Received: 19 February 2024 | Revised: 28 March 2024 | Accepted: 16 April 2024

DOI: 10.1002/sat.1519

ORIGINAL PAPER

WILEY

Energy-efficient physical layer security schemes for low Earth orbit satellite systems

Satya Chan [1] | Sooyoung Kim [2] | Hee Wook Kim [1] | Bon-Jun Ku [1] | Daesub Oh [1]

[1]Radio and Satellite Research Division, ETRI, Daejeon, South Korea

[2]Division of Electronics Engineering, IT Convergence Research Centre, Jeonbuk National University, Jeonju, South Korea

Correspondence
Sooyoung Kim, Division of Electronics Engineering, IT Convergence Research Centre, Jeonbuk National University, Jeonju, South Korea.
Email: sookim@jbnu.ac.kr

Funding information
Institute for Information and Communications Technology Promotion Grant funded by the Korea Government (MSIT, Development of the spectrum sharing technology for Non-GSO satellite system), Grant/Award Number: 2021-0-00719; National Research Foundation of Korea (NRF) funded by the Korea government (MSIT), Grant/Award Number: NRF-2021R1A2C1003121

Summary

This paper introduces four proposals to enhance physical layer security (PLS) in low Earth orbit (LEO) satellite systems. The first proposal leverages the Alamouti code aided by artificial noise (AN) and involves the collaborative use of two LEO satellites, ensuring secure downlink transmission. Its efficiency is further enhanced when implementing a power-balanced Alamouti code. The second PLS proposal capitalizes on an reconfigurable intelligent surface (RIS) to introduce interference to potential eavesdroppers. As the RIS manages the reflected channel, this security measure is achieved without necessitating additional transmit power or receiver operations. The third proposal integrates the first and second solutions, resulting in improved secrecy rates compared to the individual proposals, nearly reaching the maximum achievable rate. The fourth proposal is based on a relay-based method, securing all transmission links from the satellite to the relay and from the satellite and relay to the legitimate user. The secrecy performance simulation results presented in the paper demonstrate the remarkable effectiveness of the proposed solutions.

KEYWORDS
artificial noise, LEO satellite, PLS, RIS, security

1 | INTRODUCTION

The advent of low Earth orbit (LEO) satellite constellations has revolutionized global connectivity, reaching even the most remote regions. LEO satellites are considered a crucial contender for the next generation of mobile communication. Consequently, the need to ensure security in mobile communication has become increasingly important. Safeguarding user information, preventing unauthorized network access, and thwarting malicious attacks on the communication infrastructure are of vital concern. The emergence of LEO satellite systems as viable options for non-terrestrial networks (NTNs) has further intensified the focus on information security.[1–3]

Traditional cryptography (TC) presents challenges, particularly regarding power consumption and computational capacity, especially for resource-constrained devices, like the internet of things (IoT) devices. Additionally, TC encryption and decryption rely on mathematical algorithms, making it theoretically impossible to reverse the encryption without the corresponding decryption key. However, due to the rapid advancement of computing power, encryption alone may no longer be sufficient to prevent unauthorized individuals from accessing and exploiting confidential information.[4]

To address the challenges of ensuring secure communication, numerous studies have proposed physical layer security (PLS) schemes for multi-antenna systems, such as space-time block coding (STBC). One common PLS method is the incorporation of artificial noise (AN).[5–14] In these

schemes, AN is strategically inserted into the null space of the legitimate channel, eliminating it at the legitimate receiving end, while introducing significant interference to any unauthorized eavesdroppers.

However, employing AN-aided techniques requires additional energy for the AN component, leading to decrease in power efficiency.[15] Furthermore, integrating AN that relies on channel characteristics can result in a high peak-to-average power ratio, which imposes a burden on the power amplifier. These two disadvantages are particularly critical for satellite systems with limited power resources and high-power amplifiers featuring non-linear characteristics. Although reducing the power of the AN can enhance power efficiency by reducing the transmit power, it also diminishes interference to eavesdroppers, potentially increasing the risk of information leakage.

Our recent preliminary study demonstrated the power efficiency of the Alamouti scheme incorporating AN.[16] This PLS scheme introduces AN in a manner that reduces the overall transmit power, eliminating the need for additional power consumption for security purposes. The study demonstrates that the proposed approach achieves comparable performance compared to the conventional AN-aided scheme, with approximately 5 dB less power, making it an excellent candidate for a satellite system.

On the other hand, the reconfigurable intelligent surface (RIS), also known as the smart surface, has garnered substantial attention in recent years as an effective means of enhancing capacity, as well as security performance.[17–22] This cutting-edge technology consists of an array of passive elements that can manipulate the phase of electromagnetic signals. These manipulations are employed to achieve the desired reflection and propagation characteristics of the signals. By dynamically controlling the reflection pattern, the RIS demonstrates its potential to amplify signal strength, alleviate interference, and vastly enhance communication performance within wireless networks.

The previous study introduced an RIS-aided PLS scheme designed for the 5G-enabled industrial IoT[18]; it demonstrated that the RIS can be efficiently used for PLS application to enhance the secrecy sum-rate of the industrial wireless network, even in the presence of eavesdroppers around the facility. In addition, the study in Qiao et al[20] proposed enhanced security for uplink transmission by integrating the RIS with an energy-harvesting jamming device. Another proposal for PLS in 6G networks also explores the utilization of RIS to enhance security for low-end IoT devices, mitigating eavesdropping and jamming attacks.[21] Additionally, a framework was proposed to analyze secrecy performance in 6G networks by leveraging RIS to mitigate signal degradation.[22] This framework evaluates various eavesdropping scenarios and secrecy metrics, highlighting the effects of fading parameters, atmospheric turbulence, and pointing errors on secrecy performance through analytical expressions and simulations. Another study in Lee et al[23] proposed a cooperative transmission using the RIS within a clustered LEO satellite communication system. Their method aimed to improve the signal-to-noise ratio (SNR) for users with a low elevation angle from a LEO satellite, which was achieved by deploying RIS on the other satellite in the same orbit.

Motivated by these investigations and considerations, this paper investigates PLS schemes tailored to LEO satellite systems. Several new PLS proposals are thoroughly explored within the context of LEO satellite systems. These proposals encompass the AN-based, RIS-aided, and relay-based methods, all aimed at enhancing communication security.

The novelty of this paper can be summarized as follows: First, an application is introduced to LEO satellite systems, namely, the Alamouti scheme with AN, to enhance security, as well as power efficiencies. Then, a novel method is presented to disturb eavesdropping attempts by introducing noisy channel to the eavesdropper using the RIS, thus ensuring data security. This method applies the novel idea of invoking interference, which makes the legitimate channel constant, while that of the eavesdropper dynamic. This study estimates the phases of the RIS elements using a well-known iterative technique called the Newton-Raphson method. Furthermore, the research introduces another novel approach to enhance transmission security in LEO satellite systems through the use of relay, with all links safeguarded by AN. Finally, this study provides security measure equations accompanied by simulation results.

The remaining sections are organized as follows: Section 2 provides insights into related works concerning the AN-based PLS scheme with the power-balanced Alamouti code and the fundamental concepts of RIS-aided security enhancement. Section 3 advances various proposals for applying PLS in the LEO satellite system, and formulates their security performance metrics in terms of secrecy capacity (SC) and secrecy rate (SR). Section 4 presents the simulation results, while Section 5 concludes the paper with a summary and discussion of the findings.

2 | RELATED WORKS

2.1 | AN-based PLS scheme with power-balanced Alamouti code

A previous study introduced a PLS scheme utilizing the Alamouti code,[9,12] and Figure 1 illustrates the system configuration. This setup consists of three primary components: Alice, the legitimate transmitter; Bob, the legitimate receiver; and Eve, the eavesdropper. In this setup, Alice is equipped with two antennae, while Bob and Eve have one antenna each. This results in a 2×1 system configuration. We assume that Alice and Bob possess access to the channel state information (CSI) $\mathbf{h} = [h_1 h_2]^T$, representing the channel vector between them. Additionally, Eve has access to the CSI $\mathbf{g} = [g_1 g_2]^T$, which characterizes the channel between Alice and Eve. It is also assumed that Eve is located at a distance of several wavelengths from Bob, ensuring the independence of $\mathbf{h}$ and $\mathbf{g}$.

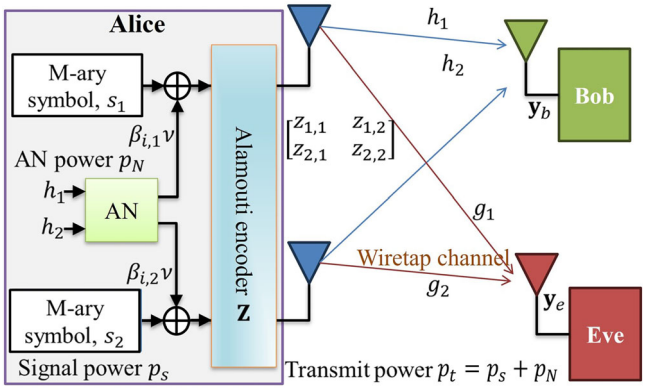

FIGURE 1 AN-added Alamouti code.

Initially, the Alamouti code involves the encoding of two signals, resulting in a 2×2 signal matrix over two consecutive time slots.[24] We denote the transmit signals to be encoded as s_1 and s_2. Consequently, the Alamouti encoded signal matrix can be represented as

$$\mathbf{S} = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}. \tag{1}$$

Next, for the AN-added Alamouti code, the encoded signal matrix across two time slots takes the following form[9–12]:

$$\mathbf{Z} = \begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix} = \mathbf{S} + \mathbf{W}, \tag{2}$$

where $\mathbf{W}$ is an AN matrix, which can be expressed as

$$\mathbf{W} = \begin{bmatrix} \beta_{1,1}\nu & \beta_{1,2}\nu \\ -(\beta_{2,1}\nu)^* & (\beta_{2,2}\nu)^* \end{bmatrix}. \tag{3}$$

The parameter $\beta_{i,k}$ represents the coefficient of ν for the ith time slot and the kth transmit antenna. Meanwhile, ν is a complex Gaussian random variable characterized by the mean of zero and unit variance.

As a result, there is a need to allocate power for the AN, denoted as p_N, in addition to the signal power, p_s. This allocation of power for AN increases the total transmit power. We note that the coefficient $\beta_{i,k}$ must be designed under the following conditions:

$$\begin{aligned} \beta_{1,1}h_1 + \beta_{1,2}h_2 &= 0, \\ \beta_{2,1}^* h_1 + \beta_{2,2}^* h_2 &= 0. \end{aligned} \tag{4}$$

Based on the above, AN will be canceled upon reception at Bob, and one of the possible set of solutions for $\beta_{i,k}$ can be expressed as

$$\beta_{1,1} = -h_2, \beta_{1,2} = h_1, \beta_{2,1} = h_2^*, \beta_{2,2} = h_1^*. \tag{5}$$

Hence, the signal vector received by Bob can be expressed as

$$\mathbf{y}_b = \begin{bmatrix} (y_b)_1 \\ (y_b)_2 \end{bmatrix} = \begin{bmatrix} h_1 s_1 + h_2 s_2 + (n_b)_1 \\ h_2 s_1^* - h_1 s_2^* + (n_b)_2 \end{bmatrix}, \tag{6}$$

where $(y_b)_i$ and $(n_b)_i$ represent the received signal and additive white Gaussian noise (AWGN) at the ith time slot at Bob, respectively. Subsequently, the detection process can be carried out in the same way as the conventional Alamouti scheme,[24] leading to

$$\begin{aligned} \hat{\mathbf{s}}_b &= \frac{1}{\|h_1\|^2 + \|h_2\|^2} \begin{bmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{bmatrix} \begin{bmatrix} (y_b)_1 \\ (y_b)_2^* \end{bmatrix} \\ &= \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \frac{1}{\|h_1\|^2 + \|h_2\|^2} \begin{bmatrix} h_1^* (n_b)_1 + h_2 (n_b)_2^* \\ h_2^* (n_b)_1 - h_1 (n_b)_2^* \end{bmatrix}. \end{aligned} \tag{7}$$

On the other hand, the signal vector received by Eve can be expressed as

$$\begin{aligned}\mathbf{y}_e &= \begin{bmatrix}(y_e)_1\\(y_e)_2\end{bmatrix}\\ &= \begin{bmatrix} g_1 s_1 + g_2 s_2 + \beta_{1,1} g_1 + \beta_{1,2} g_2 + (n_e)_1\\ g_2 s_1^* - g_1 s_2^* - \beta_{2,1} g_1 + \beta_{2,2} g_2 + (n_e)_2, \end{bmatrix},\end{aligned} \tag{8}$$

where $(y_e)_i$ and $(n_e)_i$ are the received signal and AWGN, respectively, at the ith received time slot at Eve. Similarly, the detected signal vector at Eve, $\hat{\mathbf{s}}_e$, is as follows:

$$\begin{aligned}\hat{\mathbf{s}}_e &= \frac{1}{\|g_1\|^2 + \|g_2\|^2}\begin{bmatrix} g_1^* & g_2\\ g_2^* & -g_1\end{bmatrix}\begin{bmatrix}(y_e)_1\\(y_e)_2^*\end{bmatrix}\\ &= \begin{bmatrix}s_1\\s_2\end{bmatrix} + \mathbf{w}_e + \frac{1}{\|g_1\|^2 + \|g_2\|^2}\begin{bmatrix} g_1^*(n_e)_1 + g_2(n_e)_2^*\\ g_2^*(n_e)_1 - g_1(n_e)_2^*\end{bmatrix},\end{aligned} \tag{9}$$

where $\mathbf{w}_e$ denotes the interference vector incurred by AN, which can be expressed as

$$\mathbf{w}_e = \begin{bmatrix} g_1^* \nu(g_1\beta_{1,1} + g_2\beta_{1,2}) - g_2\nu(g_1^*\beta_{2,1} - g_2^*\beta_{2,2})\\ g_2^*\nu(g_1\beta_{1,1} + g_2\beta_{1,2}) + g_1\nu(g_1^*\beta_{2,1} - g_2^*\beta_{2,2})\end{bmatrix}. \tag{10}$$

It is important to note that Eve encounters interference from the AN in the shape of $\mathbf{w}_e$, which remains independent of her SNR. This situation significantly complicates her task of extracting information.

While the above strategy effectively safeguards against unauthorized data access by introducing AN targeted at disrupting the eavesdropper's signals, it does come at the cost of requiring additional power for the AN. Since the AN operates independently of the transmitted signal, the total transmission power, p_t, equals the sum of p_s and p_N, as depicted in Figure 1. Consequently, equal power allocation to both the signal and AN components would lead to a power loss of 3 dB.

Addressing this issue, an approach called the power-balanced (PB) Alamouti method is presented to devise an AN that mitigates the overall transmission power, rather than requiring additional power allocation for security.[16] As both the transmit signal and AN are complex numbers, a method involving a signal-dependent complex AN is introduced to curtail the total transmit power. Figure 2 demonstrates the operational concept of this technique.

In this strategy, AN is initially generated in the null space of the legitimate channel, as in the previous method.[9–12] Subsequently, the phase of the AN is manipulated to reduce the amplitude of the signal. Precisely, during each time slot, the complex-valued AN vector is rotated in the opposite direction to the signal, thereby reducing the power of the transmit signal. To commence, we consider the power of AN, denoted as

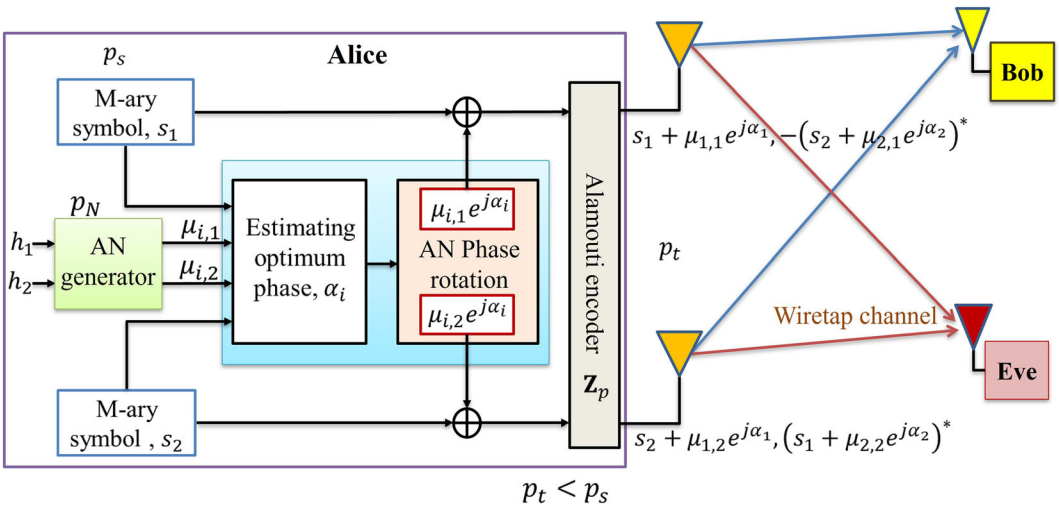

FIGURE 2 Concept of the AN-aided Alamouti coding scheme.[16]

$p_N = E[|\mu_{i,1}|^2 + |\mu_{i,2}|^2]$, where $\mu_{i,k} = \beta_{i,k}\nu$. Subsequently, the objective is to determine the optimal phase rotation for AN, which serves to minimize the overall transmit power, p_t. It is important to note that to preserve the diversity gain from the Alamouti code, the same orthogonality principle should be maintained for the AN matrix as in the encoding matrix or channel matrix. Consequently, it is imperative that ANs within the same time slot undergo identical phase rotation.

By denoting the phase rotation at the ith time slot as α_i, the encoding matrix employing the PB-Alamouti code can be expressed as

$$\mathbf{Z}' = \begin{bmatrix} z'_{1,1} & z'_{1,2} \\ z'_{2,1} & z'_{2,2} \end{bmatrix} = \mathbf{S} + \mathbf{W}' = \begin{bmatrix} s_1 + \mu_{1,1}e^{j\alpha_1} & s_2 + \mu_{1,2}e^{j\alpha_1} \\ -\left(s_2 + \mu_{2,1}e^{j\alpha_2}\right)^* & \left(s_1 + \mu_{2,2}e^{j\alpha_2}\right)^* \end{bmatrix}, \tag{11}$$

where

$$\mathbf{W}' = \begin{bmatrix} \mu_{1,1}e^{j\alpha_1} & \mu_{1,2}e^{j\alpha_1} \\ -\left(\mu_{2,1}e^{j\alpha_2}\right)^* & \left(\mu_{2,2}e^{j\alpha_2}\right)^* \end{bmatrix}. \tag{12}$$

To achieve transmit power efficiency, the following objective function is used to find the optimum phase rotation, α_i, as well as AN power, p_N.[16]

$$\underset{\alpha_i, p_N}{\operatorname{argmin}} \left((p_t)_i = \|z'_{i,1}\|^2 + \|z'_{i,2}\|^2 \right), \tag{13}$$

where $(p_t)_i$ denotes the total transmit power for the ith time slot. The solution shows that the optimal p_N is one half of p_s, and the optimal phase rotation, $\alpha_{i,\text{opt}}$, can be estimated as

$$\alpha_{i,\text{opt}} = \pi + \phi_i, \tag{14}$$

where $\phi_i = \tan^{-1}(\chi_i/\zeta_i)$ and

$$\begin{aligned} \zeta_i &= s_1^{\Re}\mu_{i,k=i}^{\Re} + s_1^{\Im}\mu_{i,k=i}^{\Im} + s_2^{\Re}\mu_{i,k\neq i}^{\Re} + s_2^{\Im}\mu_{i,k\neq i}^{\Im}, \\ \chi_i &= -s_1^{\Re}\mu_{i,k=i}^{\Im} + s_1^{\Im}\mu_{i,k=i}^{\Re} - s_2^{\Re}\mu_{i,k\neq i}^{\Im} + s_2^{\Im}\mu_{i,k\neq i}^{\Re}. \end{aligned} \tag{15}$$

The expressions $a^{\Re}$ and $a^{\Im}$ are denoted as the real and imaginary parts of a complex number a, respectively.

In summary, Alice estimates $\mathbf{W}'$ for each Alamouti coded signal pair with optimum phase rotation and AN power allocation and transmits the PB-Alamouti code. Since $\mathbf{W}'$ is designed to be located in the null space of the legitimate channel, the detected signal at Bob will be the same as (7). In contrast, the signal received by Eve encounters notable interference due to the AN. This can be expressed as

$$\mathbf{y}_e = \begin{bmatrix} g_1(s_1 - \mu_{1,1}e^{j\alpha_1}) + g_2(s_2 + \mu_{1,2}e^{j\alpha_1}) + (n_e)_1 \\ g_2\left(s_1 + \mu_{2,2}e^{j\alpha_2}\right)^* - g_1\left(s_2 + \mu_{2,1}e^{j\alpha_2}\right)^* + (n_e)_2 \end{bmatrix}. \tag{16}$$

Theoretical analysis proved that the PB-Alamouti scheme could achieve 3 dB and 6 dB power gains compared to the conventional Alamouti scheme without PLS and the conventional AN-aided Alamouti code, respectively.

2.2 | RIS-aided security enhancing

The utilization of RIS has been proposed in previous works with the primary objective of maximizing signal strength at the receiver and enhancing the security.[17–23] Unlike signals reflected from other surfaces, such as buildings, the phase of the signal reflected from the RIS can be controlled by adjusting the phases of the elements of the RIS. Significant gain is noticed when its phases are optimized.[23]

Figure 3 illustrates a system with a transmitter (Alice) and a receiver (Bob). The RIS with N elements in the system is used to enhance the signal strength received by Bob, and the control center is responsible for optimizing the phase of the RIS elements. First, the accumulated channel from Alice to Bob, h_b, can be represented as

$$h_b = \mathbf{h}_{rb}\boldsymbol{\Theta}\mathbf{h}_{ar} + h_{ab}, \tag{17}$$

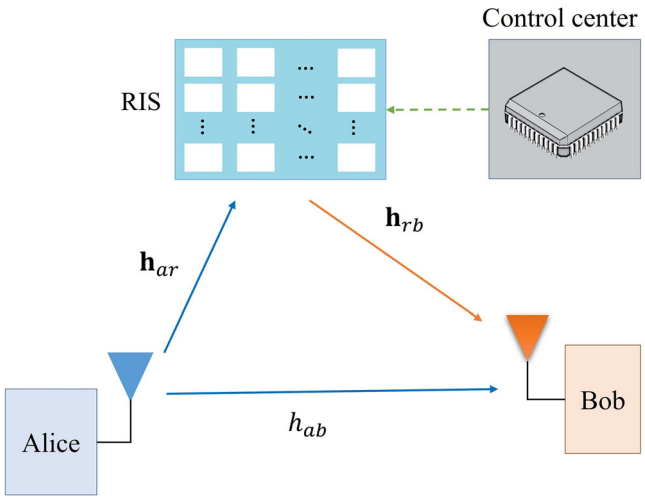

FIGURE 3 An RIS-aided system.

where $\mathbf{h}_{rb} \in \mathbb{C}^{1\times N}$ is a channel vector from the RIS to Bob, $\mathbf{h}_{ar} \in \mathbb{C}^{N\times 1}$ is a channel vector from Alice to the RIS, and h_{ab} is the direct channel from Alice to Bob. The diagonal matrix $\mathbf{\Theta} \in \mathbb{C}^{N\times N}$ is composed of the phases of the RIS elements, that is, $\mathbf{\Theta} = \text{diag}([e^{j\theta_1} e^{j\theta_2} \ldots e^{j\theta_N}])$, where $\theta_n \in [0, 2\pi)$ signifies the phase of the nth element of the RIS. To maximize the signal quality at Bob, the optimization problem can be formulated as

$$\mathbf{v}_{opt} = \underset{\mathbf{v}}{\text{argmax}} \|h_b\|^2 = \underset{\mathbf{v}}{\text{argmax}} \|\mathbf{h}_{rb}\mathbf{\Theta}\mathbf{h}_{ar} + h_{ab}\|^2, \tag{18}$$

where $\mathbf{v} = [e^{j\theta_1} e^{j\theta_2} \ldots e^{j\theta_N}]$, and $\mathbf{v}_{opt}$ is an optimal solution of $\mathbf{v}$. Since $\mathbf{h}_{rb}\mathbf{\Theta}\mathbf{h}_{ar} = \mathbf{h}_{rb}\text{diag}(\mathbf{h}_{ar})\mathbf{v}^T$, (18) can be re-expressed as[20]

$$\mathbf{v}_{opt} = \underset{\mathbf{v}}{\text{argmax}} \|\mathbf{h}_{rb}\text{diag}(\mathbf{h}_{ar})\mathbf{v}^T + h_{ab}\|^2. \tag{19}$$

For simplicity, let $\mathbf{t} = \mathbf{h}_{rb}\text{diag}(\mathbf{h}_{ar})$. Then, the solution of the above optimization problem can be given as

$$\mathbf{v}_{opt} = [e^{j(\angle h_{ab} - \angle t_1)} \ldots e^{j(\angle h_{ab} - \angle t_n)} \ldots e^{j(\angle h_{ab} - \angle t_N)}], \tag{20}$$

where $\angle x$ denotes the phase of a complex number x and t_n is the nth element of $\mathbf{t}$.

3 | EFFICIENT PLS SCHEMES FOR THE LEO SATELLITE SYSTEM

This section provides a number of new PLS application models for LEO satellite systems. In this study, we assume that Eve, the eavesdropper, is passive. Consequently, legitimate parties lack CSI concerning Eve. Additionally, we consider the channels from Alice to Bob and Alice to Eve as being independent. Table 1 presents an overview of the system configurations and techniques employed in the proposals. For instance, the first proposal targets a 2×1 system comprising two LEO satellites and one user equipment (UE), with the method based on AN.

3.1 | Cooperative PLS with two LEO satellites

Figure 4 demonstrates our first proposal of the PLS for LEO satellite systems and shows a LEO satellite configuration consisting of two satellites named Alice1 and Alice2. Bob serves as the authorized recipient, while Eve acts as the potential passive eavesdropper. It is assumed that each participant is equipped with a single antenna. Alice1 and Alice2 establish communication through either a ground-based control center or inter-satellite link. In addition, a delay compensation technique can be used to achieve synchronization between Alice1 and Alice2.[25] In this scenario, either the conventional AN-aided or PB-Alamouti scheme can be implemented to enhance security.

TABLE 1 Summary of the system configurations and PLS schemes for the proposals.

Proposal no.	MIMO configuration	PLS schemes
1	2×1, (2 LEO, 1 UE)	AN-aided, PB-Alamouti
2	1×1, (1 LEO, 1 UE)	RIS-aided
3	2×1, (2 LEO, 1 UE)	AN and RIS-aided
4	2×1, (1 LEO, 1 Relay, 1 UE)	Relay-based AN-aided

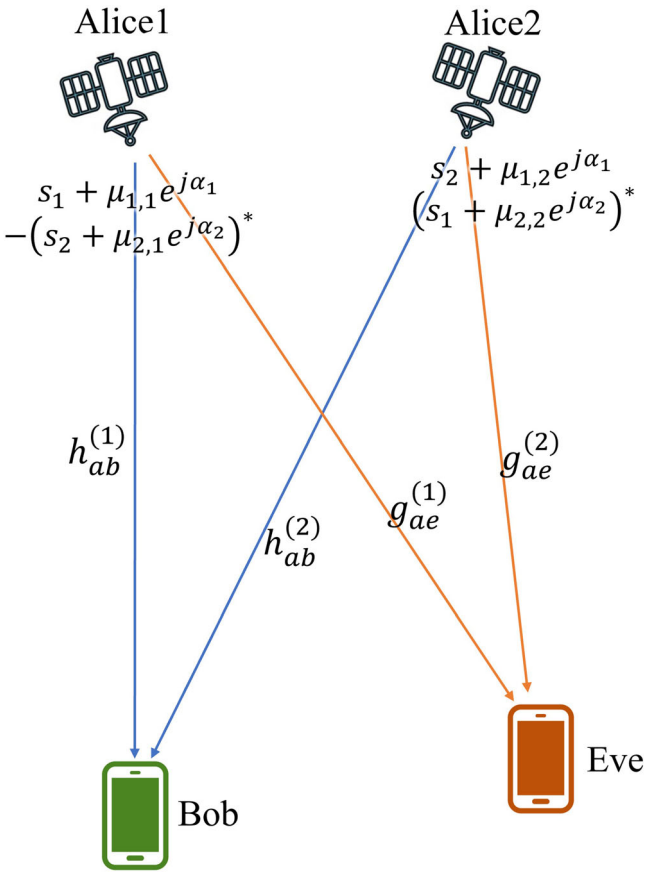

FIGURE 4 PLS with the PB-Alamouti code for LEO satellite system.

To assess the security performance of the schemes explained above, we utilize SC, as well as SR. The SC is defined as the capacity difference between Bob and Eve, as[12,15]

$$C_s = \max\{0, C_b - C_e\}, \tag{21}$$

where C_b and C_e are the capacities of Bob and Eve, respectively, and can be expressed as

$$C_b = \log_2(1 + SNR_b), \tag{22}$$

$$C_e = \log_2(1 + SNR_e), \tag{23}$$

where SNR_b and SNR_e are the SNRs at Bob and Eve, respectively, which can be estimated as

$$SNR_b = \frac{\|\mathbf{Sh}\|^2/2}{\sigma_b^2}, \tag{24}$$

$$SNR_e = \frac{\|\Lambda \mathbf{g}\|^2/2}{\|\Omega \mathbf{g}\|^2/2 + \sigma_e^2}, \tag{25}$$

where Λ and Ω are signal and AN matrices. For AN-aided scheme, $\Lambda = \mathbf{S}$ and $\Omega = \mathbf{W}$.

For the PB-Alamouti scheme, we note that the added AN, $\mathbf{W}'$ contains signal dependent information, and thus we cannot treat this as pure noise. For this reason, we decompose $\mathbf{W}'$ into signal dependent information and pure noise parts as follows:

$$\mathbf{W}' = E[\mathbf{W}'|\mathbf{S}] + \mathbf{W}'_n, \tag{26}$$

where $E[\mathbf{W}'|\mathbf{S}]$ and $\mathbf{W}'_n$ are signal dependent and pure noise parts of $\mathbf{W}'$, respectively. We note that $E[\mathbf{W}'|\mathbf{S}]$ is a constant valued matrix, and thus the eavesdropper may able to learn a discernible pattern when a substantial volume of signals is received. Conversely $\mathbf{W}'_n$ is a pure random noise component with zero mean and represents the fluctuationg component of $\mathbf{W}'$, and thus the eavesdropper cannot retieve any discernible pattern to glean information from it. Consequently, using PB-Alamouti code, $\Lambda = \mathbf{S} + E[\mathbf{W}'|\mathbf{S}]$, and $\Omega = \mathbf{W}'_n$. In addition, σ_b^2 and σ_e^2 represent the variances of the AWGN at Bob and Eve, respectively.

Moreover, the SR, denoted as R_s, was formulated by considering the difference in mutual information (MI) exchanged between Alice and Bob and Alice and Eve, respectively,[6,12] as

$$R_s = \max\{0, \mathrm{I}(\mathbf{y}_b;\mathbf{S}) - \mathrm{I}(\mathbf{y}_e;\Lambda)\}, \tag{27}$$

where $\mathrm{I}(\mathbf{y}_b;\mathbf{S})$ represents the MI at Bob and $\mathrm{I}(\mathbf{y}_e;\Lambda)$ denotes the MI at Eve.

Let S_A be a set of possible Alamouti encoding matrices $\mathbf{S}$ obtained through M-ary modulation. In this context, it can be defined as $S_A = \{\mathbf{S}_{(1)},...,\mathbf{S}_{(l)},...,\mathbf{S}_{(M^2)}\}$, where $\mathbf{S}_{(l)}$ represents the lth element within the set S_A. Then, the MI between Alice and Bob can be estimated as[12]

$$\mathrm{I}(\mathbf{y}_b;\mathbf{S}) = \log_2 M - \frac{1}{2M^2}\sum_{l}^{M^2} \mathbb{E}_{\mathbf{h},\mathbf{n}_b}\left(\log_2 \sum_{q}^{M^2} (\psi_b)_{l,q}\right), \tag{28}$$

where $\mathbb{E}_{\mathbf{h},\mathbf{n}_b}[\cdot]$ represents an expected operation with respect to the variables $\mathbf{h}$ and $\mathbf{n}_b$. Furthermore,

$$(\psi_b)_{l,q} = \exp(-(|\mathbf{d}_b + \mathbf{n}_b|^2 - |\mathbf{n}_b|^2)/\sigma_b^2), \tag{29}$$

where $\mathbf{d}_b = (\mathbf{S}_{(l)} - \mathbf{S}_{(q)})\mathbf{h}$. Likewise, for AN-aided Alamouti scheme,

$$\mathrm{I}(\mathbf{y}_e;\Lambda) = \log_2 M - \frac{1}{2M^2}\sum_{l}^{M^2} \mathbb{E}_{\mathbf{g},\mathbf{n}'_e}\left(\log_2 \sum_{q}^{M^2} (\psi_e)_{l,q}\right), \tag{30}$$

where $\mathbf{n}'_e = \Omega\mathbf{g} + \mathbf{n}_e$, and $(\psi_e)_{l,q} = \exp(-(\|\mathbf{d}_e + \mathbf{n}'_e\|^2 - \|\mathbf{n}'_e\|^2)/{\sigma_e}'^2)$, and $\mathbf{d}_e = (\Lambda_{(l)} - \Lambda_{(q)})\mathbf{g}$, where $\Lambda_{(l)} = \mathbf{S}_{(l)}$, and $\Lambda_{(l)} = \mathbf{S}_{(l)} + E[\mathbf{W}'|\mathbf{S}_{(l)}]$ for AN-aided and PB-Alamouti schemes, respectively. Note that ${\sigma_e}'^2$ represents the variance of $\mathbf{n}'_e$, which can be expressed as ${\sigma_e}'^2 = E[\mathbf{n}'^H_e \mathbf{n}'_e]$.

3.2 | RIS-aided interference invoking PLS

The second proposal of the PLS for LEO satellite systems is to utilize RIS to invoke interference to Eve. In Figure 5, a LEO satellite system is composed of a transmitter (Alice) with a single antenna, a legitimate receiver (Bob), and an eavesdropper (Eve), each equipped with one antenna. Furthermore, this system is furnished with an RIS consisting of N elements. In this context, the RIS is assumed to be controlled by the control center, enabling it to enhance signal strength at Bob, while simultaneously disrupting signals at Eve.

In order to achieve this purpose, the proposed method introduces random noise to Eve, while maintaining constant amplitude at Bob during the coherent time when all channels are assumed to be constant. Therefore, we frequently randomize the phases of the RIS elements, Θ, in order to invoke interference to Eve, but not to Bob. In other words, Θ must be designed under the constraint of Bob's channel, that is, infinite number of solutions of Θ. In the following, we will elaborate on how we can have infinite solutions for Θ to induce a noisy channel at Eve while ensuring Bob's channel remains constant. The channel parameters within this system are outlined as in Section 2.2: h_{ab} denotes the direct channel between

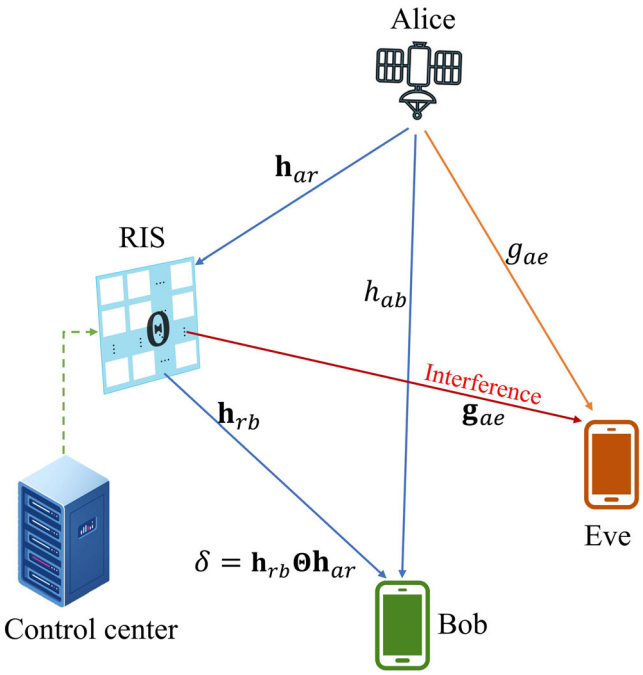

FIGURE 5 Interference invoking using RIS for LEO satellite system.

Alice and Bob, $\mathbf{h}_{ar}$ represents the channel between Alice and the RIS, $\mathbf{h}_{rb}$ is the channel between the RIS and Bob, g_{ae} is the direct channel between Alice and Eve, and $\mathbf{g}_{re}$ represents the channel between the RIS and Eve.

The signal received at Bob can be expressed as

$$y_b = (\mathbf{h}_{rb}\Theta\mathbf{h}_{ar} + h_{ab})s + n_b \tag{31}$$

where s is the transmit signal and n_b is the AWGN at Bob. Correspondingly, the signal received by Eve can be represented as

$$y_e = (\mathbf{g}_{re}\Theta\mathbf{h}_{ar} + g_{ae})s + n_e, \tag{32}$$

where n_e represents the AWGN at Eve.

Since we assume that Eve attempts to covertly eavesdrop on the signal transmitted by Alice, the control center cannot regulate the signal strength at Eve. Instead, we focus on optimizing the phases of the RIS elements to maximize the signal strength received by Bob. To use the RIS to invoke interference, the phases of the RIS elements should be randomized, creating a random channel from the RIS to the eavesdroppers. In this way, the RIS functions as a jamming device against Eve. To achieve this goal, we maintain the channel of Bob as constant for a coherence time, while that of Eve remains random. According to (17) and (20), the optimum accumulated channel from Alice to Bob can be simply expressed as

$$\mathbf{h}_{rb}\Theta_{opt}\mathbf{h}_{ar} + h_{ab} = \delta_{max} + h_{ab}, \tag{33}$$

where $\Theta_{opt} = \text{diag}(\mathbf{v}_{opt})$ and $\delta_{max} = \mathbf{h}_{rb}\Theta_{opt}\mathbf{h}_{ar}$ can be interpreted as the optimal reflected channel coefficient, which is achieved using (20). With δ_{max}, Bob can achieve the maximum accumulated channel capacity. Since there is only a single solution of Θ to achieve δ_{max}, which is Θ_{opt}, Θ_{opt} is static during the coherence time, and thus, it cannot be used to invoke random interference to Eve.

To solve the above problem, we use a constant reflected channel coefficient δ at Bob, with which the channel gain at Eve will be random during the coherence time. In other words,

$$\delta = \mathbf{h}_{rb}\Theta\mathbf{h}_{ar}. \tag{34}$$

We note that if $|\delta| > |\delta_{max}|$, (34) has no solution; while if $|\delta| < |\delta_{max}|$, it has an infinite number of solutions. Therefore, the proposed method sets $|\delta| < |\delta_{max}|$ and utilizes multiple solutions of Θ to cause the dynamic interference at Eve. In this condition, δ remains a constant value during the coherence time, and Bob can simply detect the signal without any knowledge of Θ.

In this paper, we propose to use the Newton-Raphson method to find multiple solutions of $\boldsymbol{\Theta}$ as detailed in Appendix A. We can find multiple $\boldsymbol{\Theta}$ values with their respective initial conditions of the Newton-Raphson method. As we frequently adjust $\boldsymbol{\Theta}$ using its random multiple solutions for (34), Eve will experience noisy channel. In other words, the reflected channel at Eve, $\mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar}$, is not deterministic leading to serious interference to Eve. Therefore, high-security protection can be achieved.

To derive the SC and SR, we denote $\tilde{g}_{\boldsymbol{\Theta}}$ as the knowledge of Eve about her reflected channel. The SNR at Bob and Eve can then be expressed as follows:

$$SNR_b = \frac{\|(\delta + h_{ab})s\|^2}{\sigma_b^2}, \tag{35}$$

$$SNR_e = \frac{\|(\tilde{g}_{\boldsymbol{\Theta}} + g_{ae})s\|^2}{\|(\tilde{g}_{\boldsymbol{\Theta}} - \mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar})s\|^2 + \sigma_e^2}. \tag{36}$$

Then, the SC for this proposal can be estimated by inserting the above into (21)–(23).

To estimate the SR, we define S_r as a set of M-ary modulation symbols, that is, $S_r = \{s_{(1)},\ldots,s_{(l)},\ldots,s_{(M)}\}$. Then, the MI between Alice and Bob can be formulated as

$$\mathrm{I}(y_b;s) = \log_2 M - \frac{1}{M}\sum_{l}^{M} \mathbb{E}_{h_{ab},n_b}\left(\log_2 \sum_{q}^{M} (\tilde{\psi}_b)_{l,q}\right), \tag{37}$$

where $(\tilde{\psi}_b)_{l,q} = \exp(-(|(\delta + h_{ab})(s_{(l)} - s_{(q)}) + n_b|^2 - |n_b|^2)/\sigma_b^2)$. Likewise,

$$\mathrm{I}(y_e;s) = \log_2 M - \frac{1}{M}\sum_{l}^{M} \mathbb{E}_{\tilde{g}_{ae},\tilde{n}_e}\left(\log_2 \sum_{q}^{M} (\tilde{\psi}_e)_{l,q}\right), \tag{38}$$

where $\tilde{g}_{ae} = \tilde{g}_{\boldsymbol{\Theta}} + g_{ae}$, $(\tilde{\psi}_e)_{l,q} = \exp(-(|\tilde{g}_{ae}(s_{(l)} - s_{(q)}) + \tilde{n}_e|^2 - |\tilde{n}_e|^2)/\tilde{\sigma}_e^2)$ and $\tilde{n}_e = (\mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar} - \tilde{g}_{\boldsymbol{\Theta}})s_{(l)} + n_e$, and $\tilde{\sigma}_e^2$ is a variance of $\tilde{n}_e$. Then, the SR for this proposal can be estimated by inserting the above into (27).

3.3 | Integration of AN and the RIS-aided PLS

The third proposal is to integrate the first and second proposals. Figure 6 depicts a LEO satellite system equipped with an AN-aided PLS scheme, for example, the PB-Alamouti scheme in combination with RIS. In this scenario, the security protection is provided from two sources, that is, the AN from the satellites and the interference from the RIS. For the formulation, we redefine the channel variables as $h_{ab}^{(1)}$ and $h_{ab}^{(2)}$, which are denoted as the direct channels from Alice1 and Alice2, respectively, to Bob. Similarly, we denote $g_{ae}^{(1)}$ and $g_{ae}^{(2)}$ as the direct channels from Alice1 and Alice2, respectively, to Eve. The channel vectors from Alice1 and Alice2 to the RIS are denoted as $\mathbf{h}_{ar}^{(1)}$ and $\mathbf{h}_{ar}^{(2)}$, respectively. Finally, $\mathbf{h}_{rb}$ and $\mathbf{g}_{re}$ represent the channel vectors from the RIS to Bob and Eve, respectively.

The received signal vector at Bob can be represented as

$$\mathbf{y}_b = \mathbf{S}\check{\mathbf{h}} + \mathbf{n}_b = \begin{bmatrix} \check{h}_1 s_1 + \check{h}_2 s_2 + (n_b)_1 \\ \check{h}_2 s_1^* - \check{h}_1 s_2^* + (n_b)_2 \end{bmatrix}, \tag{39}$$

where

$$\check{h}_i = \mathbf{h}_{rb}\boldsymbol{\Theta}\mathbf{h}_{ar}^{(i)} + h_{ab}^{(i)} = \delta^{(i)} + h_{ab}^{(i)}, \tag{40}$$

and $|\delta^{(i)}| < |\delta_{max}^{(i)}|$, $\delta_{max}^{(i)} = \mathbf{h}_{rb}\boldsymbol{\Theta}_{opt}\mathbf{h}_{ar}^{(i)}$ and $\check{\mathbf{h}} = [\check{h}_1 \check{h}_2]^T$. In addition, the received signal vector at Eve can be expressed as

$$\mathbf{y}_e = \Lambda\grave{\mathbf{g}} + \check{\mathbf{n}}_e, \tag{41}$$

where $\grave{\mathbf{g}} = \mathbf{g}_{\boldsymbol{\Theta}} + [g_{ae}^{(1)} g_{ae}^{(2)}]^T$ and $\mathbf{g}_{\boldsymbol{\Theta}}$ is the knowledge of Eve regarding her reflected channel vector. The variable $\check{\mathbf{n}}_e$ is denoted as an accumulated interference-plus-noise vector at Eve, which can be expressed as

$$\check{\mathbf{n}}_e = \dot{\mathbf{n}}_e + \ddot{\mathbf{n}}_e + \mathbf{n}_e, \tag{42}$$

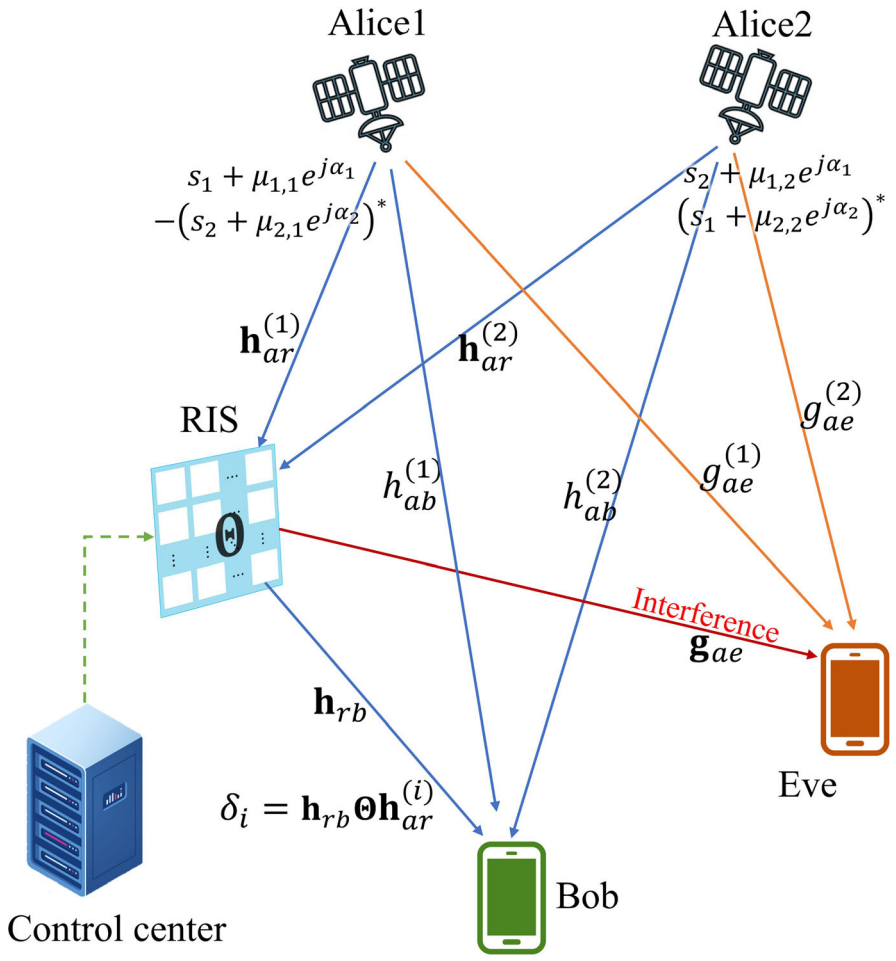

FIGURE 6 PLS with the PB-Alamouti code and RIS for LEO satellite system.

where $\dot{\mathbf{n}}_e$ is the received noise vector caused by the AN, $\ddot{\mathbf{n}}_e$ is the interference vector received from the RIS, and $\mathbf{n}_e$ is the AWGN vector. The noise vector $\dot{\mathbf{n}}_e$ can be expressed as

$$\dot{\mathbf{n}}_e = \boldsymbol{\Omega}\check{\mathbf{g}}, = \boldsymbol{\Omega}\begin{bmatrix}\check{g}_1\\ \check{g}_2\end{bmatrix}, \tag{43}$$

where $\check{g}_i = \mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar}^{(i)} + g_{ae}^{(i)}$, and,

$$\ddot{\mathbf{n}}_e = \boldsymbol{\Lambda}\ddot{\mathbf{g}} = \boldsymbol{\Lambda}\left(\mathbf{g}_{\boldsymbol{\Theta}} - \begin{bmatrix}\mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar}^{(1)}\\ \mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar}^{(2)}\end{bmatrix}\right). \tag{44}$$

The SC of this integrated system can be estimated by inserting the following SNR values of Bob and Eve, respectively into (21)–(23):

$$SNR_b = \frac{\|\mathbf{S}\check{\mathbf{h}}\|^2/2}{\sigma_b^2}, \tag{45}$$

$$SNR_e = \frac{\|\boldsymbol{\Lambda}\,\mathbf{g}\|^2/2}{\|\boldsymbol{\Omega}\check{\mathbf{g}} + \boldsymbol{\Lambda}\ddot{\mathbf{g}}\|^2/2 + \sigma_e^2}. \tag{46}$$

Likewise, the SR can be estimated by using the following MI at Bob and Eve, respectively. First, the MI at Bob can be represented as

$$\mathrm{I}(\mathbf{y}_b;\mathbf{S}) = \log_2 M - \frac{1}{2M^2}\sum_{l}^{M^2}\mathbb{E}_{\check{\mathbf{h}},\mathbf{n}_b}\left(\log_2\sum_{q}^{M}(\check{\psi}_b)_{l,q}\right), \tag{47}$$

where $(\breve{\psi}_b)_{l,q} = \exp(-(|\breve{\mathbf{d}}_b + \mathbf{n}_b|^2 - |\mathbf{n}_b|^2)/\sigma_b^2)$, and $\breve{\mathbf{d}}_b = (\mathbf{S}_{(l)} - \mathbf{S}_{(q)})\breve{\mathbf{h}}$. Furthermore, the MI at Eve can be estimated as follows:

$$\mathrm{I}(\mathbf{y}_e;\boldsymbol{\Lambda}) = \log_2 M - \frac{1}{2M^2}\sum_{l}^{M^2}\mathbb{E}_{\mathbf{g},\breve{\mathbf{n}}_e}\left(\log_2\sum_{q}^{M}(\breve{\psi}_e)_{l,q}\right), \tag{48}$$

where $(\breve{\psi}_e)_{l,q} = \exp(-(|\breve{\mathbf{d}}_e + \breve{\mathbf{n}}_e|^2 - |\breve{\mathbf{n}}_e|^2)/\breve{\sigma}_e^2)$, $\breve{\mathbf{d}}_e = (\boldsymbol{\Lambda}_{(l)} - \boldsymbol{\Lambda}_{(q)})\,\mathbf{g}$, and $\breve{\sigma}_e^2$ is the variance of $\breve{\mathbf{n}}_e$. The SR can then be estimated by inserting the above MI at Bob and Eve into (27).

3.4 | AN-aided PLS with relay

The fourth proposal is for the system using terrestrial relay components. Figure 7 illustrates a satellite communication configuration featuring a relay component. In this setup, we assume that the channel gain for the direct path between Alice and Bob, h_1, is much weaker, compared to the channel gains for the paths connecting Alice to the relay, and from the relay to Bob, h_R and h_2, respectively. Therefore, this scenario assumes the significant role played by the relay in enhancing the signal quality received by Bob.

As a result, the relay holds a crucial position in maintaining a secure communication link between Alice and Bob. To put this system into operation, we employ a time division scheme. Time is partitioned into four distinct time slots, labeled τ_1–τ_4. During time slots τ_1 and τ_2, Alice transmits signals $s_1 + \mu_{1,2}e^{j\alpha_1}$ and $s_2 + \mu_{2,2}e^{j\alpha_2}$ to the relay. Time slots τ_3 and τ_4 are designated for the transmission of PB-Alamouti-coded signals from both Alice and the relay to Bob.

It is worth noting that even if Eve attempts to intercept the signal from Alice to the relay during time slots τ_1 and τ_2, she will still be subject to the adverse effects of the AN, which ultimately guarantees a secure link in each time slot. In this scenario, Alice requires access to channel information pertaining to the connections between her and Bob, as well as between the relay and Bob. This information is crucial for her to design the AN. To this end, the AN for the PB-Alamouti code can be designed as in Section 2.1, which is a function of h_1 and h_2. At τ_1 and τ_2, the signal received at the relay can be expressed as

$$\mathbf{y}_R = \begin{bmatrix} h_R(s_1 + \mu_{1,2}e^{j,\alpha_1}) + (n_R)_1 \\ h_R(s_2 + \mu_{2,2}e^{j,\alpha_2})^* + (n_R)_2 \end{bmatrix}, \tag{49}$$

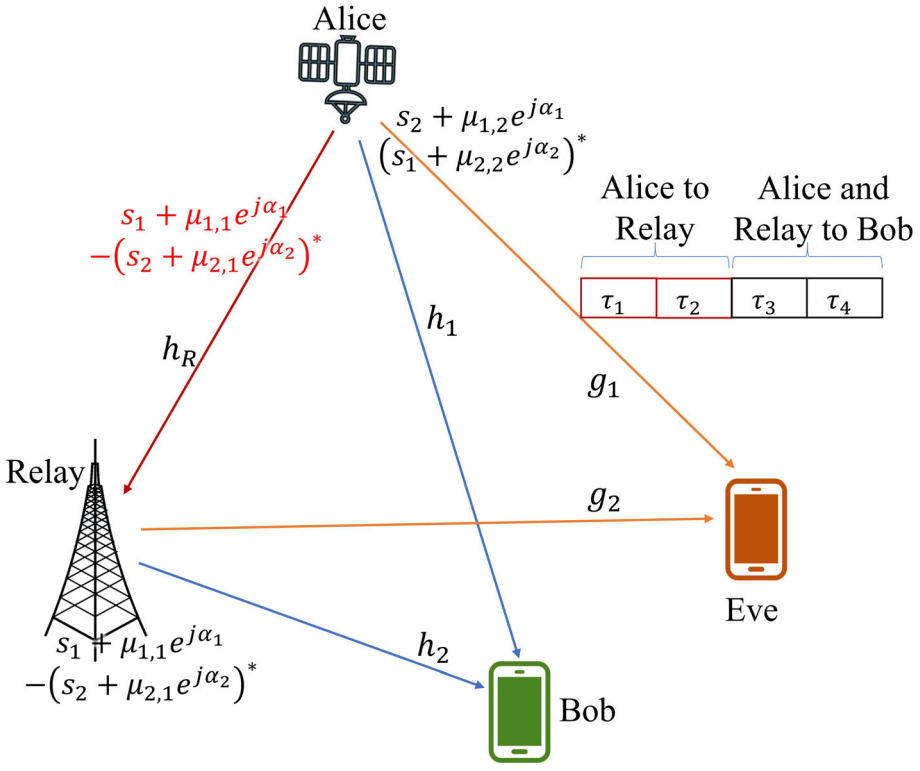

FIGURE 7 Relay-based PB-Alamouti code for LEO satellite system.

where $(n_R)_1$ and $(n_R)_2$ are the AWGN of the relay at τ_1 and τ_2, respectively. The relay does not involve the direct detection of the original signals. Instead, it focuses on identifying the signals sent by Alice by effectively eliminating the channel coefficient from the received signals. As a result, the detected signal at the relay can be written as

$$\mathbf{s}_R = \frac{\mathbf{y}_R}{h_R} = \begin{bmatrix} s_2 + \mu_{1,2} e^{j,\alpha_1} + (\tilde{n}_R)_1 \\ \left(s_1 + \mu_{2,2} e^{j,\alpha_2}\right)^* + (\tilde{n}_R)_2 \end{bmatrix}, \tag{50}$$

where $(\tilde{n}_R)_i = \frac{(n_R)_i}{h_R}$.

The signal matrix at τ_3 and τ_4 can be expressed as

$$\mathbf{Z}_R = \mathbf{S} + \boldsymbol{\Omega} + \begin{bmatrix} 0 & (\tilde{n}_R)_1 \\ 0 & (\tilde{n}_R)_2 \end{bmatrix} \tag{51}$$

Next, the received signal vector at Bob can be written as

$$\begin{aligned} \acute{}\mathbf{y}_b &= \begin{bmatrix} (\acute{y}_b)_1 \\ (\acute{y}_b)_2 \end{bmatrix} = \mathbf{Z}_R \mathbf{h} \\ &= \begin{bmatrix} h_1 s_1 + h_2 s_2 + h_2 (\tilde{n}_R)_1 + (n_b)_1 \\ h_2 s_1 - h_1 s_2^* + h_2 (\tilde{n}_R)_2 + (n_b)_2 \end{bmatrix}, \end{aligned} \tag{52}$$

where $\mathbf{h} = [h_1 h_2]^T$ and h_1 and h_2 are the channel gains from Alice and the relay to Bob, respectively. Likewise, the received signal vector at Eve can be expressed as

$$\begin{aligned} \acute{}\mathbf{y}_e &= \begin{bmatrix} (\acute{y}_e)_1 \\ (\acute{y}_e)_2 \end{bmatrix} = \mathbf{Z}_R \mathbf{g} \\ &= \begin{bmatrix} g_1 (s_1 - \mu_{1,1} e^{j\alpha_1}) + g_2 (s_2 + \mu_{1,2} e^{j\alpha_1}) \\ g_2 \left(s_1 + \mu_{2,2} e^{j\alpha_2}\right)^* - g_1 \left(s_2 + \mu_{2,1} e^{j\alpha_2}\right)^* \end{bmatrix} + \begin{bmatrix} g_2 (\tilde{n}_R)_1 + (n_e)_1 \\ g_2 (\tilde{n}_R)_2 + (n_e)_2 \end{bmatrix}, \end{aligned} \tag{53}$$

where $\mathbf{g} = [g_1 g_2]^T$, and g_1 and g_2 are the channel gains from Alice and the relay to Eve, respectively.

Due to the utilization of the relay, the SC and SR will be influenced by $(\tilde{n}_R)_i$ in addition to the receiver noise. By adding the noise term transmitted from the relay, the capacities at Bob and Eve can be expressed as

$$C_b = \log_2 \left(1 + \frac{\|\mathbf{Sh}\|^2 / 2}{\|h_2 / h_R\|^2 \sigma_R^2 + \sigma_b^2}\right), \tag{54}$$

$$C_e = \log_2 \left(1 + \frac{\|\boldsymbol{\Lambda}\mathbf{g}\|^2 / 2}{\|\boldsymbol{\Omega}\mathbf{g}\|^2 / 2 + \|g_2 / h_R\|^2 \sigma_R^2 + \sigma_e^2}\right), \tag{55}$$

where σ_R^2 is the noise variance at the relay. Accordingly, the SC can be estimated using (21).

On the other hand, the MI at Bob can be expressed as

$$\mathrm{I}(\mathbf{y}_b; \mathbf{S}) = \log_2 M - \frac{1}{2M^2} \sum_{l}^{M^2} \mathbb{E}_{\acute{\mathbf{H}}, \mathbf{n}_b} \left(\log_2 \sum_{q}^{M^2} (\psi_b)_{l,q} \right), \tag{56}$$

where $\acute{}\mathbf{n}_b = h_2 / h_R \mathbf{n}_R + \mathbf{n}_b$. The variable $(\psi_b)_{l,q} = \exp(-(|\mathbf{d}_b + \acute{}\mathbf{n}_b|^2 - |\mathbf{n}_b|^2) / \sigma_b^2)$, where $\acute{}\sigma_b^2 = \|h_2 / h_R\|^2 \sigma_R^2 + \sigma_b^2$. Likewise, the MI at Eve can be expressed as

$$\mathrm{I}(\mathbf{y}_e; \boldsymbol{\Lambda}) = \log_2 M - \frac{1}{2M^2} \sum_{l}^{M^2} \mathbb{E}_{\acute{\mathbf{H}}, \mathbf{n}_e} \left(\log_2 \sum_{q}^{M^2} (\psi_e)_{l,q} \right), \tag{57}$$

where $\acute{}\mathbf{n}_e = \boldsymbol{\Omega}\mathbf{g} + g_2 / h_R \mathbf{n}_R + \mathbf{n}_e$, $(\psi_e)_{l,q} = \exp(-(|\mathbf{d}_e + \acute{}\mathbf{n}_e|^2 - |\mathbf{n}_e|^2) / \sigma_e^2)$, and $\acute{}\sigma_e^2$ is the variance of $\acute{}\mathbf{n}_e$. Finally, the SR can be estimated by inserting the above MI at Bob and Eve into (27).

4 | SIMULATION RESULTS

To assess the performance of each method, we present simulation results related to secrecy, specifically the SC and SR, using the following system configuration. The system operates at the 12 GHz frequency band and has satellites positioned at an altitude of 1000 km. The transmit antenna gain is fixed at 30 dBi, and the received antenna gains and noise spectral densities for all receiving components are uniformly set to 5 dBi and −200 dBW/Hz, respectively. Additionally, loss of 5 dB, for example, rain fading, is applied to all the links from the satellite.

Table 2 summarizes the simulation setup for all the PLS methods proposed in this paper, along with their corresponding figure numbers showing the security performances. The channels from satellite to all the ground components are assumed to be Rician fading channels with Rician factor K, having uniform probability density function (PDF), $\mathcal{U}(5,15)$ dB for the systems in Sections 3.1,3.2, and 3.3, where $\mathcal{U}(a,b)$ represents uniform PDF in the range $(a$ to $b)$. For the simulation of the method described in Section 3.4, we purposely assume the channel between the satellite and the relay to be Gaussian and that between the satellite and the user to be a Rician fading channel with Rician factor K, having $\mathcal{U}(-3,3)$ dB to make the channel between the satellite and relay better than that from the satellite to the user. On the other hand, the channels between all the ground components are assumed to be Rayleigh fading channels.

Furthermore, the modulation schemes used in the simulation include both quadrature phase shift keying (QPSK) and 16-quadrature amplitude modulation (16-QAM). We note that in all the simulations with AN-based methods, the AN power is set to be equal to the transmit signal power. In addition, we assume that the RIS is mounted on a building or tower, for all systems utilizing RIS technology. The distances from the RIS to both Bob and Eve are fixed at 500 meters, respectively, and the number of RIS elements is set to 200.

In the system model of the first proposal, which involves the joint use of two satellites, two PLS methods, namely, the AN-aided and PB-Alamouti schemes, are applicable. Figures 8 and 9 show the secrecy performance for this proposal. Figures 10 and 11 depict the performances

TABLE 2 PLS methods, channel models used in the simulation, and figure numbers for the results.

Proposal no.	PLS method	Channel model	Fig. no.
1 (Section 3.1)	AN-aided	Rician, $K \in \mathcal{U}(5,15)$ dB	8 and 9
	PB-Alamouti		
2 (Section 3.2)	RIS-aided	From Sat.: Rician, $K \in \mathcal{U}(5,15)$ dB,	10 and 11
3 (Section 3.3)	RIS + AN-aided	RIS to user: Rayleigh	12 and 13
	RIS-aided + PB-Alamouti		14 and 15
4 (Section 3.4)	Relay-based	Sat. to relay: Gaussian,	16 and 17
		Sat. to user: Rician, $K \in \mathcal{U}(-3,3)$ dB,	
		Relay to user: Rayleigh	

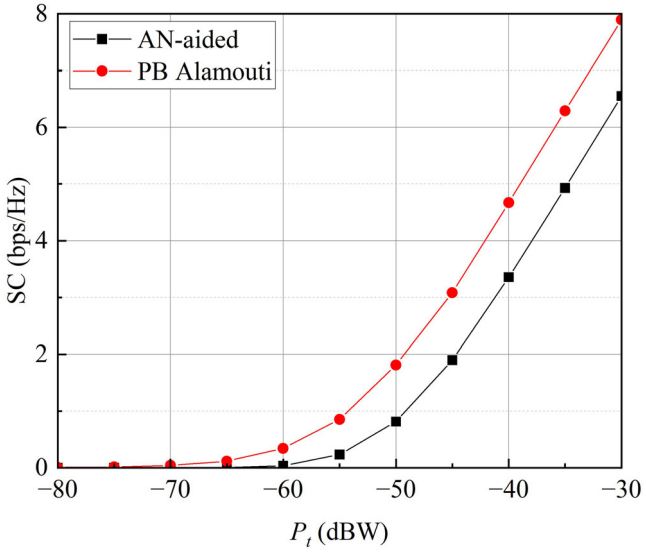

FIGURE 8 Comparison of secrecy capacity for PLS schemes using AN-aided and PB-Alamouti code in LEO satellite system.

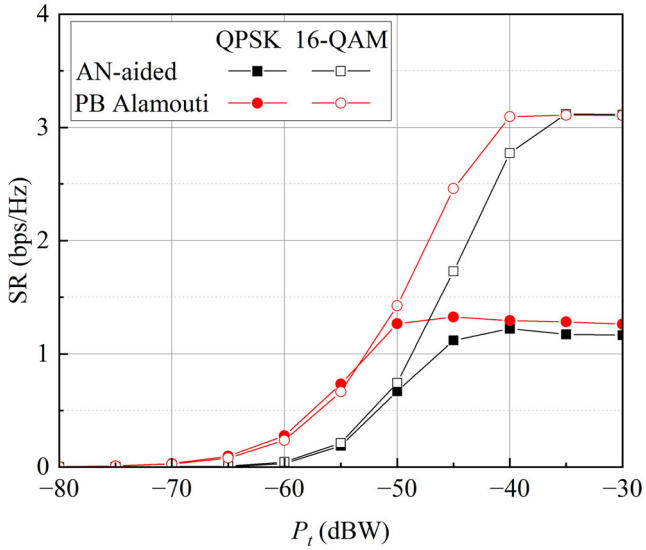

FIGURE 9 Comparison of secrecy rate for PLS schemes using AN-aided and PB-Alamouti code in LEO satellite system.

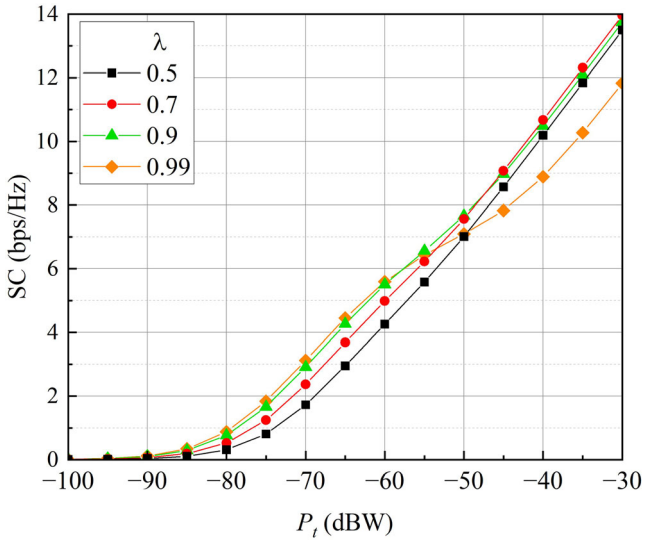

FIGURE 10 Comparison of secrecy capacity of the RIS-aided PLS for LEO satellite system according to λ

of the second proposal, which is the RIS-aided PLS scheme. For the third proposal, two options are applicable to its system model, that is, the integration of RIS, and either the AN-aided or PB-Alamouti method. Figures 12—15 present the results for the third proposal. Lastly, Figures 16 and 17 show the results for the fourth proposal, which utilizes a relay-based technique, that is compatible with the AN-aided and PB-Alamouti methods.

Figures 8 and 9 depict the SC and SR performances of the first proposal, respectively, detailed in Section 3.1. The results demonstrate the feasibility of applying both the AN-aided and PB-Alamouti schemes to this system. Notably, the PB-Alamouti scheme consistently outperforms the AN-aided scheme, due to its efficient phase rotation capability, providing a power gain of approximately 3.5 dB, as shown in Figure 8. Given the passive nature of Eve, it is conceivable that the SNR at Eve may eventually surpass that at Bob. As a result, the SR, as presented in Figure 9, offers valuable insights into the actual level of secrecy achievable. Similarly, it is observed that PB-Alamouti yields higher SR than the AN-aided scheme in the low-power region. Specifically, it delivers approximately 3.5 dB of power gain, as reported for the SC performance. However, both methods attain almost the same SR when they reach their saturation points.

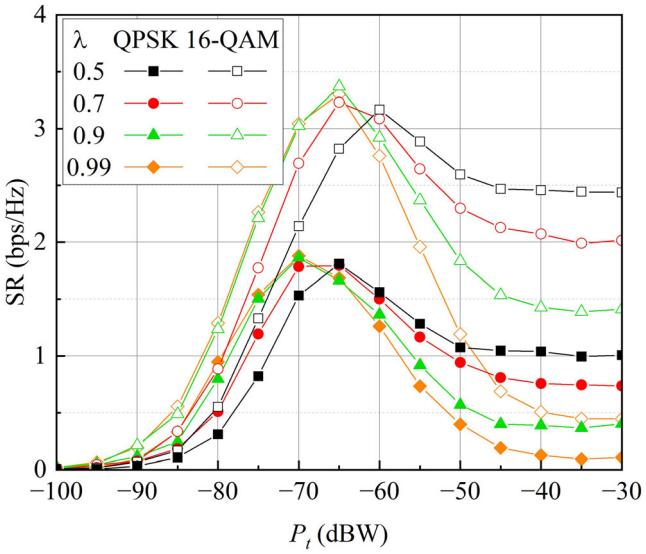

FIGURE 11 Comparison of secrecy rate of the RIS-aided PLS for LEO satellite system according to λ

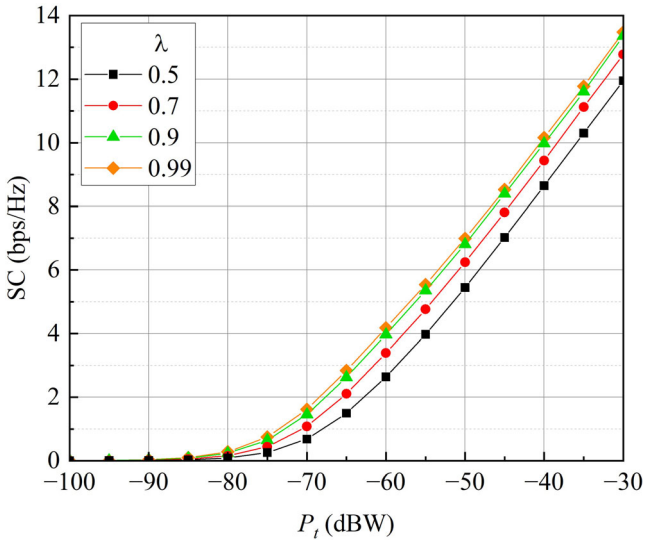

FIGURE 12 Comparison of secrecy capacity of the integrated RIS and AN-aided PLS for LEO satellite system according to λ

Figures 10 and 11 illustrate the SC and SR performances of the second proposal, respectively, described in Section 3.2. In the simulation, we assume that the knowledge of Eve on her reflected channel is the average value, that is, $\bar{g}_{\boldsymbol{\Theta}} = \mathbb{E}_{\boldsymbol{\Theta}}[\mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{h}_{ar}]$. The secrecy analysis is conducted under various $\lambda < 1$, where $\delta = \lambda\delta_{\max}$, and λ is a factor to indicate the ratio of the roles played by the RIS. In other words, λ is the ratio of the function as increasing gain at Bob, to the function as invoking interference to Eve. Therefore, λ of 0.5 implies that the RIS equally focuses on increasing gain at Bob, and invoking interference to Eve.

Referring to the SC performance in Figure 10, the SC with λ of 0.7 slightly outperforms the others, although the SC values are quite similar in the range of λ of 0.5 to 0.9. It is important to note that in the high transmit power region, an excessive increase in λ leads to performance degradation. Since we assume the same power condition for Bob and Eve, to have proper security protection, the effect of interference should be stronger in higher power condition. Additionally, high value of λ implies that the function of RIS is more focused on amplifying the channel gain of Bob, rather than interfering Eve. Therefore, under such conditions, the channel variations at Eve become smaller. For example, when $P_t = -40$ dBW, the SC performance with $\lambda = 0.99$ is approximately 1 bps/Hz lower than the others.

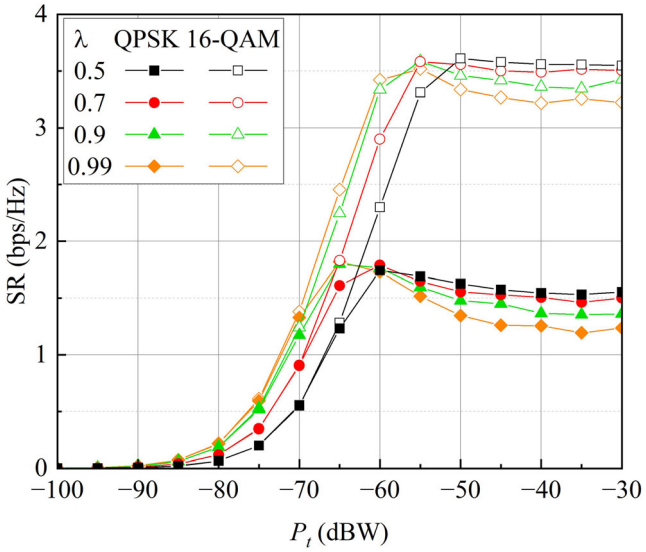

FIGURE 13 Comparison of secrecy rate of the integrated RIS and AN-aided PLS for LEO satellite system according to λ

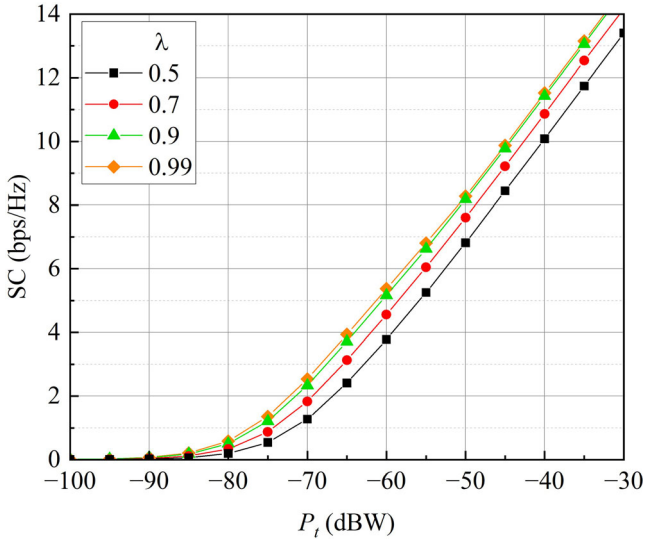

FIGURE 14 Comparison of secrecy capacity of the integrated RIS-aided and PB-Alamouti scheme for LEO satellite system according to λ

Furthermore, the SR performance in Figure 11 indicates that higher values of λ perform better in the low transmit power region because the capacity is heavily influenced by the AWGN and the channel capacity at Bob. Conversely, in the high transmit power region, the performance becomes more dependent on the interference invoked at Eve, and thus with increasing values of λ, we observe a higher degradation of performance.

Figures 12–15 illustrate the SC and SR performances of the system detailed in Section 3.3. Figures 12 and 13 show the results under the condition where both the RIS and AN-aided PLS methods are utilized. Lastly, Figures 14 and 15 present the results when integrating the RIS-aided method with the PB-Alamouti scheme. In the simulation, we assume:

$$\mathbf{g}_{\Theta} = \begin{bmatrix} \mathbb{E}_{\Theta}\left(\mathbf{g}_{re}\Theta\mathbf{h}_{ar}^{(1)}\right) \\ \mathbb{E}_{\Theta}\left(\mathbf{g}_{re}\Theta\mathbf{h}_{ar}^{(2)}\right) \end{bmatrix}. \tag{58}$$

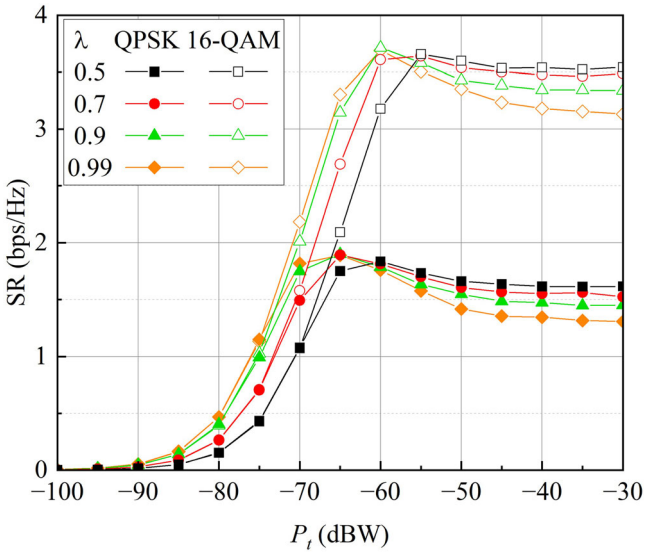

FIGURE 15 Comparison of secrecy rate of the integrated RIS-aided and PB-Alamouti scheme for LEO satellite system according to λ

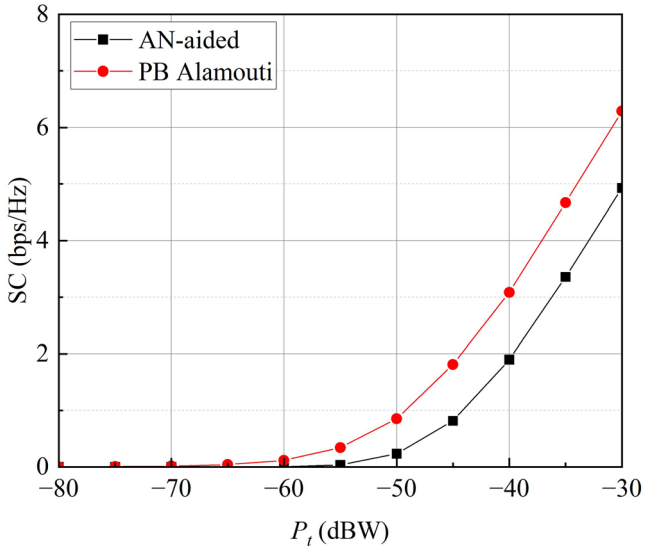

FIGURE 16 Comparison of secrecy capacity for relay-based PLS using AN-aided and PB-Alamouti code for LEO satellite system.

Different from the previous case in Figure 10, Figure 12 illustrates that when using the integrated RIS and AN-aided PLS schemes, the SC increases as λ increases. This is because the security is provided by two sources, that is, the AN and interference, and the AN is already sufficient to disturb Eve. In other words, as the channel capacity of Bob increases, the SC increases. We note that $\delta^{(i)} = \lambda\delta^{(i)}_{max}$, and λ determines the trade-off between the channel capacity of Bob and the interference at Eve. The SR in Figure 13 exhibits the same trend as SC in the low P_t region but shows a reverse performance in the high P_t region. This implies that when the SNR is sufficiently high, the function of the RIS should be more focused on causing interference to Eve than enhancing channel gains for Bob, to enhance the secrecy. Figures 14 and 15 shows the SC performances of the integration of the RIS-aided and PB-Alamouti PLS schemes, and they provide similar characteristics compared to the SC and SR in Figures 12 and 13, except for the power gain achieved by the PB-Alamouti scheme.

For the AN-based PLS using relay, its SC and SR in Figures 16 and 17 exhibit the same characteristics as in the system with two satellites in Figures 8 and 9. However, there is a reduction in magnitude because of the additional AWGN at the relay. Finally, Figures 18 and 19 compare the SC and SR performances of all the proposals introduced in this paper. Here, we set λ to 0.7 for the second and third proposals, and employed 16-QAM for SR estimation. It is shown that by adopting the RIS, the SC can be highly enhanced compared to the systems without the RIS, that is,

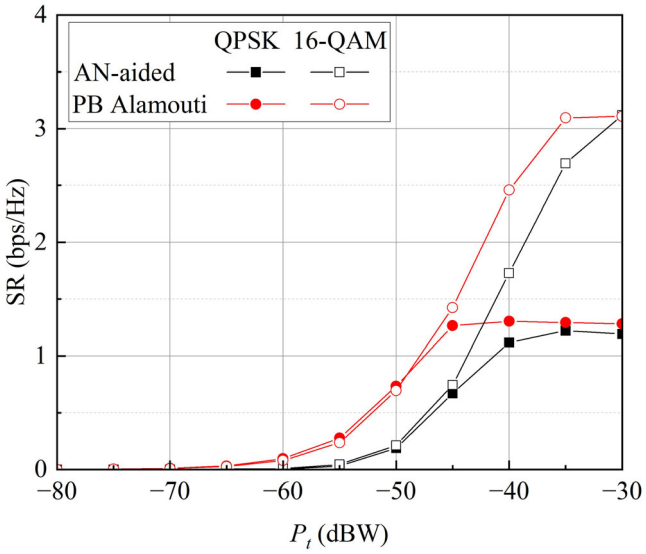

FIGURE 17 Comparison of secrecy capacity for relay-based PLS using AN-aided and PB-Alamouti code for LEO satellite system.

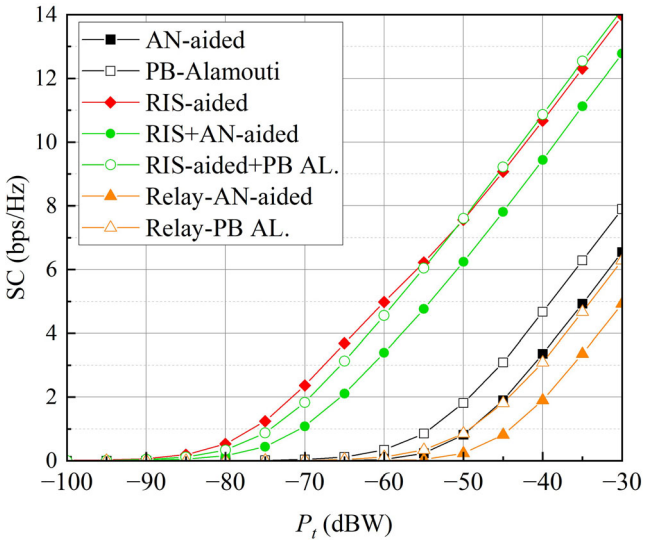

FIGURE 18 Comparison of secrecy capacity performances for all the proposals, $\lambda = 0.8$

the first and fourth proposals. In addition, adoption of the PB-Alamouti scheme further enhances the SC. The SR performance also proves that when the power is sufficiently high, the integration of the interference from the RIS and AN provides better secrecy.

Table 3 summarizes the characteristics of each proposal. Proposal 1 necessitates Alice to possess an AN generator and delay compensation technique. Proposal 2 offers security without burdening Alice or Bob, albeit requiring an RIS controller. Proposal 3, the integration of the first and second proposals, enhances security compared to either proposal individually. Proposal 4 exhibits the lowest power efficiency, yet proves vital when the relay enhances signal strength. Additionally, a performance trade-off exists between SR and signal strength at Bob.

All proposals entail distinct system configurations, each offering varying levels of security enhancement with differing complexities. Opting for an overall reduction in system complexity may involve equipping Alice with delay compensation technique and AN generator; however, this approach requires an expensive power amplifier capable of handling power fluctuations caused by AN. Alternatively, leveraging RIS technology could avoid the need for modifications to Alice, although RIS technology is still relatively new. Furthermore, if heightened security is required, integrating RIS and AN may be a viable option to consider.

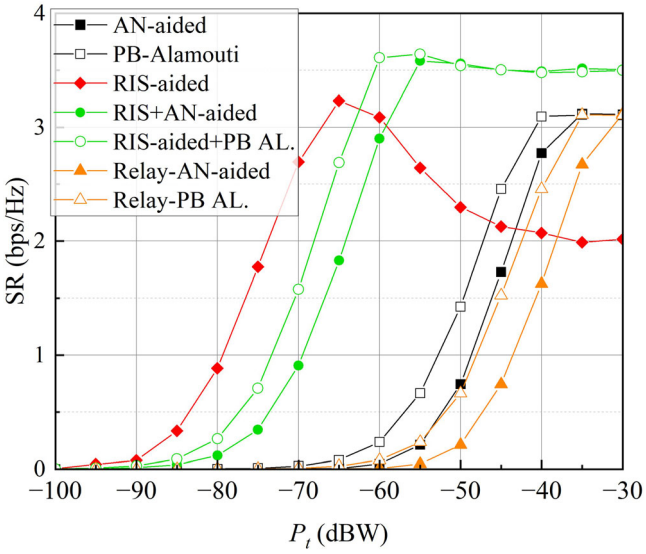

FIGURE 19 Comparison of secrecy rate performances for all the proposals with 16-QAM, $\lambda = 0.7$

TABLE 3 Performance characteristics.

Proposal	Characteristics
1	More complexity at Alice (AN generator, delay compensation technique)
2	No additional task to Alice and Bob, signal strength at Bob and security trade-off
3	Enhancing security compared to proposals 1 and 2, higher complexity
4	More complexity at transmitters as in proposal 1

5 | CONCLUSION AND DISCUSSION

This study introduced four proposals to enhance PLS in LEO satellite systems. The first proposal utilized the Alamouti code aided by AN, involving the collaborative use of two LEO satellites for secure downlink transmission. The SC and SR performances demonstrated the applicability of the AN-aided Alamouti code for security in satellite systems. Additionally, the use of the PB-Alamouti scheme proved that compared to the AN-aided Alamouti code, it could enhance power efficiency and secrecy. The second PLS proposal utilized the RIS to introduce interference to potential eavesdroppers, ensuring data security. This method applied a novel idea of invoking interference, maintaining the channel of the legitimate receiver as constant, while making that of the eavesdropper dynamic using the RIS. This approach used the well-known Newton-Raphson method to estimate the phases of the RIS elements. The results proved that this technique can provide security without burdening the transmitter and receiver. The third proposal integrated the first and second proposals, resulting in improved SR compared to the individual proposals, while nearly reaching the maximum achievable rate. The fourth proposal suggested the use of a relay to activate the AN-aided and PB-Alamouti scheme, and is designed for the environment where the direct signal from the satellite is hardly available. The transmission links from the satellite to relay, and from the satellite and relay to the legitimate user, are safeguarded by AN, making it difficult for the eavesdropper to detect information. The results prove that providing security is feasible.

Given the utilization of perfect channel state information (CSI) in this study, future research endeavors will delve into exploring secrecy aspects under the imperfections of CSI. Furthermore, an examination will be conducted to assess the efficacy of the proposed methodologies in scenarios where the SNR of Eve surpasses that of Bob. In addition, it is crucial to ensure that the RIS is visible to Eve to uphold security. Hence, an investigation into the influence of RIS placement on security will be carried out. Specifically, we will evaluate performance metrics with the RIS positioned on various platforms, including the buildings or towers, high-altitude platform stations, and satellite itself. Moreover, we will study the feasibility of the RIS-aided PLS method for multiple-input multiple-output systems in the presence of multiple eavesdroppers.

ACKNOWLEDGMENTS

This research was supported by the Institute for Information and Communications Technology Promotion Grant funded by the Korea Government (MSIT, Development of the spectrum sharing technology for Non-GSO satellite system) under Grant 2021-0-00719 and the National Research Foundation of Korea (NRF) funded by the Korea government (MSIT) (NRF-2021R1A2C1003121).

ORCID

Satya Chan https://orcid.org/0000-0002-9146-6177

Sooyoung Kim https://orcid.org/0000-0003-0817-2790

REFERENCES

1. Chettri L, Bera R. A comprehensive survey on internet of things (IoT) toward 5G wireless systems. *IEEE Internet Things J*. 2020;7(1):16-32.
2. Zaidi AA, Baldemair R, Moles-Cases V, He N, Werner K, Cedergren A. OFDM numerology design for 5G new radio to support IoT, EMBB, and MBSFN. *IEEE Commun Stand Mag*. 2018;2(2):78-83.
3. Akpakwu GA, Silva BJ, Hancke GP, Abu-Mahfouz AM. A survey on 5G networks for the internet of things: Communication technologies and challenges. *IEEE Access*. 2018;6:3619-3647.
4. Rezaei Aghdam S, Nooraiepour A, Duman TM. An overview of physical layer security with finite-alphabet signaling. *IEEE Commun Surv Tutor*. 2019;21(2):1829-1850.
5. Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Trans Wireless Commun*. 2008;7(6):2180-2189.
6. Jiang X-Q, Wen M, Hai H, Li J, Kim S. Secrecy-enhancing scheme for spatial modulation. *IEEE Commun Lett*. 2018;22(3):550-553.
7. Lee H, Shang P, Kim S. A new MIMO signal constellation for secrecy and performance enhancing. In: International Conference on Information and Communication Technology Convergence (ICTC); 2020; Jeju, South Korea:924-928.
8. Shang P, Yu W, Zhang K, Jiang X-Q, Kim S. Secrecy enhancing scheme for spatial modulation using antenna selection and artificial noise. *Entropy*. 2019;21(7).
9. Shang P, Kim S, Jiang X-Q. Efficient Alamouti-coded spatial modulation for secrecy enhancing. In: International Conference on Information and Communication Technology Convergence (ICTC); 2019; Jeju, Korea:860-864.
10. Shang P, Lee H, Kim S. Waveform design for space-time coded MIMO systems with high secrecy protection. *Electronics*. 2020;9(12).
11. Shin SY, Wicaksono IA. Improving wireless physical layer security using Alamouti code and artificial noise. In: International Conference on ICT Convergence (ICTC); 2013; Jeju, Korea:1061-1064.
12. Lee H, Kim S. Evaluation of the security performance of artificial noise-aided STBC systems. *IET Commun*. 2023;17(9):1081-1090.
13. Yu H, Joung J. Design of the power and dimension of artificial noise for secure communication systems. *IEEE Trans Commun*. 2021;69(6):4001-4010.
14. Yu H, Kim T. Training and data structures for AN-aided secure communication. *IEEE Syst J*. 2019;13(3):2869-2872.
15. Lee H, Chan S, Kim S. Efficient MIMO signal predistortion for secrecy-enhancing. *Electronics*. 2022;11(9).
16. Chan S, Lee H, Kim S. A power-balanced Alamouti scheme with security protection. Research Square; 2023.
17. Kang Z, You C, Zhang R. Irs-aided wireless relaying: Deployment strategy and capacity scaling. *IEEE Wireless Commun Lett*. 2022;11(2):215-219.
18. Ali B, Mirza J, Alvi SH, Khan MZ, Javed MA, Noorwali A. IRS-assisted physical layer security for 5G enabled industrial internet of things. *IEEE Access*. 2023;11:21354-21363.
19. Souzani A, Pourmina MA, Azmi P, Naser-Moghadasi M. Physical layer security enhancement via irs based on PD-NOMA and cooperative jamming. *IEEE Access*. 2023;11:65956-65967.
20. Qiao T, Cao Y, Tang J, Zhao N, Wong K-K. IRS-aided uplink security enhancement via energy-harvesting jammer. *IEEE Trans Commun*. 2022;70(12):8286-8297.
21. Khalid W, Rehman MAU, Van Chien T, Kaleem Z, Lee H, Yu H. Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances. *IEEE Internet Things J*. 2024;11(2):3599-3613.
22. Rahman MM, Badrudduza ASM, Sarker NA, Ibrahim M, Ansari IS, Yu H. RIS-aided mixed RF-FSO wireless networks: Secrecy performance analysis with simultaneous eavesdropping. *IEEE Access*. 2023;11:126507-126523.
23. Lee J, Shin W, Lee J. Performance analysis of IRS-assisted leo satellite communication systems. In: International Conference on Information and Communication Technology Convergence (ICTC); 2021; Jeju, Korea:323-325.
24. Alamouti SM. A simple transmit diversity technique for wireless communications. *IEEE J Sel Areas Commun*. 1998;16(8):1451-1458.
25. Ahn D, Kim S, Kim HW, Park D-C. A cooperative transmit diversity scheme for mobile satellite broadcasting systems. *Int J Satellite Commun Netw*. 2010;28(5):352-368.

AUTHOR BIOGRAPHIES

Satya Chanreceived his BTech degree in electronics engineering from NPIC, Cambodia, in 2014. Following his graduation, he dedicated his time to voluntary work at an NGO from 2014 to 2017 and served as a reporter at AE Company for 7 months. He later pursued advanced education, obtaining his ME and PhD degrees from Jeonbuk National University, Republic of Korea, in 2019 and 2023, respectively. Currently, he holds a position as a postdoctoral researcher at the Electronics and Telecommunications Research Institute (ETRI). His research interests include satellite communications and standardization, physical layer security for MIMO systems, soft detection for coded MIMO systems, and error correction coding

Sooyoung Kim received the BS degree in electrical and electronics engineering from KAIST, Korea, in 1990. After having worked Satellite Communication Technology Division, ETRI, Korea from February 1990 to September 1991, she received the MSc and the PhD degree in electrical and electronics engineering from University of Surrey, UK, in 1992 and 1995, respectively. From November 1994 to June 1996, she was employed as a research fellow at the Centre for Satellite Engineering Research, University of Surrey, UK. In 1996, she re-joined the Satellite Communication Technology Division, ETRI, Korea, and worked as a team leader until February 2004 to develop efficient transmission techniques for digital satellite communication systems. She is now a professor in Jeonbuk National University. Her research interests include coded MIMO schemes, forward error correction coding, physical layer security schemes, and satellite communications. She is a vice chairperson of the Working Party 4B of ITU-R and has been working on the standardization activities for satellite communications. She has published more than 100 technical papers in the field of wireless/satellite communications. She has been a Technical Program Committee (TPC) member at various conferences and an editorial board member of the *International Journal of Satellite Communication Systems and Networking*.

Hee Wook Kim received the MS degree in electrical from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2004. He is currently working as a principal researcher at Satellite Communication Infra Research Section of the Electronics and Telecommunications Research Institute (ETRI), Korea. His research interests include terrestrial/satellite mobile (5G/6G) communication, non-terrestrial network (NTN), UAS and UAM (urban air mobility) communication, and radio regulation. He has also been working as a standard expert for satellite and drone communications in many standardization bodies such as ITU-R, ETSI, 3GPP, RTCA, ASTM, and ICAO.

Bon-Jun Ku received the PhD degree from Chungbuk National University in 2010. Since 1999, he has worked for Electronics and Telecommunications Research Institute (ETRI). He is currently a principal member of research staff at Satellite Communication Research Division in ETRI. His research interests include satellite communications system, high altitude platform station (HAPS), and wireless communication system engineering.

Daesub Oh received the PhD degree from Jeonbuk National University in 2014. He has worked for Electronics and Telecommunications Research Institute (ETRI) since 2000. His research interests are in the broad areas of satellite communication, wireless communication, and spectrum management. He has been working in spectrum management and regulatory policies in the ITU-R, APT.

How to cite this article: Chan S, Kim S, Kim HW, Ku B-J, Oh D. Energy-efficient physical layer security schemes for low Earth orbit satellite systems. *Int J Satell Commun Network*. 2024;42(5):374-396. doi:10.1002/sat.1519

APPENDIX A

Here, we detail the method of finding multiple solutions of $\boldsymbol{\Theta}$ in (34) and (40), to cause harmful interference at Eve, using the Newton-Raphson method. First, (34) can be re-expressed as

$$\mathbf{h}_{rb}\mathrm{diag}(\mathbf{h}_{ar})\mathbf{v}^T - \delta = \mathbf{t}\mathbf{v}^T - \delta = 0. \tag{A1}$$

Since $\mathbf{v} = [e^{j\theta_1}\, e^{j\theta_2} \ldots e^{j\theta_N}]$, (A1) can be written as follows:

$$\begin{aligned} &\sum_{i=1}^{N}\left(t_i^{\Re}\cos(\theta_i) - t_i^{\Im}\sin(\theta_i)\right) - \delta^{\Re} \\ &+ j\sum_{i=1}^{N}\left(t_i^{\Re}\sin(\theta_i) + t_i^{\Im}\cos(\theta_i)\right) - j\delta^{\Im} = 0. \end{aligned} \tag{A2}$$

Since the Newton-Raphson method is only applicable to the real-valued equation, we decompose (A2) into two real-valued equations as

$$f_1(\mathbf{u}) = \sum_{i=1}^{N} \left(t_i^{\Re} \cos(\theta_i) - t_i^{\Im} \sin(\theta_i)\right) - \delta^{\Re} = 0, \tag{A3}$$

$$f_2(\mathbf{u}) = \sum_{i=1}^{N} \left(t_i^{\Re} \sin(\theta_i) + t_i^{\Im} \cos(\theta_i)\right) - \delta^{\Im} = 0, \tag{A4}$$

where $\mathbf{u} = [\theta_1 \theta_2 \ldots \theta_N]$. The solution of $\mathbf{u}$ can be iteratively updated as

$$\mathbf{u}_{k+1} = \mathbf{u}_k - \mathbf{J}_{\mathbf{u}_k}^T \left(\mathbf{J}_{\mathbf{u}_k} \mathbf{J}_{\mathbf{u}_k}^T\right)^{-1} \mathbf{F}(\mathbf{u}_k), \tag{A5}$$

where the $\mathbf{u}_k$ is the solution of $\mathbf{u}$ at the kth iteration with $\mathbf{u}_0$ as an initial guess. The Jacobian matrix with respect to $\mathbf{u}, \mathbf{J}_{\mathbf{u}}$ can be estimated as follows:

$$\mathbf{J}_{\mathbf{u}} = \frac{\partial \mathbf{F}(\mathbf{u})}{\partial \mathbf{u}}, \tag{A6}$$

and

$$\mathbf{F}(\mathbf{u}) = \begin{bmatrix} f_1(\mathbf{u}) \\ f_2(\mathbf{u}) \end{bmatrix}. \tag{A7}$$

Ultimately, the value of $\boldsymbol{\Theta}$ can be directly estimated from $\mathbf{u}$, that is, $\boldsymbol{\Theta} = \mathrm{diag}(e^{j\mathbf{u}})$. We note that different solutions for $\boldsymbol{\Theta}$ is contingent on the respective initial guess $\mathbf{u}_0$. Therefore, as many as possible solutions of $\boldsymbol{\Theta}$ can be found by imposing time-varying $\mathbf{u}_0$ values. In addition, a similar process can be applied to (40) by decomposing it into real-valued equations. Therefore, the sizes of $\mathbf{J}_{\mathbf{u}}$ and $\mathbf{F}(\mathbf{u})$ associated with (40) will be doubled.