Evaluation of Interleaving-based PLS Scheme for Satellite Communications

Thara Son, Sooyoung Kim
IT Convergence Research Center, Div. of Elec. Eng, Jeonbuk National University
Jeonju, Republic of Korea
Email: {tharason, sookim}@jbnu.ac.kr

***Abstract*—Physical layer security (PLS) schemes exploit the randomness and unpredictability of a wireless channel to establish secure communication links, and they can be considered as one of the effective techniques to provide security protection. On the other hand, satellite systems have difficulties of fully exploiting randomness and often have consistent spatial channel characteristics due to a long round trip delay and wide coverage areas, which make it difficult to apply the same PLS techniques developed originally for the terrestrial systems. This paper first reviews several PLS techniques developed for multi-antenna systems and evaluates their applicability to satellite systems, particularly dynamic interleaving-based PLS techniques. The results presented in this paper reveal that the examined PLS scheme effectively degrades the eavesdropper's decoding capability under dynamically changing satellite channel conditions.**

***Index Terms*—Bit interleaved coded modulation, physical layer security, Rician fading environment, channel correlation, channel estimation error, forward error correction.**

I. Introduction

Satellite networks have recently become key components of advanced communication systems such as the fifth generation (5G) and beyond by delivering global coverage and extending data paths into space through standalone deployments or satellite-terrestrial integrated networks [1], [2]. Satellite networks offer ubiquitous service to millions of users located hundreds of kilometers apart, yet their broadcast nature makes them vulnerable to interception by unauthorized parties [3], [4]. In the absence of protective measures, information confidentiality cannot be maintained.

Modern cryptographic techniques can secure information against attacks, but they rely on complex mathematical procedures to create shared keys for the legitimate transmitter and receiver [5]. These safeguards have traditionally been applied in the upper layers of the protocol stack, for example through encryption and authentication at the application layer or the network layer. Physical layer security (PLS), first introduced by Wyner in his wiretap channel model [6], adopts a different strategy by shaping the physical-layer signal itself to provide protection.

The basic idea behind PLS is to exploit the inherent randomness, variability, and unpredictability of wireless channel to establish secure communication links. Numerous studies have proposed PLS schemes for conventional terrestrial wireless systems. In particular, for multi-input multi-output (MIMO) systems, various PLS techniques have been developed, including artificial noise (AN)-based, phase distortion (PD)-based, and interleaving-based approaches [7]–[10].

The AN-based PLS scheme injects deliberate noise into the transmitted signal, allowing only the legitimate receiver, equipped with the correct channel state information (CSI), to effectively cancel it. In contrast, an eavesdropper with mismatched CSI experiences significant interference, hindering successful decoding [7], [8]. A key drawback of the AN-based approach is the additional transmit power required to generate artificial noise. As an alternative, a PD-based PLS scheme applies CSI-dependent phase rotations that can be reversed by the legitimate receiver but not by an eavesdropper [9]. However, both methods rely heavily on highly accurate CSI, which is often impractical in real-world scenarios. To mitigate this dependency, a dynamic interleaving-based PLS scheme has been proposed [10]. This scheme enhances robustness by employing an ancillary forward error correction (AFEC) mechanism to compensate for imperfect CSI.

Although the aforementioned methods may be effective in conventional multi-input multi-output (MIMO) systems, where the channel exhibits rich spatial diversity, their direct application to satellite systems presents challenges. Due to the dominant line-of-sight (LoS) propagation and slow-fading dynamics in satellite channels, spatial diversity is limited, making it difficult to apply MIMO schemes effectively. Furthermore, these channel characteristics also reduce channel randomness, rendering traditional PLS schemes less suitable. As a result, researchers have investigated the applicability of PLS techniques to satellite systems [11], [12]. Since multiple low Earth orbit (LEO) satellites can cooperatively function as a distributed antenna array, PLS schemes originally developed for MIMO systems have been adapted to multi-satellite LEO configurations [11]. Additionally, to enhance channel randomness, AN-based PLS techniques have been integrated with reconfigurable intelligent surfaces (RIS) for satellite networks [12]. Motivated by these studies, this paper investigates the applicability of interleaving-based PLS to satellite systems.

The remainder of the paper is organized as follows. Section II reviews various PLS techniques developed for MIMO systems. Section III presents the concept of applying interleaving-based PLS to satellite systems. Section IV discusses the

This work was supported under the framework of international cooperation program managed by National Research Foundation of Korea (No. RS-2024-00459799).

simulation results and Section V concludes the paper.

II. Review on PLS schemes for MIMO systems

The adoption of multi-antenna techniques has grown rapidly across wireless networks and widely used in terrestrial systems [13]. We consider a wiretap model, where a transmitter (Alice) communicates with a legitimate receiver (Bob), while a passive eavesdropper (Eve) attempts to intercept the information exchanged between Alice and Bob [8]–[10]. Alice and Bob are assumed to know their mutual channel, enabling Bob to separate the intended data from any deliberate distortions inserted by Alice with the aid of a PLS scheme. Under these assumptions, Bob can reliably recover the signal, while Eve struggles to decode the meaningful information.

Fig. 1 shows an AN-based PLS scheme using the Alamouti code [8]. Alice has two transmit antennas, while Bob and Eve each have a single antenna, giving a 2×1 configuration. Alice and Bob know their mutual channel vector $\mathbf{h} = [h_1, h_2]^T$, where $[\cdot]^T$ denotes matrix transpose. In contrast, the channel between Alice and Eve is given by $\mathbf{g} = [g_1, g_2]^T$. Moreover, Eve is assumed to be several wavelengths away from Bob, so $\mathbf{h}$ and $\mathbf{g}$ are treated as independent.

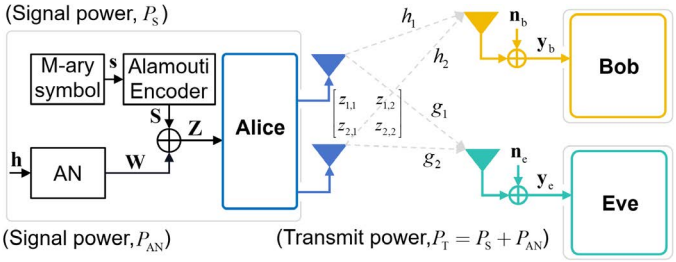

Fig. 1. Operational principle of the AN-based PLS scheme for Alamuti code.

The transmit symbol vector $\mathbf{s} = [s_1, s_2]^T$ is encoded with the Alamouti space-time block-code (STBC), producing the 2×2 matrix $\mathbf{S}$ over two consecutive time slots [14]. Artificial noise is then imposed by adding the matrix $\mathbf{W}$ to $\mathbf{S}$, yielding $\mathbf{Z} = \mathbf{S} + \mathbf{W}$. The AN matrix is designed to vanish at Bob. One common choice is to pick $\mathbf{W}$ from the null space of Bob's channel vector, so that $\mathbf{h}^H\mathbf{W} = 0$ [7]. Accordingly, Bob receives $\mathbf{y}_b = \mathbf{h}\mathbf{Z} + \mathbf{n}_b$ and Eve receives $\mathbf{y}_e = \mathbf{g}\mathbf{Z} + \mathbf{n}_e$, where $\mathbf{n}_b$ and $\mathbf{n}_e$ denote additive white Gaussian noise (AWGN), at Bob and Eve, respectively. The signal detection can be carried out using the standard Alamouti procedure [14]. Since Eve does not know Bob's channel, AN appears as interference and degrades her decoding ability. Although AN-based PLS effectively blocks unauthorized access, it requires extra transmit power for the artificial noise. There exists a trade-off between the error rate performance and secrecy rate, depending on the amount of the added AN [11], [12]. Furthermore, the addition of random AN causes high peak to average power ratio (PAPR) problem.

To mitigate the above problems, the phase-distortion (PD) PLS scheme replaces AN with CSI-driven phase rotations, so no extra power allocation is required. Moreover, this method is applicable for both STBC and MIMO systems. Fig. 2 illustrates the PD principle for a MIMO system. Initially, Alice spatially multiplexes the symbol vector $\mathbf{s}$ and transmits it to Bob and Eve through channels $\mathbf{H}$ and $\mathbf{G}$, respectively. Before transmission, she pre-distorts $\mathbf{s}$ with a diagonal phase matrix $\mathrm{diag}(\mathbf{q})$, yielding $\mathbf{s}' = \mathrm{diag}(\mathbf{q})\mathbf{s}$. The vector $\mathbf{q}$ is obtained by summing the phases in each column of $\mathbf{H}$. Bob receives $\mathbf{y}_b = \mathbf{H}\mathbf{s}' + \mathbf{n}_b$ and detects the symbols using the effective channel $\mathbf{H}' = \mathbf{H}\,\mathrm{diag}(\mathbf{q})$ with a conventional MIMO detector [9]. Eve, lacking $\mathbf{H}$, cannot remove the distortion and suffers a severe decoding loss. Although their effectiveness, both AN- and PD-based approaches depend heavily on accurate knowledge of the legitimate channel, which is often impractical in real-world systems due to the challenges of achieving perfect CSI.

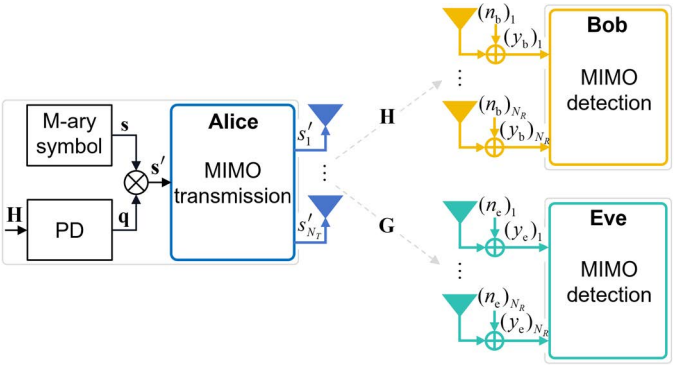

Fig. 2. Operational principle of the PD-based PLS scheme for MIMO system.

To overcome these problems, a dynamic interleaving-based PLS scheme is employed [10]. Fig. 3 outlines the operational principle of the sub-block-wise interleaving approach for a coded MIMO system under imperfect channel conditions. By using bit-interleaved coded modulation (BICM) with low-density parity check (LDPC) code, the source information matrix $\mathbf{U}$ is encoded to form a codeword matrix $\mathbf{C}$. Then $\mathbf{C}$ is divided into L sub-blocks $\mathbf{B}_i$, $1 \le i \le L$. Given that $\mathbf{H}_i$ represents the CSI for $\mathbf{B}_i$, the interleaving index δ_i is derived from $\mathbf{H}_i$ and used as the starting position for the diagonal interleaving process.

We use δ_i to generate the interleaved version of $\mathbf{B}_i$ as $\mathbf{B}'_i = \pi_{\delta_i}(\mathbf{B}_i)$, where $\pi_{\delta_i}(\cdot)$ denotes the interleaving operation with index δ_i. The resulting blocks $\mathbf{B}'_1$ through $\mathbf{B}'_L$ are then serially concatenated to form the sub-block-wise interleaved codeword $\mathbf{C}'$. Finally, all binary representations of δ_1 to δ_L are combined into a vector denoted as $\mathbf{d}$. Treating $\mathbf{d}$ as the systematic information, an AFEC code is applied to generate its corresponding parity $\mathbf{p}$. The purpose of employing AFEC is to protect the interleaving process against CSI errors that may affect the interleaving indices at the receiver. The parity $\mathbf{p}$ is then partitioned into MIMO frames and arranged into a matrix $\mathbf{P}$, which is subsequently interleaved to produce $\mathbf{P}'$. This interleaved parity matrix $\mathbf{P}'$ is transmitted over the MIMO channel, followed by the interleaved codeword $\mathbf{C}'$.

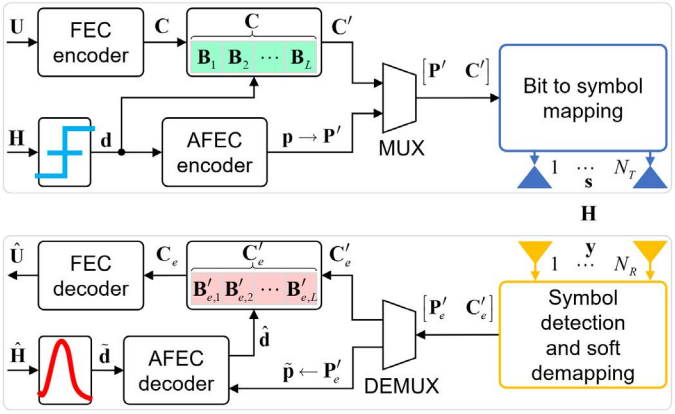

Fig. 3. Sub-block-wise interleaving-based PLS scheme with coded MIMO system.

At the receiving end, we receive $\mathbf{P}'_e$ followed by $\mathbf{C}'_e$ which are the log-likelihood ratio (LLR) estimation version of $\mathbf{P}'$ and $\mathbf{C}'$, respectively. First, we deinterleave $\mathbf{P}'_e$ as $\mathbf{P}_e$ and reshape it to vector $\tilde{\mathbf{p}}$. Further, the received $\mathbf{C}'_e$ along with its estimated channel matrix $\hat{\mathbf{H}}$, are partitioned into L sub-blocks, giving $\mathbf{B}'_{e,i}$ and $\hat{\mathbf{H}}_i$, respectively. At the same time, we estimate $\tilde{\mathbf{d}}$ from the channel estimation error, where $\tilde{\mathbf{d}}$ is the LLR value vector for $\mathbf{d}$. This vector $\tilde{\mathbf{d}}$ serves as systematic part, then concatenated with $\tilde{\mathbf{p}}$ is ready to be used for the decoding process for the AFEC. After decoding, the corrected index vector is obtained and sub-block-wise deinterleaving is applied to all $\mathbf{B}_{e,1}$ to $\mathbf{B}_{e,L}$ and serially concatenated to form $\mathbf{C}_e$. After that, the sub-block-wise deinterleaved codeword $\mathbf{C}_e$ serves as the input for LDPC decoding to estimate the source information $\hat{\mathbf{U}}$.

III. Evaluation on Interleaving-based PLS for Satellite System

Fig. 4 presents a system model for applying the interleaving-based PLS scheme to a satellite system. We assume a transparent satellite transponder, where the satellite gateway (Alice) transmits information to the satellite through an error-free channel. The satellite then relays the signal to the legitimate user (Bob) over a Rician channel with a channel gain of h. Upon receiving the signal, Bob attempts to detect information with the estimated channel state information, $\hat{h}$ expressed as follows:

$$\begin{aligned}\hat{h} &= h + n_h \\ &= \left(\sqrt{\frac{K}{K+1}} + \sqrt{\frac{1}{K+1}} h_R\right) + n_h, \end{aligned} \tag{1}$$

where $h_R \sim \mathcal{CN}(0,1)$ and $n_h \sim \mathcal{CN}(0,\sigma_h^2)$ are complex Gaussian random variables representing a Rayleigh fading component and CSI estimation error at Bob, respectively. Here, K denotes the Rician factor. Due to the wide beam coverage of the satellite, the channels observed by Bob and Eve are spatially correlated. Accordingly, Eve may be able to intercept the signal through a correlated channel gain g with a correlation factor ρ, as follows:

$$g = \sqrt{\frac{K}{K+1}} + \sqrt{\frac{1}{K+1}} \left(\sqrt{\rho^2} h_R + \sqrt{1-\rho^2} g_R\right), \tag{2}$$

where $g_R \sim \mathcal{CN}(0,1)$ is a complex Gaussian random variable representing a Rayleigh fading component. She also tries to retrieve the information by using her own CSI estimation, $\hat{g}$ given by:

$$\hat{g} = g + n_g, \tag{3}$$

where $n_g \sim \mathcal{CN}(0,\sigma_g^2)$ is the CSI estimation error at Eve.

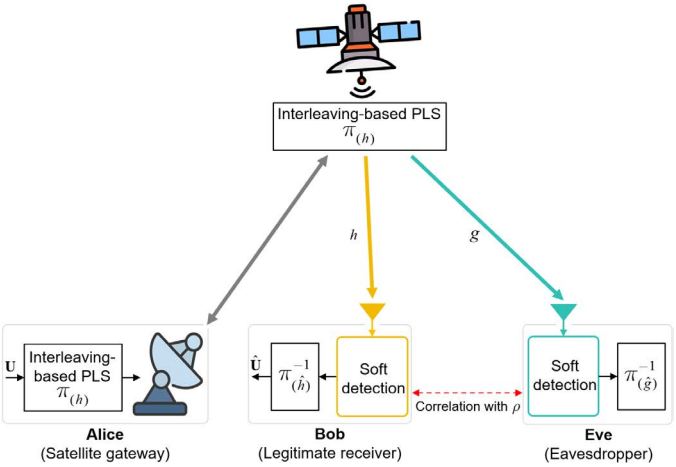

Fig. 4. System configuration for PLS-aided satellite communication system.

Alice employs (n,k) LDPC coding scheme specified in beyond 5G standard [15], where n and k denote the codeword and information lengths, respectively. The source information matrix $\mathbf{U}$ size of $m \times k$ undergo an encoding process to generate a codeword $\mathbf{C}$ with size of $m \times n$, where m is the number of bit per modulation symbol. Next, $\mathbf{C}$ is divided into multiple sub-blocks of $\mathbf{B}_1, ..., \mathbf{B}_i, ..., \mathbf{B}_L$, $L = \lceil n/l \rceil$, where l is the number of columns in each sub-block, and $\lceil \cdot \rceil$ is the ceiling operation. Each $\mathbf{B}_i$ having a size of $m \times l$. Letting $\mathbf{h}_i$ denote the CSI vector associated with sub-block $\mathbf{B}_i$, the interleaving index δ_i is extracted from $\mathbf{h}_i$. Sub-block-wise interleaving is then applied to each $\mathbf{B}_i$, producing the interleaved block $\mathbf{B}'_i$. Each index δ_i is represented as a binary combination of length $z = \log_2(l)$ bits. The binary representations are concatenated to form the vector $\mathbf{d}$ of length zL bits, which is then encoded using AFEC. After the encoding process, the parity $\mathbf{p}$ is generated with length of l_p bits. The length of $\mathbf{p}$, l_p determines error correction capability of AFEC. For the transmission, $\mathbf{p}$ is reshaped into a matrix $\mathbf{P}$ with a size of $m \times \lambda$, where $\lambda = l_p/m$. Each column of $\mathbf{P}$ and $\mathbf{C}'$ is modulated and transmitted over the channel.

At the receiver, soft detection is first performed to obtain the LLR matrices $\tilde{\mathbf{P}}$ and $\tilde{\mathbf{C}}'$, which represent the error-corrupted AFEC parity and codeword, respectively. The LLR matrix $\tilde{\mathbf{C}}'$, along with its corresponding estimated channel $\mathbf{h}$, is partitioned into L sub-blocks denoted as $\tilde{\mathbf{B}}_i$ and $\hat{\mathbf{h}}_i$, respectively. At

the same time, we derive $\tilde{\mathbf{d}}$, the LLR vector for the systematic data $\mathbf{d}$, from the imperfect CSI as described in [10]. Next, we reshape $\tilde{\mathbf{P}}$ into vector $\tilde{\mathbf{p}}$, which is then concatenated with $\tilde{\mathbf{d}}$ to form the AFEC codeword for decoding. After AFEC decoding, the interleaved sub-blocks $\tilde{\mathbf{B}}_i'$ are deinterleaved back into $\tilde{\mathbf{B}}_i$, which are then concatenated to reconstructed $\tilde{\mathbf{C}}$. Finally, $\tilde{\mathbf{C}}$ is fed into the LDPC decoder to recover the source information $\hat{\mathbf{U}}$.

IV. Simulation Results

We evaluate the performance of the a dynamic interleaving-based PLS scheme by using a satellite system model presented in Section III. Quadrature phase shift keying (QPSK)-modulated signals are transmitted and forwarded to the user through a Rician fading channel. The system employs the (6144, 4096) LDPC code with a rate of 2/3, standardized in the beyond 5G system [15]. The interleaving index is set to $z = 6$ bits, resulting in a sub-block length of $l = 64$ bits. Given a codeword length of 6144 bits, we divide it into $L = \lceil 6144/64 \rceil = 96$ sub-blocks, forming an interleaving index vector $\mathbf{d}$ of length $zL = 576$ bits. For AFEC, we apply $(576 + l_p, 576)$ LDPC code, where l_p is selected using a rule of thumb to ensure decoding performance comparable to the (6144, 4096) LDPC code. We assume that channel estimation error at Bob and Eve are equal, i.e., $\sigma_h^2 = \sigma_g^2$, where σ_h^2 and σ_g^2 are the variance of the channel estimation error at Bob and Eve, respectively.

We investigate the bit-error rate (BER) performance according to Rician factor, K, channel correlation factor, ρ, and signal-to-noise ratio (SNR) of channel estimation error, γ. Fig. 5 illustrates the BER results for various K values under $\gamma = 10$ dB and $\rho^2 = 0.1$. For comparison, we also consider a baseline scenario without any PLS mechanisms, referred to as 'NPLS' in the simulation. To achieve performance comparable to the main LDPC code, the AFEC parity length l_p is set to 450, 400, and 350 bits for $K = 0$ dB, 5 dB, and 10 dB, respectively. When K is smaller, the channel approaches the Rayleigh fading condition. As a result, for $K = 0$ dB, the PLS scheme with AFEC achieves BER performance close to that of the NPLS baseline. In contrast, both the PLS scheme without AFEC and Eve suffer from mismatched interleaving indices due to channel estimation errors, leading to significant performance degradation. However, as K increases, the channel exhibits dominant LoS components, increasing the dependency between the channels for Bob and Eve. Accordingly, the performance at Eve exhibit the same slope indicating that she can retrieve the information with just a few additional decibels of power.

Fig. 6 presents the effect of channel correlation when $\gamma = 10$ dB, by considering $\rho^2 = 0.1$ and 0.5, respectively. In the case of $K = 0$ dB, for $\rho^2 = 0.1$, Eve experiences significant performance degradation due to the highly unpredictable channel and the lower channel correlation between her and Bob. Once ρ^2 is set to 0.5, Eve's performance slightly improves due to increased channel correlation with Bob, but it remains insufficient for reliable decoding. Conversely, when $K = 10$ dB, the channel becomes more dependent each other. As a result, Eve can decode the information by using slightly more power than Bob. Specifically, Eve requires only 1 dB and 0.2 dB more power than Bob to achieve a BER of 10^{-5}, under $\rho^2 = 0.1$ and 0.5, respectively.

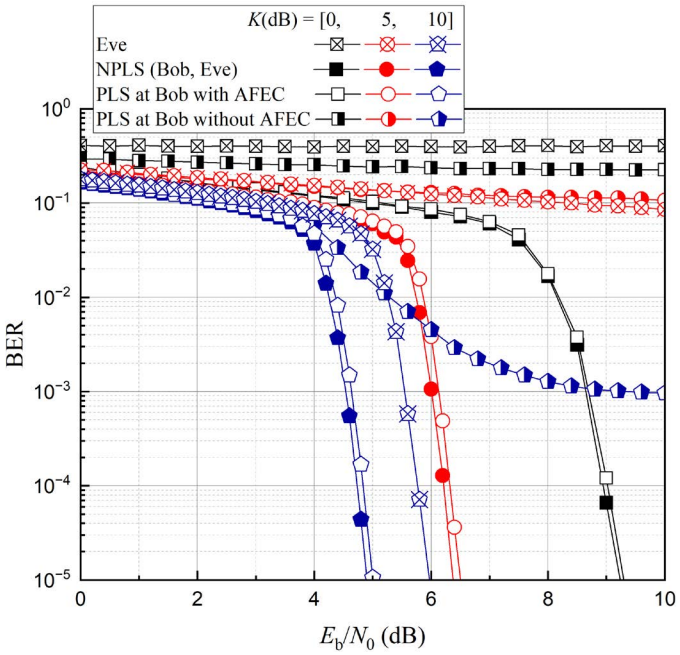

Fig. 5. BER performance comparison for the interleaving-based PLS scheme under $\gamma = 10$ dB and $\rho^2 = 0.1$.

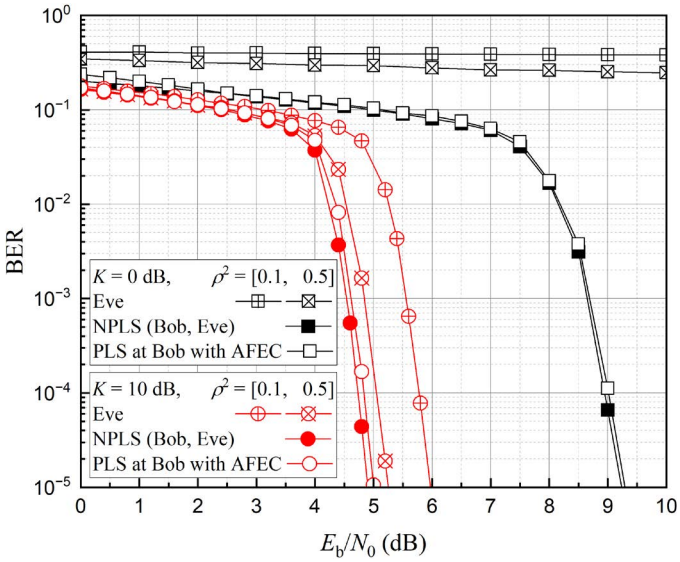

Fig. 6. BER performance comparison under $\gamma = 10$ dB with various K and ρ^2 values.

Next, we consider a more practical scenario in which the K-factor varies dynamically, particularly in the case of LEO satellites, where the K-factor fluctuates due to the rapid movement of the satellites. In this setting, we generate a

uniformly distributed random variable $K \sim \mathcal{U}[0, 10]$ (dB) for each codeword to emulate the varying Rician channel conditions experienced by different transmitted codewords. Fig. 7 illustrates the BER performance under this condition when ρ^2 is set to 0.5. The results demonstrate that the examined PLS scheme remains robust even under comparatively high correlation conditions, as long as sufficient channel dynamics are guaranteed.

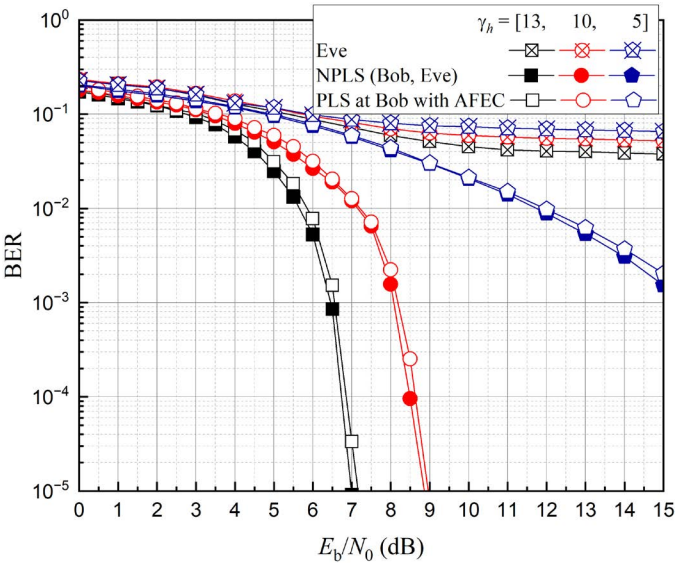

Fig. 7. BER performance comparison under dynamically changing K values and $\rho^2 = 0.5$.

V. Conclusion

In this paper, we evaluated an interleaving-based PLS scheme for satellite communication systems. Simulation results demonstrated that the interleaving-based PLS scheme offers robust security and high resilience against channel estimation errors. Under fixed Rician K-factor conditions, especially with a strong LoS component, Eve was completely able to achieve performance close to that of Bob, resulting in potential information leakage. Despite the advantages of the interleaving-based PLS scheme, appreciable information leakage may still occur under dominant LoS conditions. This implies that sufficient channel dynamics should be conditioned in order to achieve full capability of the PLS scheme. In future work, we aim to investigate hybrid approaches to further reduce the probability of successful decoding by Eve under dominant LoS conditions and higher channel correlation with the legitimate receiver.

References

[1] M. Giordani and M. Zorzi, "Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities," *IEEE Network*, vol. 35, no. 2, pp. 244-251, March/April. 2021.

[2] S. Dang, O. Amin, B. Shihada, and M. Alouini, "What should 6G be?," *Nature Electronics*, vol. 3, pp. 20-29, Jan. 2020.

[3] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, Firstquarter. 2020.

[4] M. Kang, S. Park and Y. Lee, "A Survey on Satellite Communication System Security," *Sensors*, vol. 24, no. 9, May. 2024.

[5] M. Mehic, L. Michalek, E. Dervisevic, P.Burdiak and M. Plakalovic, "Quantum Cryptography in 5G Networks: A Comprehensive Overview," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 302-346, Firstquarter. 2024.

[6] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8 pp. 1355-1387, Oct. 1975.

[7] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, June. 2008.

[8] H. Lee and S. Kim, "Evaluation of the Security Performance of Artificial Noise-Aided STBC Systems," *IET Communications*, vol. 17, pp. 1081-1090, April. 2023.

[9] H. Lee, S. Chan, S. Kim, "Efficient MIMO Signal Predistortion for Secrecy-Enhancing," *Electronics*, vol. 11, no. 9, April. 2022.

[10] T. Son, H. Lee and S. Kim, "A Secure Coded MIMO System Under Imperfect Channel Estimation," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 12, pp. 18834-18845, Dec. 2024.

[11] H. Lee and S. Kim, "Space-time block code based cooperative physical layer security schemes for LEO Satellite Systems," *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, South Korea, vol. 17, pp. 554-557, Oct. 2023.

[12] S. Chan, S. Kim, H-W. Kim, B-J. Ku and D. Oh, "Energy-efficient physical layer security schemes for low Earth orbit satellite systems," *International Journal of Satellite Communications and Networking*, vol. 42, no. 5, pp. 374-396, May. 2024.

[13] D. P. Souto *et al.*, "Emerging MIMO Technologies for 6G Networks," *Sensors*, vol. 23, no. 4, Feb. 2023.

[14] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.

[15] TS 38.212,V18.2.0, 3GPP, "5G;NR; Multiplexing and Channel Coding (Release 18)," May. 2024.