Evaluation of physical-layer security schemes for space-time block coding under imperfect channel estimation

Seunggyu Hwang, Hyein Lee, Sooyoung kim
IT Convergence Research Center, Jeonbuk National University
Jeonju, Korea
{seunggyuh, leehyein96, sookim}@jbnu.ac.kr

***Abstract*—With the advent of massive machine type of communications, security protection becomes more important than ever. Efforts have been made to impose security protection capability to physical-layer signal design, so called physical-layer security (PLS). The purpose of this paper is to evaluate the performance of PLS schemes for a multi-input-multi-output (MIMO) systems with space-time block coding (STBC) under imperfect channel estimation. Three PLS schemes for STBC schemes are modeled and their bit error rate (BER) performances are evaluated under various channel estimation error environments, and their performance characteristics are analyzed.**

***Index Terms*—physical-layer security (PLS), multiple-input multiple-output (MIMO), space time block coding (STBC), channel estimation error**

I. Introduction

Since the development of fourth-generation (4G) wireless communications, multi-input-multi-output (MIMO) systems using multiple transmit and receive antennas have emerged. Space time block coding (STBC) schemes are used to improve bit error rate (BER) performance by sending the same message signal through multiple transmit antennas at different times and spaces. The first STBC scheme was proposed by Alamouti to achieve the maximum diversity gain using an orthogonal signal design for two transmit antennas [1]. Afterwards, quasi-orthogonal STBC (QO-STBC) methods were developed for the system with more than two transmit antennas, satisfying the full rate [2].

As MIMO systems are widespread with increasing communication volume, concerns on illegal wiretapping are increased accordingly. To the end, a number of physical-layer security (PLS) schemes for STBC have been proposed [3]–[5]. The basic principle of these methods is to utilize the channel information of the legitimate channel. One of the most popular ways is to inject artificial noise (AN) which lies on the null space of the legitimate channel so that it can be cancelled at the legitimate receiver, while the injected AN plays serious interference to the illegal receiver [6]. The AN-aided PLS scheme for the Alamouti code was proposed to enhance the security [3]. Although this scheme achieved excellent security protection against an illegal eavesdropper, adding AN certainly requires additional power.

Later, a technique to add artificial interference (AI) was proposed in order not to waste additional power for security protection, and it was applied so-called linear decoding QO-STBC (LD-QO-STBC) [4]. Recently, another PLS method has been proposed, where the phase of the transmit signal was distorted for security protection [5]. The excellency of this method lied in that it can achieve full diversity gain for a system with more than two transmit antenna, because the phase distortion (PD) was made in a way to accomplish orthogonal channel matrix at the receiving end. Therefore, this method effectively prevents wiretapping and also achieves excellent error performance with a simple detection scheme.

Because all of the above mentioned schemes utilize the channel state information (CSI) of the legitimate channel, error performance as well as security protection at the legitimate receiver should be conditioned on accurate CSI. However, channel estimation errors are inevitable in practical fading channels, especially for a fast-fading environment. For this reason, this study evaluates the performance of the previously mentioned PLS methods under imperfect CSI conditions. For a fair comparison, we first derive equations for the PLS signals for a 4×1 system. Afterwards, we derive equations to detect signals at the legal and illegal receivers, respectively, by using an imperfect CSI model. In addition, we compare and investigate the characteristics of BER performance simulation results, and analyze how the channel estimation errors are affected to each method.

The rest of this paper is organized as follows. Section II first introduces a wiretap channel model with the aforementioned PLS methods to pursue security, and then presents mathematical representation of the signal waveforms with PLS capabilities for a 4×1 system. Section III is dedicated to derive

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

formulas for signal detection under imperfect CSI. Section IV presents various simulation results, and investigates the BER performance under various error environments. Finally, Section V draws the conclusion.

II. PLS SCHEMES FOR STBC

A. System model

We consider a wireless network utilizing STBC equipped with a PLS scheme, that consist of three nodes, as shown in Fig. 1. A transmitter node is referred to as Alice and has four transmit antennas with a STBC encoding matrix, $\mathbf{X}$ to transmit $\mathbf{s} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \end{bmatrix}^T$ which is a complex modulation symbol vector for four time periods. A legitimate receiver is referred to as Bob, and an eavesdropper is referred to as Eve. The security protected signals, $\mathrm{T}(\mathbf{X}, \tilde{\mathbf{h}})$ are transmitted via $\mathbf{h}$ and $\mathbf{g}$ to Bob and Eve, respectively, where $\mathbf{h}$ and $\mathbf{g}$ are channel gain vectors from four transmit antennas of Alice to Bob and Eve respectively. In addition, transmitter Alice and legitimate receiver Bob share the estimated CSI vector at Bob, $\tilde{\mathbf{h}}$.

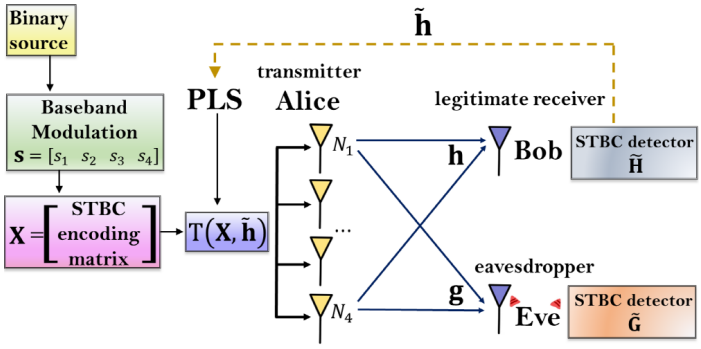

Fig. 1. A wiretap channel model with STBC scheme

Bob and Eve have one receive antenna, respectively, and they have their own detector to retrieve information for the used STBC scheme. The detector at Bob and Eve utilizes $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{G}}$, respectively, which are estimated channel matrices with errors.

B. AN-aided PLS

A previous study reported a PLS scheme for the Alamouti code by adding AN which can only be nulled out at the legitimate receiver [3]. Because the eavesdropper cannot remove AN, security can be obtained. We refer to this method as AN-PLS in this paper. Here, we derive equations for the AN-PLS applied to the 4×1 QO-STBC scheme with the following encoding matrix [2].

$$\mathbf{X}_{\mathrm{Q}} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ s_3 & s_4 & s_1 & s_2 \\ -s_4^* & s_3^* & -s_2^* & s_1^* \end{bmatrix}. \tag{1}$$

The encoding matrix for the AN-PLS can be represented as follows:

$$\mathbf{X}_{\mathrm{Q}} + \mathbf{X}_{\mathrm{AN}} = \begin{bmatrix} s_1 + \psi_{11} & s_2 + \psi_{12} & s_3 + \psi_{13} & s_4 + \psi_{14} \\ -(s_2 + \psi_{21})^* & (s_1 + \psi_{22})^* & -(s_4 + \psi_{23})^* & (s_3 + \psi_{24})^* \\ s_3 + \psi_{31} & s_4 + \psi_{32} & s_1 + \psi_{33} & s_2 + \psi_{34} \\ -(s_4 + \psi_{41})^* & (s_3 + \psi_{42})^* & -(s_2 + \psi_{43})^* & (s_1 + \psi_{44})^* \end{bmatrix}, \tag{2}$$

where $\mathbf{X}_{\mathrm{AN}}$ represents an AN matrix with the same size as $\mathbf{X}_{\mathrm{Q}}$, $\psi_{ik} = \beta_{ik}\nu$, β_{ik} denotes a coefficient of AN for the i-th time slot at the k-th antenna, and ν is the complex Gaussian AN with zero-mean and unit variance.

The elements of $\mathbf{X}_{\mathrm{AN}}$ should satisfy the following equation:

$$\forall_i \sum_k (\mathbf{X}_{\mathrm{AN}})_{ik} h_k = 0, \tag{3}$$

where $(\mathbf{X}_{\mathrm{AN}})_{ik}$ is the element of $\mathbf{X}_{\mathrm{AN}}$ in the i-th row and k-th column and h_k is the CSI from the k-th transmit antenna from the Alice to Bob. For example, when i=1, we can find the following set of solutions for β_{1k} as follows:

$$\begin{cases} \beta_{11} = \pm h_2 \\ \beta_{12} = \mp h_1 \\ \beta_{13} = \pm h_4 \\ \beta_{14} = \mp h_3 \end{cases} \text{or} \begin{cases} \beta_{11} = \pm h_3 \\ \beta_{12} = \pm h_4 \\ \beta_{13} = \mp h_1 \\ \beta_{14} = \mp h_2 \end{cases} \text{or} \begin{cases} \beta_{11} = \pm h_4 \\ \beta_{12} = \mp h_3 \\ \beta_{13} = \pm h_2 \\ \beta_{14} = \mp h_1 \end{cases}. \tag{4}$$

The same principle is applied to find AN when $1<i\leq 4$. Since AN is designed to be the null space of Bob's CSI, Eve cannot cancel AN.

C. AI-aided PLS

The LD-QO-STBC method reduced the complexity of signal detection by applying a rotation operator to the encoding matrix of QO-STBC scheme [7]. However, this method has a problem of having zero-crossing signal value. A PLS scheme for the LD-QO-STBC was proposed by introducing AI [4], and we refer to this method as AI-PLS in this paper. The encoding matrix of the 4×1 LD-QO-STBC scheme is represented as linear combination of s_i, as follows:

$$\mathbf{X}_{\mathrm{L}} = \frac{1}{\sqrt{2}} \begin{bmatrix} s_1 + s_3 & s_2 + s_4 & s_3 - s_1 & s_4 - s_2 \\ -s_2^* - s_4^* & s_1^* + s_3^* & s_2^* - s_4^* & s_3^* - s_1^* \\ s_3 - s_1 & s_4 - s_2 & s_1 + s_3 & s_2 + s_4 \\ s_2^* - s_4^* & s_3^* - s_1^* & -s_2^* - s_4^* & s_1^* + s_3^* \end{bmatrix}. \tag{5}$$

Some of the elements in $\mathbf{X}_{\mathrm{L}}$ can have the null value because each element consists of the sum of two symbols. In addition, if an entry is zero value, one of the other entry in the same row has a $2s_i$ value. AI was designed to prevent this zero

value transmission as well as to impose security protection as follows:

$$\begin{cases} w_{ik} = \frac{x_{i(k+2)}h_{k+2}}{2} & \\ w_{i(k+2)} = -\frac{x_{i(k+2)}h_k}{2} & \text{if } k\text{=1,2 and } x_{ik} = 0, \\ w_{ik} = \frac{x_{i(k-2)}h_{k-2}}{2} & \\ w_{i(k-2)} = -\frac{x_{i(k-2)}h_k}{2} & \text{if } k\text{=3,4 and } x_{ik} = 0, \\ w_{ik} = 0 & x_{ik} \neq 0,\ x_{i(k\pm2)} \neq 0, \end{cases} \tag{6}$$

where x_{ik} denotes the i-th row and k-th column entry of (5), and w_{ik} denotes AI added to x_{ik}. Therefore, the encoding matrix with AI is expressed as follows:

$$\mathbf{X}_{\mathrm{L}} + \mathbf{X}_{\mathrm{AI}} = \left[x_{ik} + w_{ik}\right]_{4\times4}, \tag{7}$$

where $\mathbf{X}_{\mathrm{AI}}$ represents an AI matrix with the same size as $\mathbf{X}_{\mathrm{L}}$ and consists of AI in (6). As in the previous case, the AI is deigned by using Bob's CSI, it can be cancelled only at Bob, not Eve.

D. Phase-distortion-aided PLS

The aforementioned PLS schemes required additional energy for introducing artificial signals [3] [4], and also incurred serious high peak-to-average power ratio (PAPR) problem. In order to solve these problems, a new PLS method for distorting the phase of the transmit signal was proposed [5]. In this method, phase distortion was introduced to a non-orthogonal encoding matrix so that the channel matrix at the receiver can be a full orthogonal matrix. By this way, an excellent security protection was achieved, and the full-rate and full-diversity was also achieved leading to better error rate performance. We refer to this method as PD-PLS in this paper.

To get an encoding matrix for the 4×1 PD-PLS system, the following non-orthogonal matrix is first used [5]:

$$\mathbf{X}_{\mathrm{R}} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2 & s_1 & -s_4 & s_3 \\ -s_3 & s_4 & s_1 & -s_2 \\ -s_4 & -s_3 & s_2 & s_1 \end{bmatrix}. \tag{8}$$

Afterwards, the phase distortion is applied, leading to the following encoding matrix:

$$\mathbf{X}_{\mathrm{P}} = \left[e^{-j\angle h_1}\mathbf{x}_1 \quad e^{-j\angle h_2}\mathbf{x}_2 \quad \dots \quad e^{-j\angle h_4}\mathbf{x}_4\right], \tag{9}$$

where $j = \sqrt{-1}$, $\angle h_k$ denotes the phase of h_k, and $\mathbf{x}_k$ is the k-th column vector of $\mathbf{X}_{\mathrm{R}}$. Because the phase distortion introduced in (9) leads to the null phase at Bob, the received signal at Bob will have only amplitude value of the channel gain. This eventually leads to a real-valued orthogonal channel matrix. However, Eve will suffer from serious interference caused by phase distortion.

III. Security protected signal detection under imperfect CSI

A. Channel estimation error

Channel estimation error for a channel gain h is usually modelled as follows [8]–[12]:

$$h = \sqrt{1-\rho^2}\tilde{h} + \sqrt{\rho^2}e, \tag{10}$$

where $\tilde{h}$ is the estimated CSI, with an error of e which has the variance of ρ^2 and zero-mean. In this way, the estimated $\tilde{h}$ with e can be considered as the orthogonal projection of h on the estimation plane, i.e., least mean squared error estimation of h [8].

Referring to the wiretap channel model in Fig. 1, the channel vectors at Bob and Eve can be represented as follows:

$$\mathbf{h} = \sqrt{1-\rho^2}\tilde{\mathbf{h}} + \sqrt{\rho^2}\mathbf{e}_{\mathrm{b}}, \tag{11}$$

$$\mathbf{g} = \sqrt{1-\rho^2}\tilde{\mathbf{g}} + \sqrt{\rho^2}\mathbf{e}_{\mathrm{e}}, \tag{12}$$

where $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ are the estimated CSI vectors at Bob and Eve, with error vectors of $\mathbf{e}_{\mathrm{b}}$ and $\mathbf{e}_{\mathrm{e}}$, respectively. Each element of $\mathbf{e}_{\mathrm{b}}$ and $\mathbf{e}_{\mathrm{e}}$ has the variance of ρ^2 and zero-mean. In the following, we use $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ during the detection processes on the condition that Alice use $\tilde{\mathbf{h}}$ for PLS.

B. Signal detection of AN-PLS

With the AN-PLS under imperfect CSI, the signal received by Bob, $\mathbf{y}_{\mathrm{b}}$ can be represented as follows:

$$\mathbf{y}_{\mathrm{b}} = \mathbf{X}_{\mathrm{Q}}\mathbf{h} + \mathbf{n}_{\mathrm{b}} + \boldsymbol{\varepsilon}_{\mathrm{AN}}, \tag{13}$$

where $\mathbf{n}_{\mathrm{b}}$ is an additive white Gaussian noise (AWGN) at Bob and $\boldsymbol{\varepsilon}_{\mathrm{AN}}$ refers to uncancelled AN because of imperfect CSI. In this case, AN will not be perfectly cancelled at the receiver. For example, the first element of $\boldsymbol{\varepsilon}_{\mathrm{AN}}$ can be represented as follows, if we use the first solution set of (4).

$$(\boldsymbol{\varepsilon}_{\mathrm{AN}})_1 = \frac{\sqrt{\rho^2}}{\sqrt{1-\rho^2}}\begin{bmatrix}\psi_{11} & \psi_{12} & \psi_{13} & \psi_{14}\end{bmatrix}\mathbf{e}_{\mathrm{b}}. \tag{14}$$

Upon receiving $\mathbf{y}_{\mathrm{b}}$, Bob conducts signal detection using the following zero-forcing method:

$$\hat{\mathbf{s}}_{\mathrm{b}} = (\tilde{\mathbf{H}}_{\mathrm{Q}}^H\tilde{\mathbf{H}}_{\mathrm{Q}})^{-1}\tilde{\mathbf{H}}_{\mathrm{Q}}^H\mathbf{y}_{\mathrm{b}}, \tag{15}$$

where $\hat{\mathbf{s}}_{\mathrm{b}}$ is the detected signal at Bob, and $\tilde{\mathbf{H}}_{\mathrm{Q}}$ is the following channel matrix:

$$\tilde{\mathbf{H}}_{\mathrm{Q}} = \begin{bmatrix} \tilde{h}_1 & \tilde{h}_2 & \tilde{h}_3 & \tilde{h}_4 \\ \tilde{h}_2^* & -\tilde{h}_1^* & \tilde{h}_4^* & -\tilde{h}_3^* \\ \tilde{h}_3 & \tilde{h}_4 & \tilde{h}_1 & \tilde{h}_2 \\ \tilde{h}_4^* & -\tilde{h}_3^* & \tilde{h}_2^* & -\tilde{h}_1^* \end{bmatrix}. \tag{16}$$

Furthermore, $\tilde{h}_k$ is the k-th element of $\tilde{\mathbf{h}}$, and $\tilde{\mathbf{H}}_{\mathrm{Q}}^H$ is the Hermitian of $\tilde{\mathbf{H}}_{\mathrm{Q}}$. In this detection process, the imperfectly cancelled AN term in $\boldsymbol{\varepsilon}_{\mathrm{AN}}$ will induce performance degradation.

On the other hand, Eve receives the following signal because it cannot cancel AN:

$$\mathbf{y}_{\mathrm{e}} = (\mathbf{X}_{\mathrm{Q}} + \tilde{\mathbf{X}}_{\mathrm{AN}})\mathbf{g} + \mathbf{n}_{\mathrm{e}}, \tag{17}$$

where where $\tilde{\mathbf{X}}_{\mathrm{AN}}$ is an AN matrix with an estimation error, $\mathbf{n}_{\mathrm{e}}$ is AWGN of Eve and the detected signal at Eve is as follows:

$$\hat{\mathbf{s}}_{\mathrm{e}} = (\tilde{\mathbf{G}}_{\mathrm{Q}}^{H}\tilde{\mathbf{G}}_{\mathrm{Q}})^{-1}\tilde{\mathbf{G}}_{\mathrm{Q}}^{H}\mathbf{y}_{\mathrm{e}}, \tag{18}$$

where $\tilde{\mathbf{G}}_{\mathrm{Q}}$ is the channel matrix of Eve for QO-STBC and $\tilde{\mathbf{G}}_{\mathrm{Q}}^{H}$ is the Hermitian of $\tilde{\mathbf{G}}_{\mathrm{Q}}$. Since the AN contained in $\mathbf{y}_{\mathrm{e}}$ operates as a serious noise in the signal detection process, Eve suffers from severe BER performance degradation.

C. Signal detection of AI-PLS

With the AI-PLS, the received signal at Bob can be represented as follows:

$$\mathbf{y}_{\mathrm{b}} = \mathbf{X}_{\mathrm{L}}\mathbf{h} + \mathbf{n}_{\mathrm{b}} + \boldsymbol{\varepsilon}_{\mathrm{AI}}, \tag{19}$$

where $\boldsymbol{\varepsilon}_{\mathrm{AI}}$ refers to uncancelled AI because of imperfect CSI. For example, when $x_{11} = 0$, the first element of $\boldsymbol{\varepsilon}_{\mathrm{AI}}$ can be represented as follows:

$$(\boldsymbol{\varepsilon}_{\mathrm{AI}})_1 = \frac{x_{13}\sqrt{\rho^2}}{2\sqrt{1-\rho^2}}(e_{\mathrm{b},1}h_3 - e_{\mathrm{b},3}h_1), \tag{20}$$

where $e_{\mathrm{b},k}$ represents the k-th element of $\mathbf{e}_{\mathrm{b}}$.

Then, the signal detection at Bob is performed as follows:

$$\hat{\mathbf{s}}_{\mathrm{b}} = \frac{1}{\sum_{k=1}^{4}\left\|\tilde{h}_k\right\|^2}\tilde{\mathbf{H}}_{\mathrm{L}}^{H}\mathbf{y}_{\mathrm{b}}, \tag{21}$$

where $\tilde{\mathbf{H}}_{\mathrm{L}}$ is the channel matrix of the LD-QO-STBC as follows:

$$\tilde{\mathbf{H}}_{\mathrm{L}} = \begin{bmatrix} \tilde{h}_1 - \tilde{h}_3 & \tilde{h}_2 - \tilde{h}_4 & \tilde{h}_1 + \tilde{h}_3 & \tilde{h}_2 + \tilde{h}_4 \\ \tilde{h}_2^* - \tilde{h}_4^* & \tilde{h}_3^* - \tilde{h}_1^* & \tilde{h}_2^* + \tilde{h}_4^* & -\tilde{h}_1^* - \tilde{h}_3^* \\ \tilde{h}_3 - \tilde{h}_1 & \tilde{h}_4 - \tilde{h}_2 & \tilde{h}_1 + \tilde{h}_3 & \tilde{h}_2 + \tilde{h}_4 \\ \tilde{h}_4^* - \tilde{h}_2^* & \tilde{h}_1^* - \tilde{h}_3^* & \tilde{h}_2^* + \tilde{h}_4^* & -\tilde{h}_1^* - \tilde{h}_3^* \end{bmatrix}. \tag{22}$$

As in the previous case, the imperfectly cancelled AI term in $\boldsymbol{\varepsilon}_{\mathrm{AI}}$ will induce performance degradation.

On the other hand, Eve receives the following signals because it cannot cancel AI:

$$\mathbf{y}_{\mathrm{e}} = (\mathbf{X}_{\mathrm{L}} + \tilde{\mathbf{X}}_{\mathrm{AI}})\mathbf{g} + \mathbf{n}_{\mathrm{e}}, \tag{23}$$

where $\tilde{\mathbf{X}}_{\mathrm{AI}}$ is an AI matrix with an estimation error. In addition, the detected signal at Eve is as follows:

$$\hat{\mathbf{s}}_{\mathrm{e}} = \frac{1}{\sum_{k=1}^{4}\left\|\tilde{g}_k\right\|^2}\tilde{\mathbf{G}}_{\mathrm{L}}^{H}\mathbf{y}_{\mathrm{e}}, \tag{24}$$

where $\tilde{\mathbf{G}}_{\mathrm{L}}^{H}$ is the channel matrix of the LD-QO-STBC scheme at Eve. In the above equation, the uncancelled AI will incur serious performance degradation.

D. Signal detection of PD-PLS

With the PD-PLS, the signal received at Bob can be presented as follows:

$$\begin{aligned}\mathbf{y}_{\mathrm{b}} &= \tilde{\mathbf{X}}_{\mathrm{P}}\mathbf{h} + \mathbf{n}_{\mathrm{b}} \\ &= \left[e^{-j\angle\tilde{h}_1}h_1\mathbf{x}_1 + e^{-j\angle\tilde{h}_2}h_2\mathbf{x}_2 + \ldots + e^{-j\angle\tilde{h}_4}h_4\mathbf{x}_4\right] + \mathbf{n}_{\mathrm{b}},\end{aligned} \tag{25}$$

where $\tilde{\mathbf{X}}_{\mathrm{P}}$ is a phase distortion matrix with an estimation error.

For signal detection, the received signal in (25) is re-expressed in terms of the channel matrix $\tilde{\mathbf{H}}_{\mathrm{P}}$ as follows:

$$\mathbf{y}_{\mathrm{b}} = \tilde{\mathbf{H}}_{\mathrm{P}}\mathbf{s} + \mathbf{n}_{\mathrm{b}}, \tag{26}$$

where the channel matrix $\tilde{\mathbf{H}}_{\mathrm{P}}$ is represented by:

$$\tilde{\mathbf{H}}_{\mathrm{P}} = \begin{bmatrix} \|h_1\|\theta_1 & \|h_2\|\theta_2 & \|h_3\|\theta_3 & \|h_4\|\theta_4 \\ \|h_2\|\theta_2 & -\|h_1\|\theta_1 & \|h_4\|\theta_4 & -\|h_3\|\theta_3 \\ \|h_3\|\theta_3 & -\|h_4\|\theta_4 & -\|h_1\|\theta_1 & \|h_2\|\theta_2 \\ \|h_4\|\theta_4 & \|h_3\|\theta_3 & -\|h_2\|\theta_2 & -\|h_1\|\theta_1 \end{bmatrix}. \tag{27}$$

In the above, $\theta_k = e^{j\angle(h_k - \tilde{h}_k)}$. If there is no channel estimation error, then $\theta_k = e^{j\angle(0)} = 1$, and this lead to $\tilde{\mathbf{H}}_{\mathrm{P}}$ being a real-valued matrix. Eventually, $\tilde{\mathbf{H}}_{\mathrm{P}}$ becomes a full-orthogonal matrix. On the other hand, under imperfect CSI sitiation, $\tilde{\mathbf{H}}_{\mathrm{P}}$ does not satisfy full-orthogonality condition, and leads to BER performance degradation. Signal detection is performed by simply assuming that $\tilde{\mathbf{H}}_{\mathrm{P}}$ is an orthogonal matrix, as follows:

$$\hat{\mathbf{s}}_{\mathrm{b}} = \frac{1}{\sum_{k=1}^{4}\left\|\tilde{h}_k\right\|^2}\tilde{\mathbf{H}}_{\mathrm{P}}^{H}\mathbf{y}_{\mathrm{b}}, \tag{28}$$

The received signal at Eve can be represented as follows:

$$\begin{aligned}\mathbf{y}_{\mathrm{e}} &= \tilde{\mathbf{X}}_{\mathrm{P}}\mathbf{g} + \mathbf{n}_{\mathrm{e}} \\ &= \left[e^{-j\angle\tilde{h}_1}g_1\mathbf{x}_1 + e^{-j\angle\tilde{h}_2}g_2\mathbf{x}_2 + \ldots + e^{-j\angle\tilde{h}_4}g_4\mathbf{x}_4\right] + \mathbf{n}_{\mathrm{e}},\end{aligned} \tag{29}$$

and the detected signal at Eve is as follows:

$$\hat{\mathbf{s}}_{\mathrm{e}} = \frac{1}{\sum_{k=1}^{4}\left\|\tilde{g}_k\right\|^2}\tilde{\mathbf{G}}_{\mathrm{P}}^{H}\mathbf{y}_{\mathrm{e}}, \tag{30}$$

where $\tilde{\mathbf{G}}_{\mathrm{P}}$ is the channel matrix for PD-PLS scheme at Eve. The signal received by Eve contains serious interference.

IV. Evaluation of BER under imperfect channel estimation

For performance evaluation, we use the 4×1 STBC system model in Fig. 1, unless otherwise is specified. We assume that quadrature phase shift keying (QPSK) modulation is used for STBC encoding and PLS. In addition, the signal energy transmitted at each antenna at a time is normalized to one, and it is transmitted over a frequency flat Rayleigh fading channel.

Figure 2 shows the BER performances of the QO-STBC, LD-QO-STBC, and three PLS schemes introduced in Section II, when there is no channel estimation error. Without PLS, we can see that the LD-QO-STBC has slightly poor BER

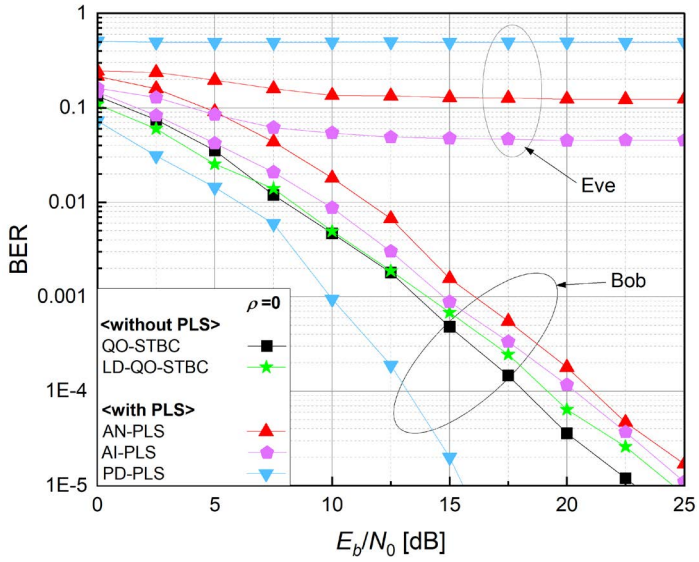

Fig. 2. BER performance comparison for 4×1 systems under perfect CSI

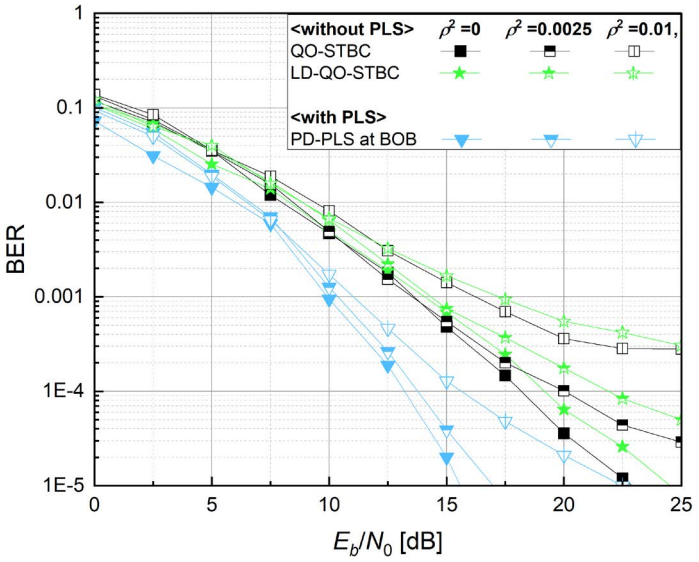

Fig. 3. BER performance comparison of the PD-PLS according to channel estimation error.

performance compared to the QO-STBC. This is because LD-QO-STBC has lower post detection signal to noise ratio (SNR) than QO-STBC. We note that the AN-PLS is the PLS embedded version of the QO-STBC, while AI-PLS is the PLS embedded version of the LD-QO-STBC. If we compare the performances of these, then the performance of the AN-PLS at Bob shows about 3 dB worse performance than that of the QO-STBC, while the performance of the AI-PLS at Bob shows about 0.97dB worse performance than the LD-QO-STBC. This is because addition of CSI-dependent AN or AI requires additional energy [13].

Comparing with BER performances among PLS schemes, the PD-PLS shows the best BER performance at Bob, because it does not require additional energy allocation for PLS. Moreover, the channel matrix at the receiving end becomes a full orthogonal matrix, and thus provides more diversity gain than the others. Regarding to the performance at Eve, the AI-PLS shows the best performance amongst, which indicates the worst security performance. This is because the AI is only added when the transmit signal have a null value, e.g., the probability of having AI is 0.25 in the case of QPSK. On the other hand, the AN-PLS injects AN continuously across the transmit signals, resulting in worse BER performance at Eve than that of the AI-PLS. When using the PD-PLS, signal detection is practically impossible at Eve, showing BER of 0.5 regardless of SNR.

Because the PD-PLS shows the best BER performance amongst, Figure 3 compares its performance under imperfect CSI with those of QO-STBC and LD-QO-STBC. Even though the channel estimation error certainly degrades the BER performance, it is clear that the employing PLS capability does not specially affected by imperfect CSI. As shown in Fig. 3, the LD-QO-STBC shows the worst BER performance as in the case with the perfect CSI, while the PD-PLS does not show specifically dominant amount of performance degradation according to ρ^2 in all given environments. In addition, the PD-PLS shows the best BER performance despite with added security capability. In particular, the full diversity nature of the PD-PLS compensates the performance degradation caused by channel estimation error, and shows even better performance compared to the QO-STBC.

Figure 4 compares the BER performance at Bob and Eve for three PLS methods. In all of these methods, the BER performance at Bob is degraded with increasing channel estimation errors. In addition, it can be seen that the BER performance of the PD-PLS is the best while that of the AN-PLS is the worst, regardless of the value of the ρ^2. For example, in an environment with a ρ^2 of 0.01, the error floor occurs when the BER is about 10^{-3} and 5×10^{-4} in the AN-PLS and AI-PLS, repectively. On the other hand, we can hardly investigate the error floor for the PD-PLD in Fig. 4. It is worthy to note that the effect of the channel estimation error cannot be investigated at Eve. Owing to the excellent security protection, serious error floor always occurs regardless of the channel estimation error. Therefore, the performance degradation caused by the PLS scheme is too serious to evidently present that caused by channel estimation error.

Figure 5 shows the BER performance at Bob and Eve according to the number of transmit antennas, in the PD-PLS. In all estimation error environments, the higher the number of transmit antennas, the better the BER performance. If we increase the number of antennas up to eight, the PD-PLS is hardly affected by the channel estimation error showing that 8×1 system with ρ^2 of 0.01 shows better performance than 2×1 or 4×1 with perfect CSI. On the other hand, the BER

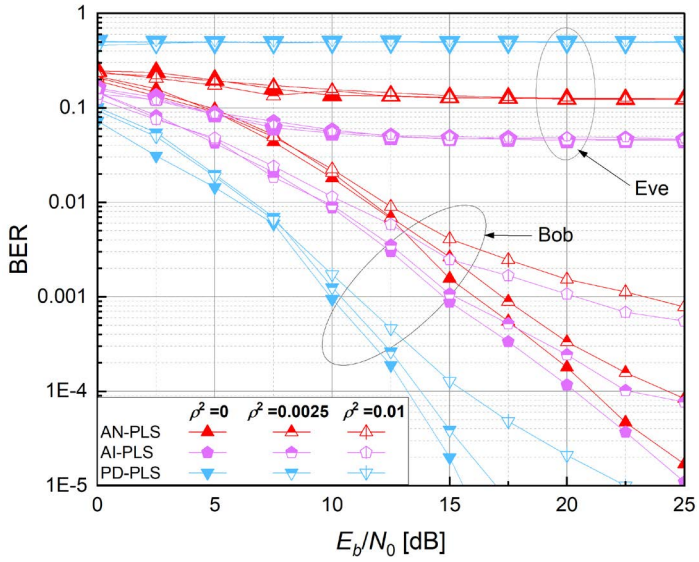

Fig. 4. BER performance of PLS methods for various 4×1 STBC schemes

performance at Eve does not show any changes according to CSI error or the number of antennas, showing constantly unrecoverable performance.

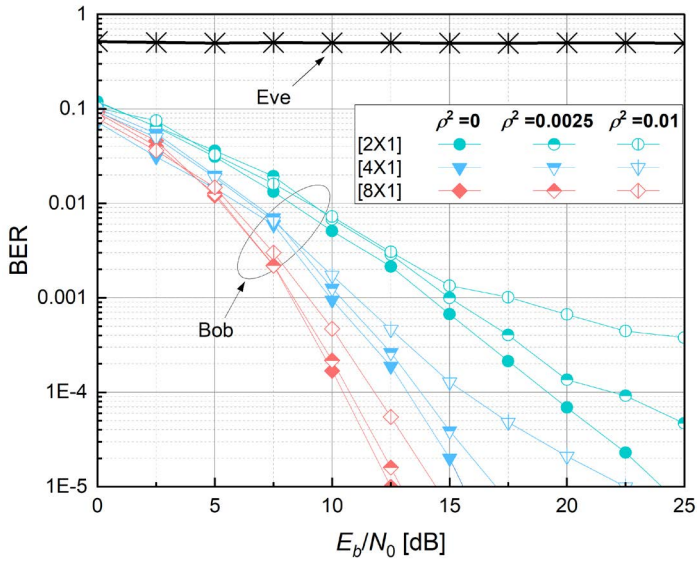

Fig. 5. BER performance of the PD-PLS for various number of transmit antennas

V. Conclusion

This paper evaluated various PLS schemes for STBC schemes under imperfect CSI. Even though the legitimate receiver suffered from the performance degradation as the channel estimation errors are increased, the employment of PLS did not specifically invoked further performance degradation. Owing to the excellent security protection capability, the BER performance at the eavesdropper Eve constantly lied in the ranges of impractical information recovery. The investigation results in the paper showed that the PD-PLS has the best BER performance, whereas the AN-PLS (when the energy of AN is the same as the message signal) has the worst BER performance at Bob. As far as the security performance is concerned, the best security protection could be achieved with the PD-PLS, whereas the worst security protection was investigated with the AI-PLS. The simulation results presented in this paper may be utilized during the system engineering process.

Acknowledgment

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

References

[1] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.

[2] H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Trans. Commun.*, vol. 49, no. 1, pp. 1-4, Jan. 2001.

[3] P. Shang, S. Kim, and X. Jiang, "Efficient alamouti-coded spatial modulation for secrecy enhancing," *Proc. Int. Conf. Inf. Commun. Technol. Convergence*, pp. 860–864, 16-18 Oct. 2019, Jeju, Korea.

[4] P. Shang, H. Lee, and S. Kim, "Waveform design for space–time coded MIMO systems with high secrecy protection," *Electronics*, vol. 9, no. 12, p. 2003, Nov. 2020.

[5] H. Lee, S. Chan, and S. Kim, "Efficient MIMO signal predistortion for secrecy-enhancing," *Electronics*, vol. 11, no. 9, p. 1425, Apr. 2022.

[6] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351-1354, Aug. 2015.

[7] U. Park, S. Kim, K. Lim, and J. Li, "A novel QO–STBC scheme with linear decoding for three and four transmit antennas," *IEEE Commun. Lett.*, vol. 12, no. 12, pp. 868-870, Dec. 2008.

[8] M. Stojanovic, J. G. Proakis and J. A. Catipovic, "Analysis of the impact of channel estimation errors on the performance of a decision-feedback equalizer in fading multipath channels," *IEEE Trans. Commun.*, vol. 43, nos. 2-4, pp. 877-886, Feb. 1995.

[9] B. Nosrat-Makouei, J. G. Andrews and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783-2794, Jun. 2011.

[10] Z. Zhou, B. Vucetic, M. Dohler, and Y. Li, "MIMO systems with adaptive modulation," *IEEE Trans. Veh. Technol.*, vol. 54, no. 5, pp. 1828-1842, Sep. 2005.

[11] F. Benkhelifa, A. Tall, Z. Rezki and M. Alouini, "On the low SNR capacity of MIMO fading channels with imperfect channel state information," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 1921-1930, Jun. 2014.

[12] Z. Rezki, A. Khisti, and M. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652-3664, Oct. 2014.

[13] H. Lee, S. Kim, "Interference energy analysis on artificial interference-aided STBC scheme for physical layer security," *presented at summer KICS.*, Jeju, Korea, Jun. 2022.