An Efficient BICM-based Physical Layer Security Scheme for Coded MIMO Systems

Thara Son, Sooyoung Kim
Jeonbuk National University
tharason@jbnu.ac.kr, sookim@jbnu.ac.kr

부호화된 MIMO 시스템을 위한 효율적인 BICM 기반 물리계층보안 방식

손타라, 김수영
전북대학교

Abstract

Physical layer security (PLS) exploits the random fluctuations of wireless channels to protect data without higher-layer encryption. However, most PLS schemes either assume perfect channel state information (CSI) or add extra error-correction coding to guard against CSI errors. This study explores the feasibility of employing a single encoder-decoder pair within an interleaving-based PLS framework. We concatenate the interleaving indices from each main information block into an extended index vector whose length closely matches that of the data payload. The encoder and decoder then alternate between processing the information blocks and the extended index vector using switch, S_1 and S_2. Simulation results demonstrate that this approach maintains strong security performance without the need for extra coding resources.

I. Introduction

Multi-input multi-output (MIMO) system enables spatial diversity which demands stronger security measures, especially for fifth-generation (5G) and beyond 5G systems [1]. To address this, physical-layer security (PLS) techniques which utilize channel state information (CSI) were considered to be effective means and numerous studies have proposed for various wireless system [2]-[5]. The artificial noise (AN) scheme injects noise into the signal so that the intended receiver can cancel it but any eavesdropper without CSI sees only interference [2]. The phase distortion (PD) scheme applies CSI-based phase shifts that the receiver reverses but an eavesdropper cannot [3]. Alternatively, a dynamic interleaving-based PLS scheme partitions data into channel-dependent sub-blocks and protects the interleaving indices with ancillary forward error correction (AFEC), achieving robustness against CSI errors [5].

Although these PLS schemes enhance transmission security, they suffer from several drawbacks. The AN-based scheme requires extra transmission power and degrades under imperfect channel conditions. The PD-based scheme depends on highly accurate CSI. Even the interleaving-based scheme, despite its robustness to CSI errors, requires an additional coding scheme. Motivated by this, we propose a method that eliminates the need for additional FEC, i.e., AFEC-combined in interleaving-based PLS schemes. We apply CSI-dependent interleaving to the information bits, which reduces index overhead. By concatenating interleaving indices from multiple information blocks into an extended index vector whose length closely matches that of the original information sequence, we can employ the same encoder and decoder without modification using the standard 5G encoder [6].

The paper is structured as follows. Section II reviews related work. Section III presents the proposed scheme. Section IV discusses the simulation results. Section V concludes the paper.

II. Related Works

In coded MIMO systems, bit-interleaved coded modulation (BICM) is essential for optimal performance. The dynamic interleaving-based PLS scheme in [4] uses CSI from channel $\mathbf{H}$ as the interleaving key. The transmitter (Alice) interleaved each data block according to $\mathbf{H}$ before transmission, and legitimate receiver (Bob) who shares the same CSI can reverse the permutation, while eavesdropper (Eve), knowing her channel $\mathbf{G}$, cannot. However, in practice, imperfect channel estimation produces an error-contaminated matrix $\tilde{\mathbf{H}}$, causing mismatches in the interleaving index. To resolve this, an AFEC-combined method was proposed in [5]. It corrects interleaving-index errors under CSI uncertainty and maintains robust security, but it requires system modifications and an additional coding layer.

III. Proposed Scheme

Figure 1 shows the transmitter block diagram of the proposed scheme. The information block is partitioned into L sub-blocks, $\mathbf{U} = [\mathbf{B}_1, ..., \mathbf{B}_i, ..., \mathbf{B}_L] = \{\mathbf{B}_i\}_{i=1}^{L}$. Each

$\mathbf{B}_i$ is interleaved via $\mathbf{B}'_i = \pi_{\delta_i}(\mathbf{B}_i)$, where δ_i is derived from the corresponding channel estimate $\mathbf{H}_i$. The interleaved sub-blocks $\mathbf{B}'_i$ are concatenated to form $\mathbf{U}'$ while the indices δ_i accumulate in the vector $\mathbf{d}$. $\mathbf{U}'$ then passes through switch S_1 into the 5G encoder to produce codeword $\mathbf{C}$ which is

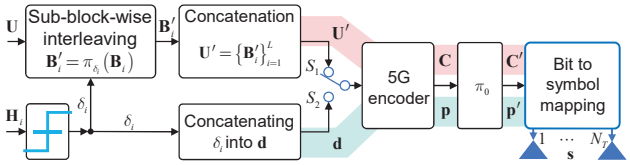

Figure 1. Operational principle of the proposed PLS scheme at the transmitter.

Figure 2 shows block diagram of the proposed scheme at the receiver. The noisy received sequence $\tilde{\mathbf{C}}'$ is first deinterleaved to get $\tilde{\mathbf{C}}$, which is then decoded to produce the interleaved information blocks $\hat{\mathbf{U}}' = \{\hat{\mathbf{B}}'_i\}_{i=1}^{L}$, through S_1. Simultaneously, for each decoded block, the receiver extracts the interleaving index from the imperfect channel estimate $\tilde{\mathbf{H}}_i$ and appends it to the index vector $\tilde{\mathbf{d}}$. This process continues to decode each incoming $\mathbf{C}'$ and accumulating interleaving index until the parity block $\tilde{\mathbf{p}}'$ arrives. At that point, the switch turns to S_2 and the concatenated vector

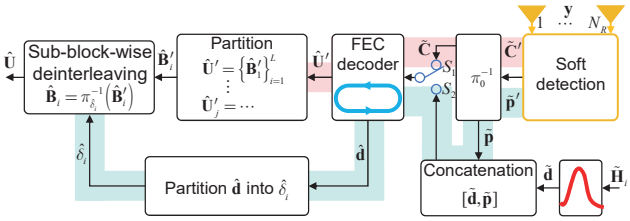

Figure 2. Operational principle of the proposed PLS scheme at the receiver.

IV. Simulation Results

We evaluate the proposed scheme using a 4×4 coded MIMO system with quadrature phase shift keying (QPSK)-modulated signals are transmitted over a frequency-flat Rayleigh fading channel. We employ the (6144, 4096) LDPC code from 5G standard [6]. Channel estimation error is modeled via the channel-estimation signal-to-noise ratio (SNR), β_h. The inteleaving index is set to 6 bits, leading to 96 sub-block per information block, $\{\mathbf{B}_i\}_{i=1}^{96}$, thus we need accumulated interleaving index from at least 7 information blocks,$\{\mathbf{U}_j\}_{j=1}^{7}$, to form vector $\mathbf{d}$ size of 4032 bits.

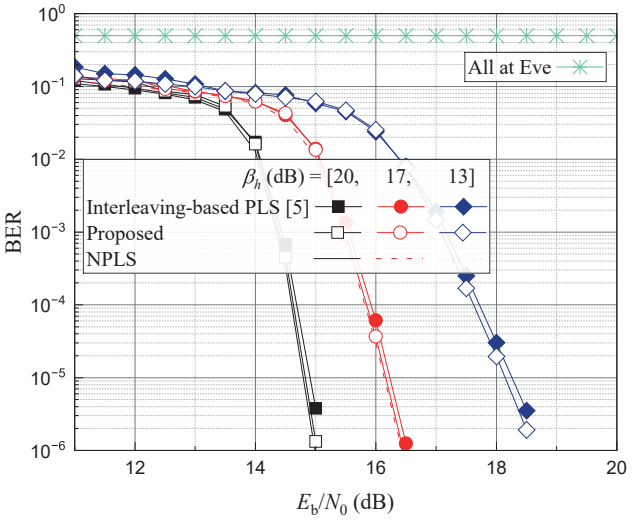

Figure 3. BER performance comparison using the (6144, 4096) LDPC code under various β_h values in a 4 × 4 MIMO system.

Figure 3 presents the simulation results, demonstrating that the proposed scheme outperforms the conventional interleaving-based PLS [5] and achieves BER performance nearly identical to a non-PLS (NPLS) system for channel estimation error levels of β_h = 20, 17, and 13 dB. This improvement arises from encoding the concatenated interleaving indices with a longer LDPC code and applying sub-block-wise interleaving only to systematic bits, thereby reducing index overhead.

V. Conclusion

This paper investigates the feasibility of switching the encoder and decoder between information blocks and the interleaving index. BER simulation results demonstrate that the system achieves performance gains without additional FEC, i.e., AFEC. However, sub-block-wise deinterleaving of the extended codeword may incur comparable delay and latency, especially for longer codewords.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation (NRF) of Korea grant funded by the Korea government (MSIT) (No RS-2024-00459799).

REFERENCES

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

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

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

[4] T. Son and S. Kim, "An Efficient PLS Scheme for Bit Interleaved Coded MIMO Systems," *2022 IEEE International Conference on Consumer Electronics-Asia*, pp. 1-3, Nov. 2022.

[5] 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.

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