_c+x)\, dx, \quad (16)$$

$$\frac{\partial P_{co}}{\partial P_R} = -\int_0^{+\infty} \frac{g_c(x)}{P_R} f_{\gamma_R}(\lambda_c+x) f_{\gamma_{D'}}(g_c(x))\, dx, \quad (17)$$

$$\frac{\partial P_{so}}{\partial P_S} = \frac{F_{\gamma_{E_1}}(\lambda_e)}{P_S}\int_0^{\infty} g_e(x) f_{\gamma_R}(g_e(x)) f_{\gamma_{E_2'}}(\lambda_e+x)\, dx + \frac{\lambda_e}{P_S} f_{\gamma_{E_1}}(\lambda_e) F_{\gamma_{E_2}}(\lambda_e), \quad (18)$$

$$\frac{\partial P_{so}}{\partial P_R} = \frac{F_{\gamma_{E_1}}(\lambda_e)}{P_R}\int_0^{\infty} g_e(x) f_{\gamma_R}(\lambda_e+x) f_{\gamma_{E_2'}}(g_e(x))\, dx, \quad (19)$$

where $g_v(x) = \lambda_v + \frac{\lambda_v^2+\lambda_v}{x}$ and $v \in \{c, e\}$. Obviously, $\frac{\partial P_{co}}{\partial P_S} < 0$, $\frac{\partial P_{co}}{\partial P_R} < 0$, $\frac{\partial P_{so}}{\partial P_S} > 0$ and $\frac{\partial P_{so}}{\partial P_R} < 0$ since $g_v(x) > 0$ and $f_{\gamma_B}(x) > 0$.

The above observation indicates that the COP monotonically decreases but SOP monotonically increases with growing transmit power for the dual-hop satellite communication system. It means that the tradeoffs between reliability and security exist. Therefore, our interest in this paper is to achieve the security-reliability tradeoff by adjusting the transmit power at the source and the relay, which can be formulated by two optimization problems as follows [19].

1) Security-Based Reliability Optimization (S-RO)

The objective of problem S-RO is to minimize COP conditioned on that SOP is below some pre-specified threshold, which can be mathematically formulated as

$$\min_{P_S,P_R} \quad P_{co}(P_S,P_R) \quad (20a)$$

$$\text{s.t.} \quad P_{so}(P_S,P_R) \le \varepsilon, \quad (20b)$$

$$0 < P_B \le P_B^{\max}, B \in \{S,R\}, \quad (20c)$$

where $0 < \varepsilon < 1$.

2) Reliability-Based Security Optimization (R-SO)

The problem R-SO is to achieve the minimum SOP by the transmit power design and ensure that COP is below a pre-specified threshold, which is mathematically expressed as

$$\min_{P_S,P_R} \quad P_{so}(P_S,P_R) \quad (21a)$$

$$\text{s.t.} \quad P_{co}(P_S,P_R) \le \varepsilon, \quad (21b)$$

$$0 < P_B \le P_B^{\max}, B \in \{S,R\}, \quad (21c)$$

where $0 < \varepsilon < 1$.

Note that these two optimization problems are both non-convex in this paper due to complex expressions of COP and SOP. Thus, it is difficult to design the transmit power for them to achieve optimal performance, which will be analyzed in the following sections.

IV. Security-Reliability Tradeoff Analysis

In this section, we design the transmit power to achieve the minimum connection outage probability (COP) in the problem of security-based reliability optimization (S-RO) as well as the minimum secrecy outage probability (SOP) in the problem of reliability-based security optimization (R-SO).

A. Transmit Power Design for Tradeoff Problems

Proposition 1: By optimizing the transmit power, the minimum COP constrained by the SOP requirement can be obtained for the AF scheme. We use P_S^* and P_R^* to denote the optimal transmit power of the source and the relay. Then, we have that

$$(P_S^*, P_R^*) = \begin{cases} (P_S^{\max}, P_R^{\max}), & \text{if } (P_{so})^\star \le \varepsilon, \quad (22a) \\ \arg\min\limits_{(P_S,P_R)\in \boldsymbol{P}_1^\circ} P_{co}, & \text{else}, \quad (22b) \end{cases}$$

where

$$\boldsymbol{p}_1^{\circ} = \{(p_S^{\circ}, P_R^{\max}), (P_S^{\max}, p_R^{\circ})\}, \tag{23a}$$
$$p_S^{\circ} = \{P_S \in (0, P_S^{\max}) | P_{so}(P_S, P_R^{\max}) - \varepsilon = 0\}, \tag{23b}$$
$$p_R^{\circ} = \{P_R \in (0, P_R^{\max}) | P_{so}(P_S^{\max}, P_R) - \varepsilon = 0\}, \tag{23c}$$

and $(P_{so})^{\star} \triangleq P_{so}(P_S^{\max}, P_R^{\max})$.

Proof: The proof is provided in Appendix B. ∎

Moreover, if m_{SE_1} or m_{SE_2} is set to a large value, the function $P_{so}(P_S, P_R) = \varepsilon$ will become to be a high-ordered equation. Although exact expressions of P_S^* in (23b) and P_R^* in (23c) are difficult to obtain, approximate values of them can be achieved with the aid of some root-finding algorithms, such as Newton's method and the Quasi-Newton method.

Proposition 2: The optimal transmit power at the source and the relay for problem R-SO under the AF scheme is determined by the following equation, which is expressed as

$$(P_S^*, P_R^*) = \begin{cases} N/A, & \text{if } (P_{co})^{\star} > \varepsilon, \quad (24a) \\ (P_S^{\max}, P_R^{\max}), & \text{else if } (P_{co})^{\star} = \varepsilon, \quad (24b) \\ \arg \min\limits_{(P_S, P_R) \in \boldsymbol{p}_2^{\circ}} P_{co}, & \text{else}, \quad (24c) \end{cases}$$

where $\boldsymbol{p}_2^{\circ} = \{(P_S, P_R) | P_{co}^{AF}(P_S, P_R) = \varepsilon, P_S \in (0, P_S^{\max}), P_R \in (0, P_R^{\max})\}$ and $(P_{co})^{\star} \triangleq P_{co}(P_S^{\max}, P_R^{\max})$.

Proof: The proof is provided in Appendix C ∎

Furthermore, approximate values of P_S^* and P_R^* can be determined by using sequential quadratic programming (SQP) for (24c).

B. Approximation for Optimal Transmit Power

Here, we first give an approximation of COP and SOP for the dual-hop satellite communication systems, which establishes the following lemma.

Lemma 2: The connection outage probability (COP) and secrecy outage probability (SOP) of the satellite communication system under AF scheme are approximately described as

$$P_{co}^{asy} = 1 - \exp\left(-\frac{K_{SR}^c}{P_S} - \frac{K_{RD}^c}{P_R}\right), \tag{25}$$

$$P_{so}^{asy} = \exp\left(-\frac{K_{SE_1}^e}{P_S}\right) + \exp\left(-\frac{K_{SR}^e}{P_S} - \frac{K_{RE_2}^e}{P_R}\right) - \exp\left(-\frac{K_{SE_1}^e}{P_S} - \frac{K_{SR}^e}{P_S} - \frac{K_{RE_2}^e}{P_R}\right), \tag{26}$$

where $K_{AB}^v \triangleq \beta_{AB}\sigma_B^2\lambda_v$, $v \in \{c, e\}$, $A \in \{S\}$ and $B \in \{R, E_1\}$ or $A \in \{R\}$ and $B \in \{D, E_2\}$.

Proof: The proof is provided in Appendix D. ∎

Then, the optimization problem in (20) can be rewritten as

$$\min_{P_S, P_R} \quad P_{co}^{asy}(P_S, P_R), \tag{27a}$$
$$\text{s.t.} \quad P_{so}^{asy}(P_S, P_R) \le \varepsilon, \tag{27b}$$
$$0 \le P_B \le P_B^{\max}, B \in \{S, R\}. \tag{27c}$$

Proposition 3: The minimum value of COP for problem SO-COP is described as

$$P_{co}^{\min} = \min\{P_{co}^{asy}(P_S^*, P_R^{\max}), P_{co}^{asy}(P_S^{\max}, P_R^*)\}, \tag{28}$$

where

$$P_S^* = \min\left\{\frac{K_{SR}^e}{\ln\left(\frac{A_1+1+\sqrt{(A_1+1)^2-4\varepsilon A_1}}{2\varepsilon}\right) - \frac{K_{RE_2}^e}{P_R^{\max}}}, P_S^{\max}\right\}, \tag{29a}$$

$$P_R^* = \min\left\{\frac{K_{RE_2}^e}{\ln\left(\frac{1-A_2}{1-\varepsilon A_2}\right) - \frac{K_{SR}^e}{P_S^{\max}}}, P_R^{\max}\right\}. \tag{29b}$$

Furthermore, $A_1 = \exp\left(\frac{K_{RE_2}^e}{P_R^{\max}}\right)$ and $A_2 = \exp\left(\frac{K_{SE_1}^e}{P_S^{\max}}\right)$.

Proof: The proof is provided in Appendix E. ∎

Moreover, the problem CO-SOP can be reformulated as

$$\min_{\boldsymbol{P}} \quad P_{so}^{asy}(P_S, P_R), \tag{30a}$$
$$\text{s.t.} \quad P_{co}^{asy}(P_S, P_R) \le \varepsilon, \tag{30b}$$
$$0 \le P_B \le P_S^{\max}, B \in \{S, R\}. \tag{30c}$$

Proposition 4: The minimum SOP for problem CO-SOP can be described as

$$P_{so}^{\min} = P_{so}^{asy}\left(\min\left\{\frac{K_{SR}^c}{-\ln(1-\varepsilon)}, P_S^{\max}\right\}, \min\left\{\frac{K_{RD}^c}{-\ln(1-\varepsilon)}, P_R^{\max}\right\}\right). \tag{31}$$

Proof: The proof is presented in Appendix F. ∎

V. Simulations

In this section, we first conduct Monte Carlo (MC) simulations to validate our analytical results for the outage performance of the concerned satellite communication system, and then apply theoretical results to demonstrate tradeoffs between security and reliability for the system.

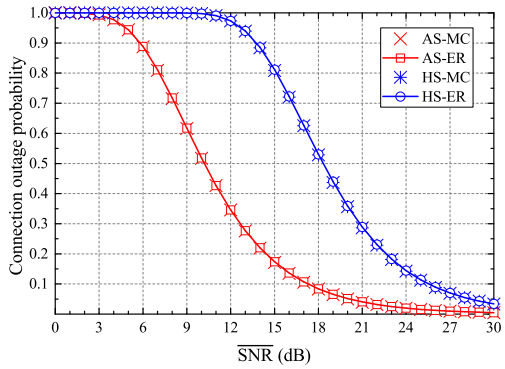
A. Simulation Settings

All channel coefficients h_{SR}, h_{RD}, h_{SE_1} and h_{RE_2} are set to follow independent distributed Shadowed-Rician (SR) fading. The variances of Gaussian noise are set to be $\sigma_R^2 = \sigma_D^2 = \sigma_{E_1}^2 = \sigma_{E_2}^2 = 1$. Without loss of generality, we consider two kinds of channel fading states, which are determined by parameters provided in [15] as $\{m_R, b_R, \Omega_R\} = \{m_D, b_D, \Omega_D\} = \{m_{E_1}, b_{E_1}, \Omega_{E_1}\} = \{m_{E_2}, b_{E_2}, \Omega_{E_2}\} = \{5, 0.251, 0.279\}$ for average shadowing (AS) condition, and $\{m_R, b_R, \Omega_R\} = \{m_D, b_D, \Omega_D\} = \{m_{E_1}, b_{E_1}, \Omega_{E_1}\} = \{m_{E_2}, b_{E_2}, \Omega_{E_2}\} = \{2, 0.063, 0.0005\}$ for heavy shadowing (HS) condition.

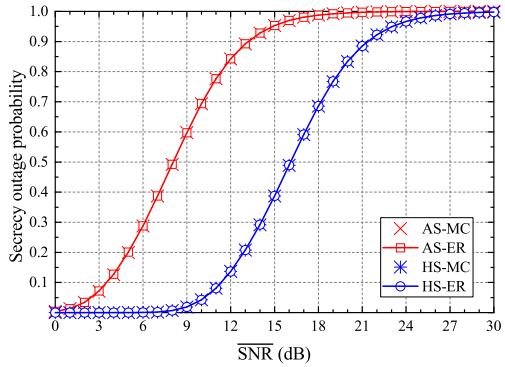
B. Validation of Outage Performance Evaluation

In this subsection, we compare the exact results (ER), asymptotic analysis (AA) and MC simulation results for the outage performance, where we set the number of trials in each task of MC simulation is to be 10^6, $\lambda_c = 2$ dB, $\lambda_e = 4$ dB and $P_S/\sigma_R^2 = P_R/\sigma_D^2 = \overline{\text{SNR}}$.

We first summarize in Fig. 2 the validation of our ER for connection outage probability (COP) and secrecy outage

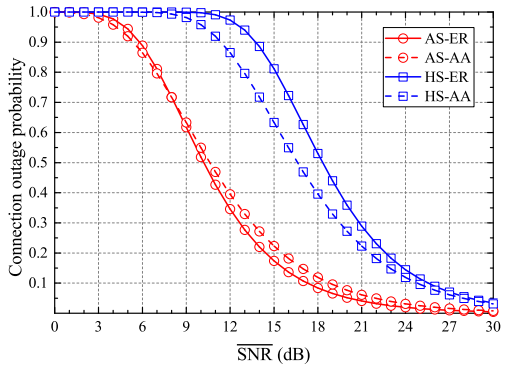


(a) Connection outage probability

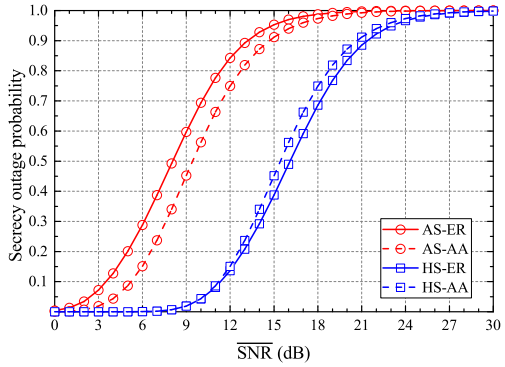


(b) Secrecy outage probability

Fig. 2: Validation of theoretical results.



(a) Connection outage probability



(b) Secrecy outage probability

Fig. 3: Validation of asymptotic analysis.

probability (SOP) via MC simulation results. The curves of theoretical analysis for COP and SOP are plotted according to (14) and (15), respectively. Whenever channel fading states approach AS or HS, the simulation results match well with the exact ones for COP and SOP. Fig. 2 shows that the COP monotonically increases but SOP decreases when $\overline{\text{SNR}}$ arises, which indicates that there is a tradeoff between COP and SOP. Another observation is that as $\overline{\text{SNR}}$ changes, outage performance has a much greater change in average shadowing conditions than that does in heavy shadowing conditions.

We then plot Fig.3 to show comparisons between ER and AA for the connection outage probability and secrecy outage probability, where approximate values for COP and SOP are calculated by (25) and (26), respectively. When $\overline{\text{SNR}}$ is over 20 dB, the difference between ER and AA of outage performance is negligible, indicating that our asymptotic analysis works well for COP and SOP in the high-SNR regime. Moreover, it is interesting to see from Fig.3(a) that approximate COP is even close to the exact COP in the low-SNR region, especially for the AS case. From Fig.3(b), it is shown that compared with the case in the satellite communication system suffers average shadowing, and our approximation has a better performance when the satellite communication system approaches heavy shadowing.

C. Tradeoffs Between Security and Reliability

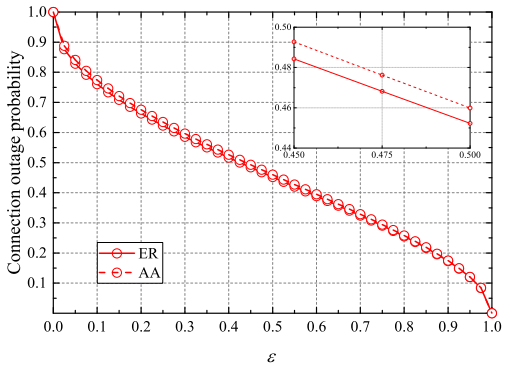
In this subsection, we present optimal performance for the tradeoff between security and reliability through transmit power design based on exact and asymptotic analysis.

1) Problem SO-COP

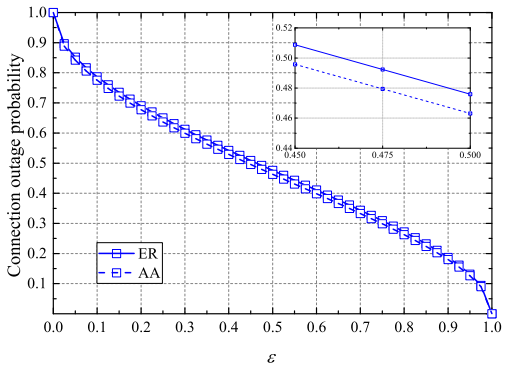
We summarize in Fig. 4 the minimum COP under limited SOP, where the curves of exact analysis are drawn on the basis of (22) and approximation results are plotted according to (28). We can observe that each point of the curve named AA is close to the corresponding one on the curve called ER under both AS and HS fading environments, which means that utilizing the design of transmit power in Proposition 3 can effectively and efficiently provide optimal transmission reliability for the dual-hop satellite communication system.

2) Problem CO-SOP

In Fig. 5, we show the optimal SOP under constrained COP, which illustrates a requirement of transmission reliability exists. Compared with the minimum SOP based on Proposition 2, we can find that a similar secrecy performance can be achieved by Proposition 4 in the AS fading scenario. For the HS environments, the asymptotic analysis will approach the ER of optimal SOP if the value of the parameter ε regarding the corresponding constraint condition is set far from 0.5. Moreover, Fig. 5 presents that the achieved SOP decreases with the growth of ε. The reason is that a large value of

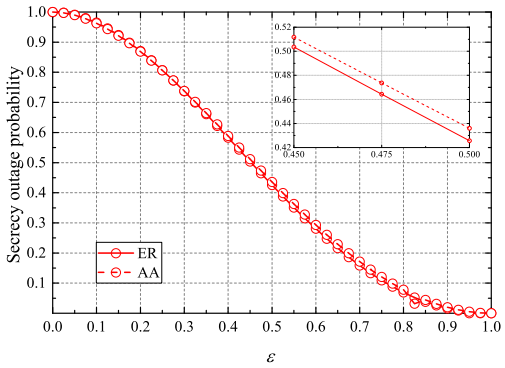


(a) Average shadowing environments

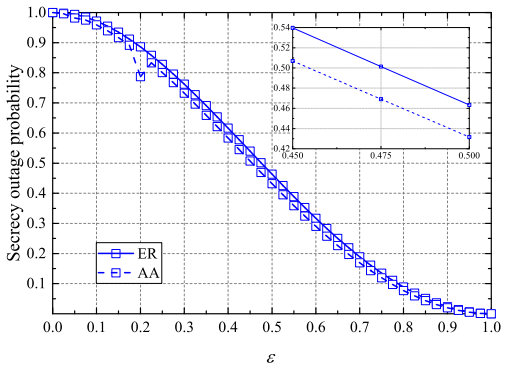


(b) Heavy shadowing environments

Fig. 4: Problem SO-COP.



(a) Average shadowing environments



(b) Heavy shadowing environments

Fig. 5: Problem CO-SOP.

ε illustrates fewer requirements of secrecy. Specifically, the point that $\varepsilon = 1$ is a special and unpractical case, where the constraint on COP is ignored and SOP can be close to zero because of low transmit power.

VI. Conclusions

This paper investigated security-reliability tradeoffs in the dual-hop satellite communication system through two metrics, namely connection outage probability and secrecy outage probability. To this end, we developed theoretical frameworks to model the optimal reliability with limited requirements of secrecy and the optimal secrecy with constraints of reliability. Aiming at optimal performance, we designed the transmit power and also proposed a method based on asymptotic analysis to seek optimal transmit power with less process. The results in this paper indicate that the asymptotic approaches can provide similar performance to the optimal transmission performance.

Acknowledgments

This work was supported in part by the National Key R&D Program of China (Grant No. 2018YFE0207600), in part by the National Natural Science Founds of China (62072368, 61972308, U20B2050), in part by Key Research and Development Program of Shaanxi Province (2021ZDLGY05-09, 2022GY-040), and in part by Natural Science Basic Research Program of Shaanxi (Program No. 2019JC-17).

Appendix A
Proof of Lemma 1

Based on [15, Eq. (B.1)], it holds that

$$P_{co} = F_{\gamma_D}(\lambda_c) = 1 - \int_0^{\infty} \bar{F}_{\gamma_R}\left(\lambda_c + \frac{\lambda_c^2+\lambda_c}{x}\right) f_{\gamma_{D'}}(\lambda_c + x)\, dx, \quad \text{(A.1)}$$

where the part respect with to the CCDF of γ_R can be rewritten as [24, Eq. (8.352.2)]

$$\bar{F}_{\gamma_R}\left(\lambda_c + \frac{\lambda_c^2+\lambda_c}{x}\right) = \sum_{k=0}^{m_{SR}-1} \sum_{p=0}^{k} \frac{\alpha_{SR}\Theta_{SR}(k)}{k!p!\Delta_{SR}^{k+1}} \left(\frac{\Delta_{SR}\lambda_c}{\bar{\gamma}_R}\right)^p \left(1 + \frac{\lambda_c+1}{x}\right)^p \times \exp\left(-\frac{\Delta_{SR}\lambda_c}{\bar{\gamma}_R}\left(1 + \frac{\lambda_c+1}{x}\right)\right). \quad \text{(A.2)}$$

Then, utilizing binomial expansion, (A.1) will be transformed by

$$P_{co} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{m_{RD}-1} \frac{\alpha_{SR}\Theta_{SR}(k)}{\Delta_{SR}^{k+1}} \frac{\alpha_{RD}\Theta_{RD}(l)}{\bar{\gamma}_D^{l+1}} \times \sum_{p=0}^{k} \sum_{r=0}^{p} \sum_{s=0}^{l} \frac{1}{k!l!^2p!} \binom{p}{r} \binom{l}{s} \left(\frac{\Delta_{SR}}{\bar{\gamma}_R}\right)^p \times \lambda_c^{p+l-s} (\lambda_c+1)^r \exp\left(-\frac{\Delta_{SR}}{\bar{\gamma}_R}\lambda_c - \frac{\Delta_{RD}}{\bar{\gamma}_D}\lambda_c\right) \times \int_0^\infty w(s,r;x)\, dx, \quad \text{(A.3)}$$

where

$$w(s,r;x) = x^{s-r} \exp\left(-\frac{\Delta_{SR}(\lambda_c^2+\lambda_c)}{\bar{\gamma}_R x} - \frac{\Delta_{RD}}{\bar{\gamma}_D}x\right). \quad \text{(A.4)}$$

With the aid of [24, Eq. (3.471.9)] and after some algebraic manipulations, (14) can be directly given.

From (10), we have that

$$P_{so} = \bar{F}_{\gamma_{E_1}}(\lambda_e) + F_{\gamma_{E_1}}(\lambda_e) \times \int_0^\infty \bar{F}_{\gamma_R}\left(\lambda_e + \frac{\lambda_e^2+\lambda_e}{x}\right) f_{\gamma_{E_2'}}(\lambda_e+x)\, dx, \quad \text{(A.5)}$$

where the integral in (A.5) can be obtained by taking the same steps as for deriving the integral in (A.1). Hence, the closed expression of secrecy outage probability for the satellite communication system can be easily obtained.

APPENDIX B
PROOF OF PROPOSITION 1

We utilize the Karush-Kugn-Tucker (KKT) conditions to design the optimal transmit power in problem (20), which is denoted as (P_S^*, P_R^*). The Lagrangian function associated with the problem is expressed by

$$L_1(P_S,P_R) = P_{co} + \mu_0(P_{so}-\varepsilon) - \mu_1 P_S + \mu_2(P_S - P_S^{\max}) - \mu_3 P_R + \mu_4(P_R - P_R^{\max}), \quad \text{(B.1)}$$

where μ_i, $i = 0, 1, \cdots, 4$, represents Lagrangian multiplier. The KKT conditions are given by

$$\frac{\partial L_1(P_S,P_R)}{\partial P_S} = 0, \quad \text{(B.2a)}$$
$$\frac{\partial L_1(P_S,P_R)}{\partial P_R} = 0, \quad \text{(B.2b)}$$
$$\mu_0 (P_{so} - \varepsilon) = 0, \quad \text{(B.2c)}$$
$$-\mu_1 P_S = 0, \quad \text{(B.2d)}$$
$$\mu_2 (P_S - P_S^{\max}) = 0, \quad \text{(B.2e)}$$
$$-\mu_3 P_R = 0, \quad \text{(B.2f)}$$
$$\mu_4 (P_R - P_R^{\max}) = 0, \quad \text{(B.2g)}$$
$$\mu_0, \mu_1, \mu_2, \mu_3, \mu_4 \geq 0, \quad \text{(B.2h)}$$
$$0 \leq P_B \leq P_B^{\max}, B \in \{S, R\}. \quad \text{(B.2i)}$$

Considering the achievement of transmission for the dual-hop satellite communication system, $P_S \neq 0$ and $P_R \neq 0$ so that $\mu_1 = \mu_3 = 0$. Then, conditions (B.2a) and (B.2b) can be transformed as [24, Eq.(8.356.4)]

$$\frac{\partial P_{co}}{\partial P_S} + \mu_0 \frac{\partial P_{so}}{\partial P_S} + \mu_2 = 0, \quad \text{(B.3)}$$
$$\frac{\partial P_{co}}{\partial P_R} + \mu_0 \frac{\partial P_{so}}{\partial P_R} + \mu_4 = 0. \quad \text{(B.4)}$$

Obviously, if $\mu_0 = \mu_2 = 0$ or $\mu_0 = \mu_4 = 0$, equations (B.3) and (B.4) will be not established since $\frac{\partial P_{co}}{\partial P_S} < 0$ and $\frac{\partial P_{co}}{\partial P_R} < 0$. Therefore, for the case that $\mu_0 = 0$, it should hold that $\mu_2 \neq 0$ and $\mu_4 \neq 0$, which means $P_S^* = P_S^{\max}$ and $P_R^* = P_R^{\max}$ if $P_{so}(P_S^{\max}, P_R^{\max}) \leq \varepsilon$.

Furthermore, it only needs to discuss the case that $\mu_0 \neq 0$ when $P_{so}(P_S^{\max}, P_R^{\max}) > \varepsilon$; otherwise, $(P_S^{\max}, P_R^{\max})$ will be the optimal transmit power for the dual-hop satellite communication system. In fact, the case that $\mu_0 \neq 0$ can be further divided into three cases as follows.

Case 1: If $\mu_2 = 0$ but $\mu_4 \neq 0$, it should satisfy that $P_{so}(P_S, P_R^{\max}) - \varepsilon = 0$. Since $\lim_{P_S \to 0} P_{so} = 0$, we have that $P_{so}(0, P_R^{\max}) - \varepsilon < 0$. Recalling the value of $P_{so}(P_S^{\max}, P_R^{\max})$, it can find the fact that a solution exists for the function $P_{so}(P_S, P_R^{\max}) = \varepsilon$, which may be the optimal value of P_S.

Case 2: If $\mu_2 \neq 0$ but $\mu_4 = 0$, with taking similar steps for analysis of *Case 1*, a value of P_R must be found to make $P_{so}(P_S^{\max}, P_R) = \varepsilon$, where $P_R \in (0, P_R^{\max}]$.

Case 3: If $\mu_2 = \mu_4 = 0$, optimal transmit power at the source and the relay, which relies on the constraint $P_{so} = \varepsilon$, will be lower than $P_S^{\max}$ and $P_R^{\max}$, respectively. It should highlight that the minimum value of P_{co} under this case is the largest one among the above cases.

Therefore, the proof is completed.

APPENDIX C
PROOF OF PROPOSITION 2

The Lagrangian function associated with problem in (21) is formulated as

$$L_2(P_S,P_R) = P_{so} + \mu_0(P_{co}-\varepsilon) - \mu_1 P_S + \mu_2(P_S - P_S^{\max}) - \mu_3 P_R + \mu_4(P_R - P_R^{\max}), \quad \text{(C.1)}$$

where μ_i, $i = 0, 1, \cdots, 4$, represents a Lagrangian multiplier. The Karush-Kuhn-Tucker (KKT) conditions are shown as

$$\frac{\partial L_2(P_S,P_R)}{\partial P_S} = 0, \quad \text{(C.2a)}$$
$$\frac{\partial L_2(P_S,P_R)}{\partial P_R} = 0, \quad \text{(C.2b)}$$
$$\mu_0 (P_{co} - \varepsilon) = 0, \quad \text{(C.2c)}$$
$$-\mu_1 P_S = 0, \quad \text{(C.2d)}$$
$$\mu_2 (P_S - P_S^{\max}) = 0, \quad \text{(C.2e)}$$
$$-\mu_3 P_R = 0, \quad \text{(C.2f)}$$
$$\mu_4 (P_R - P_R^{\max}) = 0, \quad \text{(C.2g)}$$
$$\mu_0, \mu_1, \mu_2, \mu_3, \mu_4 \geq 0, \quad \text{(C.2h)}$$
$$0 \leq P_B \leq P_B^{\max}, B \in \{S, R\}. \quad \text{(C.2i)}$$

In this paper, we assume that transmissions are always available. Thus, $P_S \neq 0$ and $P_R \neq 0$, leading the fact that $\mu_1 = \mu_3 = 0$. (C.2a) and (C.2b) can be rewritten as

$$\frac{\partial P_{so}}{\partial P_S} + \mu_0 \frac{\partial P_{co}}{\partial P_S} + \mu_2 = 0, \tag{C.3}$$

$$\frac{\partial P_{so}}{\partial P_R} + \mu_0 \frac{\partial P_{co}}{\partial P_R} + \mu_4 = 0. \tag{C.4}$$

Due to analysis in Section III-B, $\frac{\partial P_{so}}{\partial P_S} > 0$ and $\frac{\partial P_{so}}{\partial P_R} > 0$. Therefore, (C.3) and (C.4) can not be established, which illustrates that $\mu_0 \neq 0$ and optimal transmit power has to satisfy the condition that $P_{co}(P_S^*, P_R^*) = \varepsilon$. Note that $P_{co}(P_S^{\max}, P_R^{\max})$ is the lower boundary of COP in this problem. Hence, there will be no feasible solutions for $P_{co}(P_S^*, P_R^*) = \varepsilon$, if $P_{co}(P_S^{\max}, P_R^{\max}) > \varepsilon$. Hence, based on the above, (24) is obtained.

APPENDIX D
PROOF OF LEMMA 2

Consider that $\bar{\gamma}_B \to \infty$, where $B \in \{R, D', E_1, E_2'\}$. The cumulative distribution function (CDF) of signal-to-noise ratio (SNR) at the receiver B becomes [23, Eq. (07.20.06.0003.02)]

$$F_{\gamma_B}^{asy}(x) \approx 1 - \exp\left(-\frac{\beta_{AB}}{\bar{\gamma}_B} x\right), \tag{D.1}$$

where A represents S if $B \in \{R, E_1\}$ and A denotes R if $B \in \{D', E_2'\}$. Furthermore, it holds that $\gamma_D \approx \frac{\gamma_R \gamma_{D'}}{\gamma_R + \gamma_{D'}}$ and $\gamma_{E_2} \approx \frac{\gamma_R \gamma_{E_2'}}{\gamma_R + \gamma_{E_2'}}$ in such high-SNR regions. Thereby, the CDF of SNR at the receiver in the second phase can be approximately derived as

$$\begin{aligned} F_{\gamma_B}^{asy}(x) &= \mathbb{P}\left\{\gamma_R \leq x, \gamma_{B'} \geq \frac{\gamma_R x}{\gamma_R - x}\right\} + \mathbb{P}\left\{\gamma_R > x, \gamma_{B'} \leq \frac{\gamma_R x}{\gamma_R - x}\right\} \\ &= F_{\gamma_R}^{asy}(x) + \int_x^{\infty} f_{\gamma_R}^{asy}(t) F_{\gamma_{B'}}^{asy}\left(\frac{tx}{t-x}\right) dt, \end{aligned} \tag{D.2}$$

where $B \in \{D, E_2\}$. Since $\lim_{t \to \infty} \frac{tx}{t-x} = x$, we rewrite (D.2) as

$$\begin{aligned} F_{\gamma_B}^{asy}(x) &\approx F_{\gamma_R}^{asy}(x) + \int_x^{\infty} f_{\gamma_R}^{asy}(t) F_{\gamma_{B'}}^{asy}(x)\, dt \\ &= \bar{F}_{\gamma_R}^{asy}(x) F_{\gamma_{B'}}^{asy}(x) + F_{\gamma_R}^{asy}(x). \end{aligned} \tag{D.3}$$

Finally, inserting (D.1) and (D.3) into (9) and (10), (25) and (26) arise by setting $x = \lambda_c$ and $x = \lambda_e$, respectively.

Therefore, the proof is completed.

APPENDIX E
PROOF OF PROPOSITION 3

Based on Proposition 1 in Section III-B, we first discuss the case that transmit power at the source or relay achieves at its upper boundary, i.e., $P_S^{\max}$ or $P_R^{\max}$. When $P_S = P_S^{\max}$, it holds that

$$P_R \leq \frac{K_{RE_2}^e}{\ln\left(1 - \exp\left(\frac{K_{SE_1}^e}{P_S^{\max}}\right)\right) - \ln\left(1 - \varepsilon \exp\left(\frac{K_{SE_1}^e}{P_S^{\max}}\right)\right) - \frac{K_{SR}^e}{P_S^{\max}}}. \tag{E.1}$$

Then, when $P_R = P_R^{\max}$, we have that $P_S = \frac{K_{SR}^e}{\ln x}$, where x satisfies with the condition that

$$\varepsilon \exp\left(\frac{K_{RE_2}^e}{P_R^{\max}}\right) x^{\frac{K_{SE_1}^e}{K_{SR}^e} + 1} - x^{\frac{K_{SE_1}^e}{K_{SR}^e}} - \exp\left(\frac{K_{RE_2}^e}{P_R^{\max}}\right) x + 1 \geq 0. \tag{E.2}$$

Since the angles between satellite eavesdropper and the relay with respect to the source and between the ground eavesdropper and the destination with respect to the relay are small, (E.2) can be simplified by $\varepsilon A x^2 - (A+1)\, x + 1 \geq 0$, where $A = \exp\left(\frac{K_{RE_2}^e}{P_R^{\max}}\right)$. Hence, we have that

$$P_S \leq \frac{K_{SR}^e}{\ln\left(A + 1 + \sqrt{(A+1)^2 - 4\varepsilon A}\right) - \ln(2\varepsilon) - \frac{K_{RE_2}^e}{P_R^{\max}}}. \tag{E.3}$$

Finally, plugging the maximum value that P_S and P_R can achieve at into (25), the optimal COP arises.

Therefore, the proof for Proposition 3 is completed.

APPENDIX F
PROOF OF PROPOSITION 4

With the aid of (25), the relationship between P_S and P_R is given by

$$P_R \geq \frac{K_{RD}^c}{-\frac{K_{SR}^c}{P_S} - \ln(1-\varepsilon)}. \tag{F.1}$$

Since $\frac{\partial P_{so}^{asy}}{\partial P_R} > 0$, we insert the minimum value of P_R into (26), and then look for the minimum point. The derivative of P_{so}^{asy} with respect to P_S is derived as

$$\frac{d\, P_{so}^{asy}}{d\, P_R} = \frac{B_0}{K_{RD}^c P_S^2} \left(\frac{K_{SE_1}^e K_{RD}^c}{B_0 x_2} - \frac{B_1 x_1}{x_2 x_3} - \frac{B_2 x_1}{x_3}\right), \tag{F.2}$$

where $x_1 = \exp\left(\frac{K_{RE_2}^e K_{SR}^c}{K_{RD}^c P_S}\right)$, $x_2 = \exp\left(\frac{K_{SE_1}^e}{P_S}\right)$, $x_3 = \exp\left(\frac{K_{SR}^e}{P_S}\right)$, $B_0 = (1-\varepsilon)^{\frac{K_{RE_2}^e}{K_{RD}^c}}$, $B_1 = K_{RD}^c (K_{SE_1}^e + K_{SR}^e) - K_{RE_2}^e K_{SR}^c$ and $B_2 = K_{RE_2}^e K_{SR}^c - K_{RD}^c K_{SR}^e$.

Consider the case that each eavesdropper locates close to the legitimate receiver that he overhears, i.e., $\beta_{SR} \approx \beta_{SE_1}$ and $\beta_{RD} \approx \beta_{RE_2}$. Then, (F.2) is transformed as

$$\frac{d\, P_{so}^{asy}}{d\, P_R} = K_{SE_1}^e \frac{1 - (1-\varepsilon)^{\frac{\lambda_e}{\lambda_c}}}{P_S^2} \exp\left(-\frac{K_{SE_1}^e}{P_S}\right) > 0. \tag{F.3}$$

Next, the minimum value that P_S achieves at should be determined. Recalling (F.1), it can be easily seen that $P_S \geq -\frac{K_{SR}^c}{\ln(1-\varepsilon)}$. Similarly, the transmit power at R should be also higher than $-\frac{K_{RD}^c}{\ln(1-\varepsilon)}$.

Finally, plugging the minimum value of P_S and P_R into (30a), the optimal SOP for optimization problem in (30) arises.

REFERENCES

[1] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang, and T. Taleb, "Incentive jamming-based secure routing in decentralized internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 3000–3013, 2020.

[2] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure and energy-efficient precoding for mimo two-way untrusted relay systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3371–3386, 2021.

[4] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassiliou, "Secrecy capacity for satellite networks under rain fading," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 777–782, 2010.

[5] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Transactions on wireless communications*, vol. 11, no. 2, pp. 852–863, 2011.

[6] W. Lu, K. An, and T. Liang, "Robust beamforming design for sum secrecy rate maximization in multibeam satellite systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1568–1572, 2019.

[7] R. Wang and F. Zhou, "Physical layer security for land mobile satellite communication networks with user cooperation," *IEEE Access*, vol. 7, pp. 29 495–29 505, 2019.

[8] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2488–2501, 2019.

[9] P. Yan, Y. Zou, X. Ding, and J. Zhu, "Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5115–5128, 2020.

[10] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, and J. Wang, "Security-reliability tradeoff analysis for underlay cognitive two-way relay networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 6030–6042, 2019.

[11] Y. Zou, M. Sun, J. Zhu, and H. Guo, "Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8444–8456, 2018.

[12] M. Lin, Q. Huang, T. de Cola, J.-B. Wang, J. Wang, M. Guizani, and J.-Y. Wang, "Integrated 5g-satellite networks: A perspective on physical layer reliability and security," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 152–159, 2020.

[13] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet of things journal*, vol. 7, no. 1, pp. 33–52, 2019.

[14] L. Bai, L. Zhu, X. Zhang, W. Zhang, and Q. Yu, "Multi-satellite relay transmission in 5g: Concepts, techniques, and challenges," *IEEE Network*, vol. 32, no. 5, pp. 38–44, 2018.

[15] N. I. Miridakis, D. D. Vergados, and A. Michalas, "Dual-hop communication over a satellite relay and shadowed rician channels," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 9, pp. 4031–4040, 2014.

[16] K. Guo, D. Guo, Y. Huang, X. Wang, and B. Zhang, "Performance analysis of a dual-hop satellite relay network with hardware impairments," in *Proc. of 25th Wireless and Optical Communication Conference (WOCC)*. IEEE, 2016, pp. 1–5.

[17] R. Xu, X. Da, H. Hu, Y. Liang, and L. Ni, "Power and time slot allocation method for secured satellite transmission based on weighted fractional data carrying artificial noise," *IEEE Access*, vol. 6, pp. 65 043–65 054, 2018.

[18] R. Xu, X. Da, H. Hu, L. Ni, and Y. Pan, "A secure hybrid satellite-terrestrial communication network with af/df and relay selection," *IEEE Access*, vol. 7, pp. 171 980–171 994, 2019.

[19] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, vol. 123, pp. 77–87, 2017.

[20] A. Abdi, W. C. Lau, M.-S. Alouini, and M. Kaveh, "A new simple model for land mobile satellite channels: First-and second-order statistics," *IEEE Transactions on Wireless Communications*, vol. 2, no. 3, pp. 519–528, 2003.

[21] R. H. Y. Louie, Y. Li, H. A. Suraweera, and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 6, pp. 3132–3141, 2009. [Online]. Available: https://doi.org/10.1109/TWC.2009.080807

[22] A. M. Salhab, F. S. Al-Qahtani, S. A. Zummo, and H. M. Alnuweiri, "Performance analysis of amplify-and-forward relay systems with interference-limited destination in various rician fading channels," *Wirel. Pers. Commun.*, vol. 77, no. 3, pp. 1751–1773, 2014. [Online]. Available: https://doi.org/10.1007/s11277-014-1607-4

[23] I. Wolfram Research, *Mathematica,Version 12.1*. Champaign, IL, 2020.

[24] I. S. Gradshteyn, I. M. Ryzhik, I. S. Gradshteyn, and I. M. Ryzhik, - *Table of Integrals, Series, and Products (Eighth Edition)*, 1980, vol. 20, no. 96.