An Efficient PLS Scheme for Coded MIMO Systems under Imperfect Channel Estimation

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

***Abstract*—In recent years, the concept of physical layer security (PLS) has emerged as a promising approach to supplement traditional cryptographic solutions. However, many PLS techniques rely on accurate knowledge of the channel state information (CSI) at the transmitter, which can be difficult to obtain in real-world scenarios. This paper presents a physical layer security scheme designed to enhance the security of a coded multi-input multi-output (MIMO) system operating under imperfect channel estimation conditions. To achieve a high level of security, we adopt a strategy that involves a channel-dependent interleaving scheme for the coded MIMO system, and combined additional simple coding schemes to prevent serious performance degradation caused by CSI error. Simulation results presented in this paper demonstrate that the proposed scheme effectively protects the transmitted data without any information leakage to the eavesdropper.**

***Index Terms*—physical layer security, multi-input multi-output, bit interleaved coded modulation, channel state information, estimation error, forward error correction.**

I. Introduction

The upcoming generation of communications is expected to prioritize high levels of security, secrecy, and privacy as essential requirements [1][2]. As wireless communications become more common and diverse, there is an increasing need for security solutions that can protect against unauthorized access and eavesdropping [2]-[4]. Especially, multiple-antenna technologies which enable higher spectral efficiency and improved system capacity [5][6], may require stronger security protection because of their inherent space diversity nature.

Although modern cryptography can protect information against attack, it does require complex mathematical manipulations in order to generate keys shared by the legitimate transmitter and receiver. Traditionally, this kind of security measure has primarily been implemented at higher layers of the communication protocol stack, such as encryption and authentication at the application layer or network layer. On the other hand, the physical layer security (PLS) scheme which was first introduced by Wyner in his wiretap channel model [7], is a method focusing on physical layer signal design for security protection.

The basic idea behind PLS is to exploit the randomness, variability, and unpredictability of the wireless channel to establish secure communication links. It takes advantage of the fact that wireless channels introduce noise, fading, interference, and other impairments, which can be utilized to provide confidentiality and integrity of transmitted data. For example, a number of researchers reported artificial noise (AN)-based PLS techniques, where AN is intentionally added to the transmitted signal to confuse potential eavesdroppers [8]. The legitimate receiver possesses the knowledge of this noise pattern, or the noise is designed to be located in the null space of the legitimate channel, so that only the eavesdropper, who lacks this knowledge, faces difficulty in decoding the signal [9][10]. However, all these schemes necessitate accurate information about the legitimate channel.

When employing forward error correction (FEC) schemes, we can make use of interleavers for PLS. This involves utilizing instantaneous channel state information (CSI) to create an adaptive interleaver [11]-[13]. More specifically, a PLS scheme was introduced to incorporate a time-varying interleaving index, with an additional FEC scheme used to safeguard the index information [11]. On the other hand, the impact of imperfect CSI in the intereleaved coded system was analyzed in orthogonal frequency division multiplexing scheme [12]. Furthermore, dynamic interleaving-based PLS scheme was applied to coded multi-input multi-output (MIMO) systems with bit interleaved coded modulation (BICM), and it was found that the CSI-dependent dynamic interleaving index effectively maintains secrecy [13]. However, it's important to note that with this scheme, imperfect CSI easily lead to serious performance degradation for the legitimate receiver.

Motivated by these findings, this paper proposes an efficient PLS scheme, specifically tailored for coded MIMO systems employing BICM under imperfect CSI conditions. Recognizing that the dynamic interleaving index can be prone to mismatch under imperfect CSI conditions, the proposed method incorporates an additional FEC scheme to protect interleaving index information. Unlike the previous approach proposed in [11], the proposed scheme is designed to transmit only the parity information of the additional encoding, thus incurring minimal additional bandwidth cost.

This paper is organized as follows. Following this introduction, Section II reviews the related works. After presenting the concept of coded MIMO systems with iterative detection, the concept of bit interleaving scheme for PLS is introduced.

This work was supported by the National Research Foundation (NRF) of Korea grant funded by the Korea government (MSIT) (No NRF-2021R1A2C1003121).

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

Section III describes the proposed scheme. Section IV presents the simulation results and discussions, and finally, Section V draws the conclusion.

II. Related Works

A. Coded MIMO system with iterative detection

Figure 1 illustrates a coded MIMO system with N_T transmit antennas and N_R receive antennas under consideration [6]. In the transmission process, the bit information vector $\mathbf{u}$ undergoes encoding to generate the codeword $\mathbf{c}$, which has a length of N. For this study, a low-density parity check (LDPC) coding scheme is employed as the forward error correction (FEC) code.

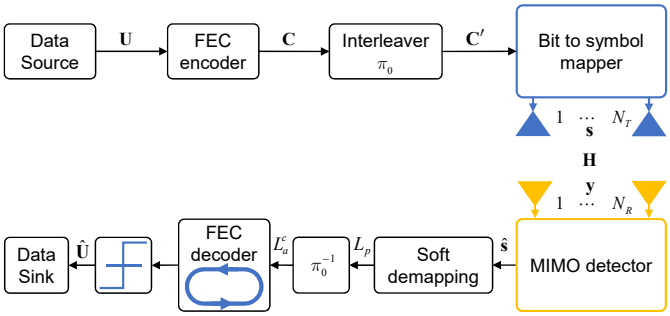

Fig. 1. Block diagram of a coded MIMO system with bit interleaver.

Once $N_T \times K$ codewords have been accumulated by using $\mathbf{U}$ with $N_T \times K$ information blocks, the next step is to perform bit interleaving over $\mathbf{C} = [\mathbf{c}_1, ..., \mathbf{c}_q, ..., \mathbf{c}_{N_T \times K}]^T$, where K represents the number of bits per transmit symbol, $\mathbf{c}_q$ is the q-th codeword vector, and the superscript $[\cdot]^T$ denotes the transpose of a matrix. The resulting interleaved coded bits in $\pi_0(\mathbf{C})$ are then partitioned into MIMO frames, each with a length of $N_T \times K$ bits, where π_0 is an interleaving operator with a fixed index. The transmitted symbol vector $\mathbf{s} = [s_1, s_2, ..., s_{N_T}]^T$ for each MIMO frame denotes the complex-valued $N_T \times 1$ is independently selected from a complex constellation O, which has a size of 2^K. The symbol vector that has been modulated is transmitted through a MIMO channel, and subsequently, the resulting symbol vector received for each MIMO frame can be expressed as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{y} = [y_1, y_2, ..., y_{N_R}]^T$ denotes the complex-valued $N_R \times 1$ received-symbol vector. Furthermore, the entries of $N_R \times N_T$ channel matrices $\mathbf{H} = [\mathbf{h}_1, ..., \mathbf{h}_j, ..., \mathbf{h}_{N_t}]$ are independent and identically distributed with zero mean and unit variance, where $\mathbf{h}_j$ represents the j-th column vector of $\mathbf{H}$. The vector $\mathbf{n}$ has $N_R \times 1$ dimensions and consists of independent, zero-mean complex Gaussian random variables with a variance of N_0 per dimension. The signal-to-noise ratio (SNR) is defined as $N_T E_s / N_0$, where E_s represents the transmitting symbol energy per antenna and N_0 represents the noise spectral density.

Once the receiver obtains the signal $\mathbf{y}$, it then proceeds to estimate the information $\hat{\mathbf{u}}$ using the decoder. Several approaches have been proposed to achieve this, including a tandem approach or a joint iterative detection and decoding (JIDD) method [6][14]. The simplest approach to extract soft bit information (SBI) is to perform symbol level detection followed by soft demapping, and then iteratively decode the resulting soft bits using a soft decoder. Another option is to use an minimum mean squared error (MMSE) detector to estimate the signal $\hat{\mathbf{s}}$, which is then processed by a soft demapper to produce SBI for an LDPC decoder. The resulting soft bits can then be iteratively decoded using a soft decoder.

B. Bit interleaving scheme for PLS

In coded modulation, bit interleaving plays a critical role in determining the decoding performance, as it can help to decorrelate the fading effects across codewords, and thus help to achieve space and time diversity. To ensure optimal performance, it is important to evenly distribute the most significant bit (MSB) and least significant bit (LSB) within the modulation symbols, as they exhibit different bit error rate (BER) performance behaviors [15]. Therefore, a diagonal bit interleaver is generally used across the codewords.

Our previous study proposed a bit interleaving scheme for a coded MIMO system operating at a wiretap channel, which can provide excellent security protection [13]. Fig. 2 illustrates the operational principle, where a transmitter (Alice) sends information using a coded MIMO scheme to a legitimate receiver (Bob), and a passive eavesdropper (Eve) tries to intercept the information. In this scenario, we assume that the channel matrix between Alice and Bob is denoted by $\mathbf{H}$, and the channel matrix between Alice and Eve is denoted by $\mathbf{G}$. Alice and Bob share the channel $\mathbf{H}$ between them, while Eve only knows the channel $\mathbf{G}$ between herself and Alice. We also assume that $\mathbf{H}$ and $\mathbf{G}$ are independent of each other, without loss of generality.

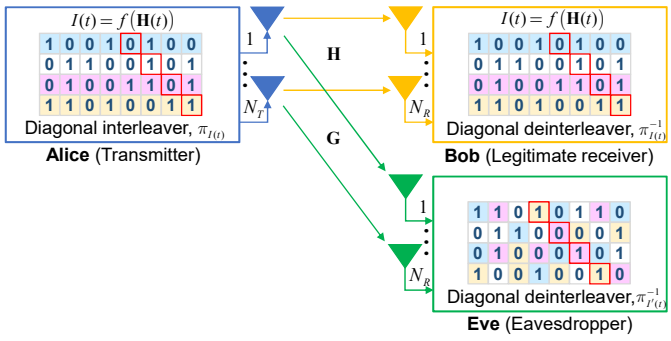

Fig. 2. Concept of the PLS scheme for the coded MIMO system with a dynamic interleaving index [13].

This method involves the dynamic variation of the interleaver index $I(t)$ at each time frame t of the interleaving process. The index $I(t)$ denotes the starting position of the diagonal interleaver within a codeword, and it is determined by a time-varying function of $\mathbf{H}$.

Since Eve lacks knowledge of the channel matrix $\mathbf{H}$, she is unable to correctly locate the index $I(t)$ of the diagonal interleaver. As a result, the interleaved information sent to the decoder will not be properly reordered, impeding the decoder's ability to recover the information correctly, and ultimately leading to degraded decoding performance. However, this method fails to provide secure information to Bob under imperfect CSI condition. This is because $I(t)$ is a function of $\mathbf{H}$, and imperfect estimation of $\mathbf{H}$ will easily mismatch the correct $I(t)$ at bob, leading to serious performance degradation.

III. The Proposed Methods

A. PLS for Coded MIMO system under imperfect CSI

The PLS scheme proposed in this research is aimed at improving the security of a coded MIMO system that operates under imperfect channel estimation conditions. Fig. 3 shows the operation principle of the proposed PLS scheme for the coded MIMO system at the transmitter side, where $N_T \times K$ codewords with a length of N bits are accumulated to $\mathbf{C}$ for interleaving. Instead of interleaving $\mathbf{C}$ as in the conventional scheme in Fig. 2, the proposed scheme first involves dividing $\mathbf{C}$ into multiple sub-blocks of $\mathbf{B}_1, \mathbf{B}_2, ...\mathbf{B}_l$, where l is the number of sub-blocks in $\mathbf{C}$, as shown in Fig. 3.

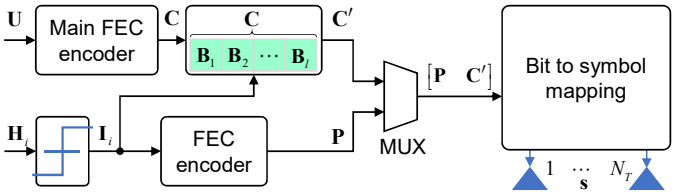

Fig. 3. Operational principle of the proposed PLS scheme at the transmitter, with CSI error protected interleaving index.

Each sub-block contains L MIMO frames with the size of $N_T \times K$ bits, and thus $l = N/L$. With this, sub-block-wise interleaving is performed. Letting $\mathbf{H}_i$ is a CSI matrix for $\mathbf{B}_i$, $1 \leq i \leq l$, the binary interleaving index vector $\mathbf{I}_i$ for $\mathbf{B}_i$ is estimated with $\mathbf{H}_i$. Since $\mathbf{I}_i$ basically indicates the starting point of interleaving process among L bits, $\mathbf{I}_i$ will be an integer value from 0 to $L-1$ consisting of $Z = \log_2 L$ bits. By using $\mathbf{I}_i$, the interleaved version of $\mathbf{B}_i$, $\mathbf{B}'_i = \pi_{\mathbf{I}_i}(\mathbf{B}_i)$ is produced.

Afterward, we concatenate $\mathbf{I}_1$ to $\mathbf{I}_l$ each with Z bit length, and produce m bits parity check vector $\mathbf{P}$ from systematic encoding process with another LDPC code. The purpose of this encoding is to protect CSI error contained $\mathbf{I}'_1$ to $\mathbf{I}'_l$, and properly locate interleaving index at the receiver. Fig 4 illustrates the transmission process of a coded MIMO system by using the proposed scheme illustrated in Fig. 3. First, the parity checks $\mathbf{P}$ is sent to the bit to symbol mapping processor with the unit of $N_T \times K$ bits for $\lambda = m/(N_T \times K)$ intervals. Next, all $\mathbf{B}'_i$s are serially sent to the symbol mapping block for modulation and then sent through the N_T antennas. Therefore, the proposed scheme requires additional information transmission of m bits, $m << N_T \times K \times N$, i.e., $\lambda << N$. Fig. 4 shows the flow chart of the PLS process at the transmitter.

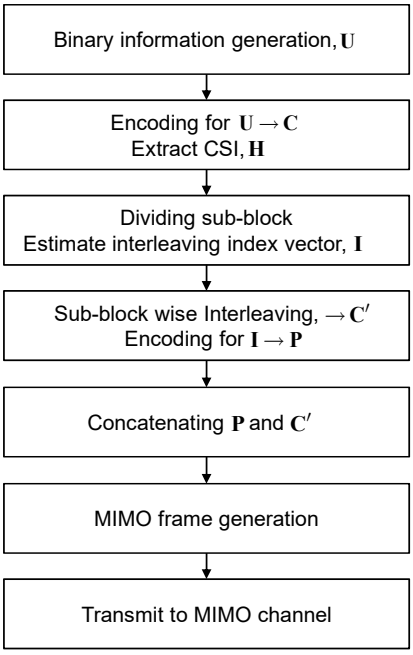

Fig. 4. Flowchart of the proposed PLS transmission process.

At the receiver, we first receive and detect soft bit information of the parity bits, $\hat{\mathbf{P}}$ as well as that of the all the received blocks $\hat{\mathbf{B}}'_i$s using soft detection and soft demapping techniques. While detecting the soft bit information usually in the form of log-likelihood ratio (LLR), we estimate the CSI at the receiver, which includes a channel estimation error. Fig. 5 illustrates the detailed process at the receiving end. Second, the estimated CSI is converted into LLR values with the same sized vector as $\mathbf{I}'_{i(LLR)}$, and concatenate all $\mathbf{I}'_{1(LLR)}$ to $\mathbf{I}'_{l(LLR)}$ in order to form the systematic part corresponding to $\hat{\mathbf{P}}$.

Third, decoding is performed to extract the proper interleaving index vectors, $\hat{\mathbf{I}}_1$ to $\hat{\mathbf{I}}_l$, regarding the concatenated systematic part and $\hat{\mathbf{P}}$ as a received codeword. Fourth, sub-block-wise deinterleaving is performed for $\hat{\mathbf{B}}'_i$ using $\hat{\mathbf{I}}_i$ to get $\hat{\mathbf{B}}_i = \pi^{-1}_{\hat{\mathbf{I}}_i}(\hat{\mathbf{B}}'_i)$. Fifth, all $\hat{\mathbf{B}}_i$ are serially concatenated to form $N_T \times K$ codewords which are ready for the input to the LDPC decoding. Finally, each codeword with its LLR values, is passed through an LDPC decoder for iterative soft decoding, and the final estimation of information is produced.

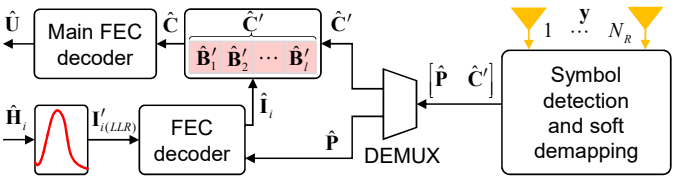

Fig. 5. Receiving process of the proposed PLS scheme.

IV. Simulation Results

It was shown that the conventional PLS method using channel dependent interleaving index for the coded MIMO

system worked very well where perfect CSI is available between Bob and Eve, showing BER performance of 0.5 at Eve [13]. However, this method may invoke serious performance degradation at Bob under imperfect CSI.

Fig. 6 compares bit error rate (BER) performances of various schemes under perfect CSI conditions. In the simulation, QPSK modulated signals are transmitted via 4×4 coded MIMO schemes over a frequency-flat Rayleigh fading channel. As an FEC scheme, LDPC code with a code rate of $8/9$ and N of $16,200$ bits, as specified in the digital video broadcasting via satellite - 2nd generation (DVB-S2) standard, is used. Furthermore, we utilize MMSE detection method followed by a soft demapping method for the LDPC decoder. For the proposed scheme, we set $L = 128$ bits, and thus $Z = 7$ bits for each sub-block. By utilizing a short $(1369, 889)$ LDPC code for encoding of interleaving index, $\mathbf{P} = 480$ bits. Since we are using the $(16200, 14400)$ LDPC code with a rate of $8/9$ for the source information, additional transmission of 480 bits corresponds to 0.37% increase of the codeword length.

According to the findings in Fig. 6, the system without PLS exhibits identical BER performances at both Bob and Eve, resulting in no secrecy protection. In contrast, under perfect CSI condition, the system with either the conventional or proposed PLS scheme achieves high security protection by preserving a good BER performance at Bob while introducing an acceptable BER of 0.5 at Eve. Additionally, the proposed scheme shows a marginal power loss less than 0.05 dB, attributed to the incorporation of an additional FEC mechanism for interleaving index, requiring additional redundancy for $\mathbf{P}$.

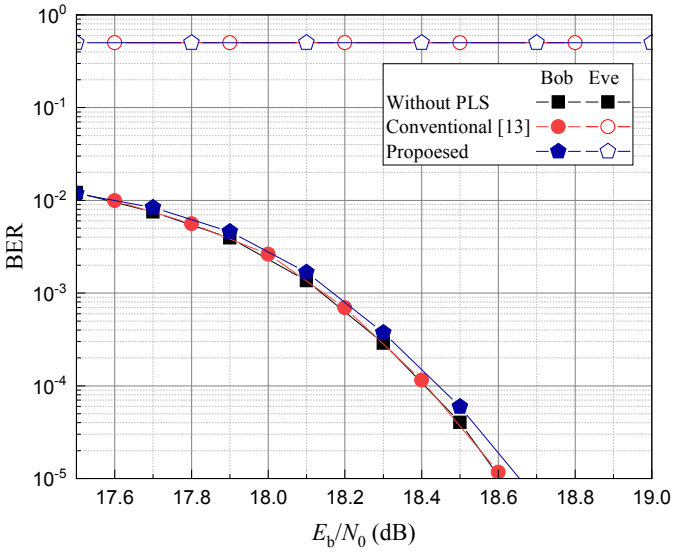

Fig. 6. BER performance comparison for a 4×4 MIMO system under perfect CSI.

On the other hand, Fig. 7 presents the BER performance of the proposed scheme, where the estimated channel matrix under imperfect CSI is modeled as follows [16]:

$$\hat{\mathbf{H}} = \sqrt{1-\rho^2}\mathbf{H} + \sqrt{\rho^2}\tilde{\mathbf{H}}, \tag{2}$$

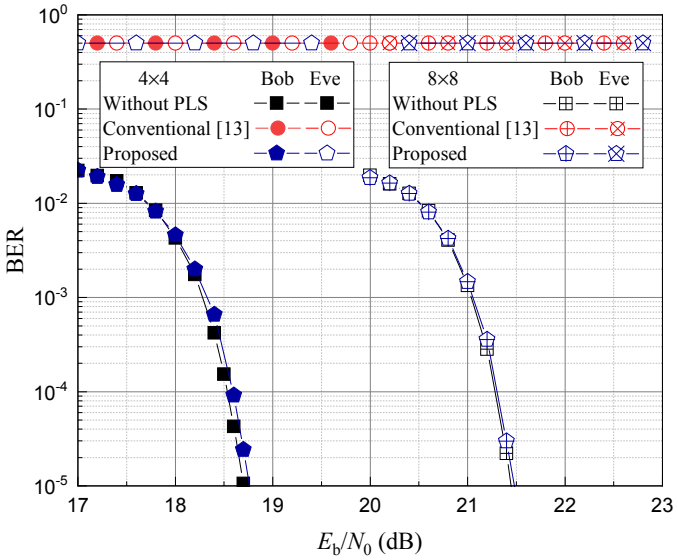

Fig. 7. BER performance comparison of the proposed PLS scheme under imperfect CSI, $\rho^2 = 10^{-3}$.

where $\mathbf{H}$ and $\hat{\mathbf{H}}$ are channel matrices with perfect and imperfect CSI, respectively, and ρ^2 denotes the variance of the estimation error. In the simulation, we used the same modulation and coding scheme as in the case of Fig. 6, and added the performance for a 8×8 system.

The proposed scheme requires additional transmission of $\mathbf{P} = 480$ bits for every $129,600$ and $259,200$ bits for 4×4 and 8×8 systems, respectively. The above figure corresponds to about 0.37% and 0.19% increase of codeword lengths for 4×4 and 8×8 systems, respectively, and thus almost no change in the effective code rate. The simulation results in the figure clearly demonstrate that the proposed scheme accurately locates proper interleaving indices at Bob, showing exactly the same performance as in the case without any PLS scheme. On the other hand, Eve could not recover any information, showing BER performance of 0.5.

The simulation results demonstrated in this paper prove that the proposed scheme with CSI-dependent interleaving indices can function as a key to protect the information from eavesdroppers. Furthermore, even in the presence of CSI errors, the interleaving indices can be reliably restored at the receiver by sacrificing a small amount of additional information for a simple FEC coding scheme. This ensures effective concealment of the information from Eve. However, it is essential to note that if Eve is granted ample time to conduct an exhaustive search of all possible interleaving indices, spanning from 0 to L in each block $\mathbf{B}_i$, the secrecy of the information will be compromised.

V. Conclusion

This study proposed a new PLS scheme for a bit-interleaved coded MIMO system operating under imperfect channel conditions. The proposed scheme utilizes CSI-dependent dynamic interleaving indices to protect information leakage to the

eavesdropper, and add a simple FEC code to recover CSI-error contaminated interleaving indices at the legitimate receiver. The simulation results in this paper reveal that the eavesdropper fails to acquire any information, regardless of CSI error conditions. Moreover, due to the simple additional FEC scheme, the legitimate receiver successfully recovers the original information even under imperfect channel estimation. In our future research, we aim to explore the optimum FEC coding scheme for various channel error conditions as well as MIMO structures.

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] "5G vision," White Paper, Feb. 2015.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. -K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, April 20188.

[4] H. A. Suraweera, C. B. Chae, and J. A. Choi, "Physical layer security in wireless networks: a tutorial," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

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

[6] M. Zhang and S. Kim, "Evaluation of MMSE-Based Iterative Soft Detection Schemes for Coded Massive MIMO System," *IEEE Access*, vol. 7, pp. 10166-10175, 2019

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

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

[9] Y. Wen, M. Yoshida, J. Zhang, Z. Chu, P. Xiao and R. Tafazolli, "Machine Learning based Attack Against Artificial Noise-Aided Secure Communication," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, pp. 1-6, 2019.

[10] X. Zhou and M. R. McKay, "Secure Transmission With Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology,*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[11] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento and F. Dias, "Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime," *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 356-360, Mar. 2016

[12] I. Ajayi, Y. Medjahdi, L. Mroueh and F. Kaddour, "Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information," *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Semarang, Indonesia, pp. 299-304, 2021.

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

[14] S. Ahmed and S. Kim, "Efficient SIC-MMSE MIMO Detection with Three Iterative Loops," *AEU - International Journal of Electronics and Communications*, vol. 72, pp. 65-71, 2017

[15] X. Jin, S. Kim, H. W. Kim and B. -J. Ku, "An Efficient MIMO Scheme for Integrated Mobile Satellite System," *IEEE International Symposium on Consumer Electronics (ISCE)*, pp. 59-60, 2013

[16] Z. Rezki, A. Khisti and M. -S. Alouini, "On the Secrecy Capacity of the Wiretap Channel With Imperfect Main Channel Estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652-3664, Oct. 2014