A Practical Physical-Layer Security Method for Precoded OSTBC-Based Systems

Jehad M. Hamamreh*, Ertugrul Guvenkaya§, Tuncer Baykas*, Huseyin Arslan*§
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
§Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620

***Abstract*—In this work, we investigate the security performance obtained by employing a practical precoded orthogonal space time block coding method (POSTBC) in MISO wireless networks. In particular, space time codewords are precoded with an optimum matrix that minimizes the error rate at only the legitimate user (Bob). The acquired results depict that there exists a security gap region in the resulting BER performance as a consequence of using POSTBC. Moreover, we enhance the performance more by developing a new hybrid and green security method called precoding along with partial pre-equalizing (PCPPE). In this method, the transmitted symbols are precoded by a new precoder composed of both the original precoder and a new designed unitary matrix that maps Bob's channel amplitudes or phases estimated over the transmitting antennas into 2D orthonormal matrix. Additionally, three issues associated with the proposed security method have been tackled. Including: the slight increase in the transmit power, the appropriate selection process of the optimal precoding matrix, and the effect of imperfect channel estimation and reciprocity. The comparative simulation results prove that PCPPE method provides a secure link among the legitimate parties without sacrificing Bob's reliability although an eavesdropper is assumed to be fully aware of the used method and the original selected precoding matrix indicator (PMI).**

I. INTRODUCTION

Wirelessly conveyed information is enormously proliferating day by day as a consequence of the massive spread of wireless devices. Moreover, the surge in wireless data communication is greatly driven by the huge amount of advantageous applications dedicated for mobile users. Since wireless media is becoming the dominant access for Internet-based services, new security requirements have urgently been demanded. In specific, users require confidential transmission for their generated wireless data, such as their important personal information along with their sensitive financial data contents. This is required to be done without relying only on high layers encryption methods. As a result, well advanced security techniques have to be designed and developed to address the security problem from its roots.

Traditionally, confidentiality has been handled by using cryptographic methods as shown in Shannon's work [1]. However, implementing security methods with Shannon's perfect secrecy is not practical in today's data volume. Additionally, the trends of future wireless systems toward decentralized and asynchronous network infrastructure make the key sharing method alongside the required key management process extremely difficult to be fulfilled. Consequently, physical security arises as a recommended principle to achieve additional protection along with the conventional methods. In Wyner's paper [2], it was explained that confidential communication between legitimate users is possible without even sharing a secret key if the eavesdropper channel is a degraded version of the legitimate receiver channel, so physical security achieved at that time using secrecy codes generated randomly by channel dependent stochastic encoders. Specifically, the secrecy capacity of MIMO based communication systems have been studied for various scenarios from an information theoretic point of view [3]-[6]. Artificial noise along side optimal power allocation in MIMO systems are also investigated for security as shown in [7]-[9]. Additionally, beam-forming MIMO based security procedures have been examined in [10]-[12]. The effect of imperfect channel estimation on the secrecy capacity of MIMO systems has also been analyzed in [13][14]. Beam-forming with optimal power allocation methods for the artificial noise mechanism in MISO scenarios were pictured in [15],[16], and for the SVD-based precoding scheme in [17]. For more details about MIMO based security methods, see [18].

In [19], a received signal strength (RSSI) based technique was suggested to secure orthogonal STBC using a shared key obtained from RSSI. In [20], another shared key based encryption method is proposed for securing STBC, in which the transmitter randomly changes the form of symbols based on precryptocoding matrix to prevent the attacker from getting the correct transmitted symbol. On the contrary to [19][20], authors of [21] proposed a secure STBC without using a shared key. They used a full rate STBC [22] scheme that allows for independent decoding at the legitimate receiver but not at the eavesdropper. They also increased the secrecy by adding aligned artificial noise. In [23], authors used precoding matrix indicator (PMI) in MIMO (spatial multiplexing mode) as a secret key assuming that PMI is only known by the legitimate parties.This is achieved by using channel sounding method and preventing the need for sending any feedback messages about PMI through the air.

However, in practical wireless systems (FDD/TDD), the selected PMI at the receiver side is usually fed back to the base station (eNodeB) via publicly accessed channel to avoid the problem of PMI mismatch selection due to imperfect channel reciprocity. This enables Eve to access the PMI and then make use of it. Additionally, in case there is no explicit feedback, still Eve can know the selected PMI by doing exhaustive search process in the available codebook and find out the used PMI. Motivated by these practical issues, this paper comes to address the problem of Eve's ability in knowing the selected

978-1-4673-9814-5/16/$31.00 ©2016 IEEE

PMI, which results in a small security performance.

To the best of our knowledge, we show for the first time in the literature from a practical perspective that the use of PMI alone in POSTBC MISO system can provide a small security gap region, considering the worst security scenario, where Eve is fully aware of the selected PMI. Then, we solve the problem of having small security gap through providing a practical power efficient security technique based on precoded OSTBC along-with partial pre-equalizing (PCPPE). In our proposed method, physical security is attained without using artificial noise as it causes waste in power resources, nor using secret key sharing as it might be cracked. Therefore, the developed green scheme can be integrated with current wireless systems such as LTE. The rest of the paper is organized as follows: system model is described in Section II. Followed by the security performance investigation of POSTBC in Section III. The details of PCPPE method are presented in Section IV. Then, simulation results are discussed in Section V. Finally, a conclusive summary is drawn in Section VI.

II. SYSTEM MODEL AND PRELIMINARIES

As depicted in Fig. 1, a multiple input single output (MISO) communication system employing precoded OSTBC is adopted. The complex baseband modulated symbols are gathered into groups of two using Alamouti STBC block. Thus, two consecutive discrete symbols x_1 and x_2 are encoded with the space-time codeword matrix

$$\mathbf{X} = \begin{bmatrix} x_1(n) & -x_2^*(n) \\ x_2(n) & x_1^*(n) \end{bmatrix}.$$

Hence, $\mathbf{X} \in C^{M \times T}$ is considered as the space time codeword of length M symbols with T period, where $*$ is the complex conjugate operator. In MISO system with N_T transmit antennas, POSTBC is usually applied to exploit the full diversity of the channel by achieving orthogonal transmission among the parallel channels such that interference between the transmitted signals is reduced. This is implemented through multiplying the space time code $\mathbf{X}$ by a precoding matrix $\mathbf{W}$ chosen from a universal codebook composed of a set of precoding matrices, that are stored at both the transmitter and receiver sides.

In particular, a trusted sender, Alice, conveys data packets to a legitimate receiver, Bob. Each packet consists of multiple consecutive precoded space time codewords ($\mathbf{WX}$). The baseband received signal at Bob's side in the first and second time slot is given in (1) in matrix form and in (3) in expanded form, where $\mathbf{H^b} \in C^{1 \times N_T}$ is the complex gain vector of N_T transmit antennas. Each antenna (independent of the others) experiences a one-tap Rayleigh fading channel with constant channel gain over one packet length, but i.i.d. from one packet to another. $\mathbf{z^b}$ is the zero-mean complex additive white Gaussian noise (AWGN). An eavesdropper, Eve, tries to receive the signal transmitted by Alice. Similarly, the signal captured by Eve is given in (2) and (4) where $\mathbf{H^e}$ and $\mathbf{z^e}$ are the complex channel response, and AWGN of eavesdropper channel, respectively.

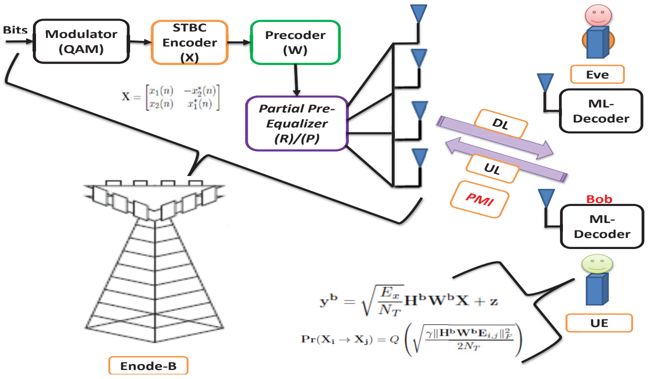
Bits
Modulator (QAM)
STBC Encoder (X)
Precoder (W)
$\mathrm{X} = \begin{bmatrix} x_1(n) & -x_2^*(n) \\ x_2(n) & x_1^*(n) \end{bmatrix}$
Partial Pre-Equalizer (R)/(P)
DL
UL
PMI
Eve
ML-Decoder
Bob
ML-Decoder
UE
Enode-B
$\mathbf{y^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^bW^bX} + \mathbf{z}$
$\mathbf{Pr(X_i \to X_j)} = Q\left(\sqrt{\frac{\gamma\|\mathbf{H^bW^bE}_{i,j}\|_F^2}{2N_T}}\right)$

Fig. 1. Precoded OSTBC model considered in this work.

$$\mathbf{y^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^bW^bX} + \mathbf{z^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^{bw}X} + \mathbf{z^b} \tag{1}$$

$$\mathbf{y^e} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^eW^bX} + \mathbf{z^e} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^{ew}X} + \mathbf{z^e} \tag{2}$$

In (1) and (2), E_x is the symbol energy, $\mathbf{N}_T$ is the number of transmit antennas, $\mathbf{H^b}$ is the channel realization of $\mathbf{N}_T$ transmit antennas, $\mathbf{W^b}$ is the optimal selected precoding matrix based on the legitimate user's channel. The process of selecting $\mathbf{W^b}$ will be discussed in the next section. $\mathbf{H^{bw}} \in C^{[1\times 2]}$ is the effective channel vector resulted from multiplying $\mathbf{H^b} \in C^{[1\times 4]}$ by $\mathbf{W^b} \in C^{[4\times 2]}$. Specifically, The entries of these matrices can be denoted as shown below:

$$\mathbf{H^{bw/ew}} = \mathbf{H^{b/e}}^{[1\times 4]} \times \mathbf{W^{b/e}}^{[4\times 2]} = \begin{bmatrix} h_1^{b/e}(n) & h_2^{b/e}(n) \end{bmatrix}.$$

Let $y_1^b(n)$ and $y_2^b(n)$ denote the received symbols at time t and $t + T_s$ respectively. Then (1) and (2) can be shown as

$$\begin{aligned} y_1^b(n) &= h_1^b(n) * x_1(n) + h_2^b(n) * x_2(n) + z_1^b(n) \\ y_2^b(n) &= -h_1^b(n) * x_2^*(n) + h_2^b(n) * x_1^*(n) + z_2^b(n) \quad (3) \\ y_1^e(n) &= h_1^e(n) * x_1(n) + h_2^e(n) * x_2(n) + z_1^e(n) \\ y_2^e(n) &= -h_1^e(n) * x_2^*(n) + h_2^e(n) * x_1^*(n) + z_2^e(n). \quad (4) \end{aligned}$$

If we take the conjugation of the received signal at the second time slot and then multiply by the hermitian transpose of Bob's and Eve's equivalent channel vector ($\mathbf{H^{bw/ew}}$), we get the following input output relationship at the receiver side:

$$\begin{bmatrix} \hat{y}_1^{b/e}(n) \\ \hat{y}_2^{b/e}(n) \end{bmatrix} = (|h_1^{b/e}(n)|^2 + |h_2^{b/e}(n)|^2) \begin{bmatrix} x_1(n) \\ x_2(n) \end{bmatrix} + \begin{bmatrix} \hat{z}_1^{b/e}(n) \\ \hat{z}_2^{b/e}(n) \end{bmatrix},$$

where any variable with hat $\hat{}$ represents the original variable multiplied by the matrix

$$\hat{H} = \begin{bmatrix} h_1^{*b/e}(n) & h_2^{b/e}(n) \\ h_2^{*b/e}(n) & -h_1^{b/e}(n) \end{bmatrix}.$$

Accordingly, the maximum likelihood (ML) signal detection process at the receiver side is simplified as follows:

$$\hat{\mathbf{X}}_{i,ML}^{\mathbf{b/e}} = \Phi\left(\frac{\hat{\mathbf{y}}_\mathbf{i}^{\mathbf{b/e}}\mathbf{(n)}}{(|h_1^{b/e}(n)|^2 + |h_2^{b/e}(n)|^2)}\right), i = 1, 2, 3, \ldots \tag{5}$$

where $\Phi(.)$ represents a slicing function that performs a separable decoding process at the receiver. Moreover, since Eve is a passive node, we assume that Alice has no information about the CSI of Eve's channel $\mathbf{H^e}$. Additionally, channel reciprocity property is adapted in our proposed method, where downlink channel can be estimated from the uplink one. As a final notice, we assume that both Bob and Eve experience independent channel realizations because the wireless channel response is unique to the locations of the transmitter and receiver as well as the environment. Therefore, $\mathbf{H^b}$ and $\mathbf{H^e}$ are uncorrelated. This assumption coincides with the practical situation where Eve's location can't be exactly at Bob's position.

III. PRECODED OSTBC METHOD

As mentioned previously, many MIMO based physical security methods have been proposed in the literature. In spite of the effectiveness of such approaches, most of them suffer from sacrificing some of the precious communication resources such as transmission power. Generally, the source of security was based on using artificial noise, optimum power allocation, beam-forming, secret key generation, and antenna subset modulation. However, here in the first part of our study, we show that choosing an optimal precoding matrix from a codebook in such a way that pairwise error probability at Bob is minimized to the lowest possible level, can provide a secrecy gap region between Bob and Eve over all expected SNR values. It is very important to emphasize that the obtained security gain is achieved considering the worst security scenario, where Eve is capable of knowing the selected PMI. Although both Alice and Bob can use the estimated channel in implementing a similar selection process to choose the best PMI without feeding back any bits about the selected PMI, in current practical wireless systems such as LTE, PMI value is usually sent via publicly accessed channel to avoid the imperfect channel reciprocity problem. Consequently, Eve can detect the selected PMI, and then use it in the detection process. In the following, the process of selecting optimal precoding matrix is discussed. Considering the precoded OSTBC described previously in the system model section, the space-time codeword $\mathbf{X}$ is multiplied by a precoding matrix $\mathbf{W}$ which is chosen from the codebook $\mathbf{G} = \{\mathbf{W}_1, \mathbf{W}_2, \mathbf{W}_3, ..., \mathbf{W}_T\}$. The objective here is to select an appropriate codeword that improves the overall system performance such as error performance is minimized. Since N_T channels remain static over several consecutive codewords, the received signal $\mathbf{y^b} \in C^{[1\times T]}$ over T becomes

$$\mathbf{y^b} = \sqrt{\frac{E_x}{N_T}}\mathbf{H^b}\mathbf{W^b}\mathbf{X} + \mathbf{z}. \tag{6}$$

For a given channel $\mathbf{H^b}$ and precoding matrix $\mathbf{W^b}$, we consider the pairwise codeword error probability $\mathbf{Pr}(\mathbf{X_i} \rightarrow \mathbf{X_j})$. This is the probability that the space-time codeword $\mathbf{X_i}$ is transmitted whereas $\mathbf{X_j}$ with $j \neq i$ is decoded. The formula of the pairwise error probability is given as [24]

$$\mathbf{Pr}(\mathbf{X_i} \rightarrow \mathbf{X_j}) = Q\left(\sqrt{\frac{\gamma\|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2}{2N_T}}\right), \tag{7}$$

where γ is the signal-to-noise ratio (SNR), given as $\gamma = \frac{Ex}{N0}$, $\mathbf{E}_{i,j}$ is the error matrix between the codewords $\mathbf{X_i}$ and $\mathbf{X_j}$ which is defined as $\mathbf{E}_{i,j} = \mathbf{X_i} - \mathbf{X_j}$ for a given STBC scheme, $\|.\|_F^2$ is the squared Frobenius norm, which physically computes the total power gain. From (5), we see that $\|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2$ needs to be maximized in order to minimize the pairwise error probability. This leads us to the following codeword selection criterion

$$\begin{aligned}\mathbf{W}_{opt} &= arg\ max\ \|\mathbf{H^b}\mathbf{W^b}\mathbf{E}_{i,j}\|_F^2,\ \mathbf{W^b} \in \mathbf{G},\ i \neq j \\ &= arg\ max\ \|\mathbf{H^b}\mathbf{W^b}\|_F^2,\ \mathbf{W^b} \in \mathbf{G}.\end{aligned} \tag{8}$$

Solving the corresponding optimization problem for arbitrary N_T, codeword length M, and codebook size L, (8) can be formulated into the Grassmannian subspace packing problem as shown in [25]. However, since this solution is somehow time-consuming and not straightforward, we use another suboptimal yet practical design method called Discrete Fourier Transform (DFT) matrices as explained in [26]. The DFT matrices given as

$$\mathbf{G} = \left[\mathbf{W}_{DFT} \quad \theta\mathbf{W}_{DFT} \quad . \quad . \quad . \quad \theta^{L-1}\mathbf{W}_{DFT}\right].$$

The first precoding matrix $\mathbf{W}_{DFT}$ is taken by selecting M columns of $N_T \times N_T$ DFT matrix, of which the (k,l)th entry is given as $e^{j2\pi(k-1)(l-1)/N_T}/\sqrt{N_T}, k, l = 1, 2, ..., N_T$. Moreover, θ is the diagonal matrix given as

$$\theta = diag\left(\left[e^{j2\pi u_1/N_T} \quad e^{j2\pi u_2/N_T} \quad . \quad . \quad . \quad e^{j2\pi u_{N_T}/N_T}\right]\right)$$

with free variables $\{u_i\}_{i=1}^{N_T}$ to be determined. Given the first precoding matrix $\mathbf{W}_{DFT}$, the remaining (L-1) precoders are obtained by multiplying $\mathbf{W}_{DFT}$ by $\theta_i, i = 1, 2, ...L - 1$. Free variables $\{u_i\}_{i=1}^{N_T}$ are determined such that the minimum chordal distance is maximized as

$$\mathbf{u} = argmax_{\{u_1,.u_{N_T}\}} min_{\{l=1,.N-1\}} d(\mathbf{W}_{DFT}, \theta^l\mathbf{W}_{DFT}). \tag{9}$$

Note that IEEE 802.16e specification for the Mobile WiMAX system employs this particular design method [26]. As shown in the previous design equations, the selection process of the suboptimal precoding matrix is based on the channel response of the intended receiver (Bob), but not Eve's channel, which is independent of Bob's one. As a result, one can intuitively expect obtaining a secrecy gap region between Bob and Eve. This intuition is verified by simulation results that show the exact performance difference between Bob and Eve as it will be demonstrated in Section V, Fig. 2. It is worth mentioning that the main reason behind the enhancement in the BER performance of Bob compared to Eve is the increase in the effective received SNR. More precisely, SNR increased as a result of achieving orthogonal transmission among the parallel channels toward Bob through precoding. Accordingly, the average received SNR over each symbol becomes

$$\mathbf{SNR} = \frac{\gamma \|\mathbf{HW}\|_F^2}{M}. \tag{10}$$

IV. PROPOSED PCPPE METHOD

In the previous method (POSTBC), it is noticed from Eve's BER performance (Fig. 2) that although there is a security gap between Bob and Eve at comparable SNRs, still there is a nontrivial amount of information leakage at Eve. In other words, Eve's good performance enables her to detect some information bits correctly. Consequently, the provided secrecy by POSTBC method alone is obviously limited, not reliable and might be insufficient in some cases, where higher security gap is extremely needed to ensure better confidentiality at any distance Eve may be located from the base station (BS). More accurately, if Eve is closer to the BS than Bob, then secure link is hard to be achieved. For instance, when the SNR value at Eve is 20 dB, while it is 10 dB at Bob, then Eve can decode the data better than Bob. This fact motivates finding a way to enhance the previous method so that better security performance (i.e. larger BER gap between Bob and Eve) can be achieved. Therefore, a hybrid technique that combines the use of precoded OSTBC along with partial pre-equalizing (PCPPE) is introduced.

In this method, a new modified precoder, that takes security requirements into account, is proposed. Particularly, besides exploiting the conventional precoding process (explained in Sec.III), the transmitter designs a new precoder that exploits the knowledge of its estimated channel amplitudes or phases experienced by each antenna with respect to the trusted receiver. These estimates are gathered in the form of amplitude based vector as shown in (11) or phase based vector as shown in (12). Now, to enhance the security performance, one can think of converting the vector $\tilde{\mathbf{R}}$ to a diagonal matrix $\mathbf{R}$ and then multiply it with the original precoding matrix $\mathbf{W}$ to get an encrypted and equalized precoding matrix denoted as $(\mathbf{RW})$. In this case the transmitted symbols are precoded by $(\mathbf{RW})$ in stead of only $\mathbf{W}$. Since $\mathbf{R}$ is related to Bob's channel amplitudes, which are independent from those associated with Eve, a security performance gain is expected to occur.

However, although this direct method can acquire a good performance gain, it creates some serious problems regarding high power fluctuation and transmit power increase. To overcome these issues, while being still able to obtain a good security performance, we perform the following mathematical processing on one of the two created vectors $\tilde{\mathbf{R}}$ or $\tilde{\mathbf{P}}$ as both of them are related to Bob's condition but not Eve. For simplicity, let's just focus on $\tilde{\mathbf{R}}$ keeping in mind that the same processing can be applied on $\tilde{\mathbf{P}}$ as well. Hence, $\tilde{\mathbf{R}}$ is used as an input vector to a Singular Value Decomposition (SVD) process to get an orthogonal matrix called $\mathbf{F}$ as shown in (13). This process is used to overcome the aforementioned problems, more precisely, the power spectrum of $\tilde{\mathbf{R}}$ is collected in $\mathbf{E}$ (one singular value), while $\mathbf{U}$ is always a unity number. Therefore, both $\mathbf{E}$ and $\mathbf{U}$ can be dropped and only matrix $\mathbf{F}$ is taken.

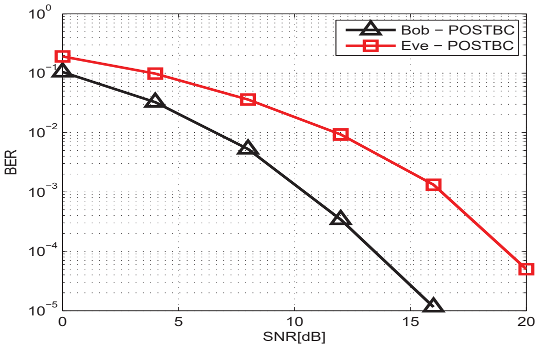

Fig. 2. BER of POSTBC scheme for two streams (M=2) and $[4 \times 1]$ antenna system with 4QAM in a block Rayleigh fading channel. The selected PMI is assumed to be known by Eve (the worst security scenario).

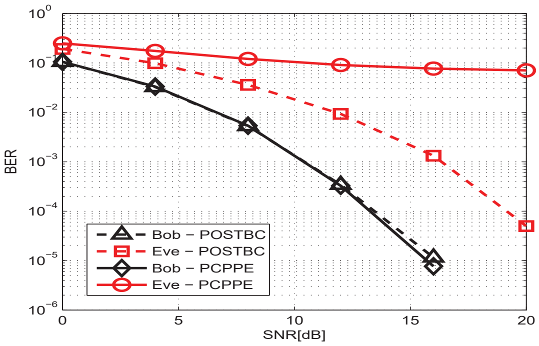

Fig. 3. BER performance comparison between POSTBC and PCPPE methods with 4QAM modulation. Both the selected PMI and the employed security method are assumed to be known by Eve (the worst security scenario).

This matrix has several interesting properties: First, it is an orthogonal matrix with size of $(N_T \times N_T)$ and norm of unity. Second, its inverse is itself and its transpose is itself. Third, it maps the amplitude channel randomness to two dimensions instead of only one. As a result, $\mathbf{F}$ is used along with $\mathbf{W_{opt}}$ to constitute a new precoding matrix called $\mathbf{V}$ as shown in (14).

$$\tilde{\mathbf{R}} = \begin{bmatrix} \frac{1}{|h^b 1|} & \frac{1}{|h^b 2|} & \frac{1}{|h^b 3|} & \cdots & \frac{1}{|h^b N_T|} \end{bmatrix} \tag{11}$$

$$\mathbf{R} = diag \left\{ \begin{bmatrix} \frac{1}{|h^b 1|} & \frac{1}{|h^b 2|} & \frac{1}{|h^b 3|} & \cdots & \frac{1}{|h^b N_T|} \end{bmatrix} \right\}$$

$$\tilde{\mathbf{P}} = \begin{bmatrix} \frac{1}{\phi(h^{b1})} & \frac{1}{\phi(h^{b2})} & \frac{1}{\phi(h^{b3})} & \cdots & \frac{1}{\phi(h^{bN_T})} \end{bmatrix} \tag{12}$$

$$\mathbf{SVD} \left\{ \tilde{\mathbf{R}} \right\} = \mathbf{UEF'} \tag{13}$$

$$\mathbf{V} = \mathbf{FW_{opt}} \tag{14}$$

$$\mathbf{W_{opt}} = arg\ max\ Tr\left(\|\mathbf{HFW}\|_F^2 \right), \ \ \mathbf{W} \in \mathbf{G} \tag{15}$$

$$\mathbf{y^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}} \mathbf{H^b F^b W^b_{opt} X} + \mathbf{z^b} \tag{16}$$

$$\mathbf{y^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}} \mathbf{H^b V^b_u X} + \mathbf{z^b} = \sqrt{\frac{\mathbf{E}_x}{N_T}} \mathbf{H^{bvw}_u X} + \mathbf{z^b} \tag{17}$$

$$\mathbf{y^e} = \sqrt{\frac{\mathbf{E}_x}{N_T}} \mathbf{H^e V^b_u X} + \mathbf{z^e} = \sqrt{\frac{\mathbf{E}_x}{N_T}} \mathbf{H^{evw}_u X} + \mathbf{z^e} \tag{18}$$

Yet, another necessary modification is still needed to be performed. This new amendment is related to the traditional selection process of $\mathbf{W_{opt}}$. Previously, $\mathbf{W_{opt}}$ is chosen merely based on Bob's channel to minimize the pair-wise error probability. However, because of the modification that has been performed on the precoding process, the new selection should take into account the effect of $\mathbf{F^b}$ on the pair-wise probability as it becomes a kernel part of the precoding process, where it is specifically designed to meet security requirements. Otherwise, a performance degradation is going to happen. The new selection process is represented mathematically by (15), where $\mathbf{W_{opt}}$ is chosen based on both $\mathbf{H^b}$ and $\mathbf{F^b}$. After doing this modification along with avoiding the aforementioned problems, the secure communication is now ready to be started. Note that both the transmitter and receiver should be able to estimate and construct the effective channel vector $\mathbf{H_u^{bvw}}$ and use it properly to detect and decode the transmitted symbols. Fig. 4 summarizes the signaling procedure of the PCPPE scheme based on a practical MISO system with codebook-based precoding. As shown, the receiver (Bob) first sends out a reference signal to the transmitter (Alice) to estimate the channel matrix $\mathbf{H^b}$. The transmitter uses $\mathbf{H^b}$ to calculate $\mathbf{F^b}$ using SVD process, then use it along with $\mathbf{H^b}$ in finding the PMI from the universal codebook $\mathbf{G}$ that maximizes the norm found in (15). Then, Alice sends out the selected PMI via a publicly accessed channel (i.e. Eve can detect the PMI), followed by sending another reference signal to Bob. Under the assumption of channel reciprocity, Alice and Bob are able to compute the same effective channel vector $\mathbf{H_u^{bvw}}$, but Eve is unable to obtain the same one since her channel is different than Bob's one. After this signaling process, secure communication starts.

V. Simulation Results

Since our proposed security scheme is based on signal processing, the effectiveness of the developed technique is characterized by BER performance verses average SNR [18]. First, the codebook using the design method in [26], which is adopted in WiMAX wireless systems, is generated with the following parameters $N_T = 4$, $M = 2$, and $L = 64$. Then the BER performance of the precoded OSTBC with $N_T = 4$, $N_R = 1$ is simulated. For more details about POSTBC simulation, see [24]. Fig. 3 depicts a comparative BER performance between Bob and Eve in a block flat Rayleigh fading channel using QAM modulation considering two cases: the first case is with only POSTBC, which is also shown alone in Fig. 2, whereas the second is with PCPPE in which the original precoder is modified by the estimated channel amplitudes. It is obvious that there is a small security gap region in the first case (POSTBC). This gap is improved more by employing the modified precoder using PCPPE method. It is evident that the performance of Bob gets better, while it gets worse for Eve since her extracted new precoding matrix is different from Bob, whose channel is uncorrelated with Eve due to being in different location. By doing this, secure link has been assured at any distance Bob or Eve might be located from the BS. Fig. 5 shows that phase based PCPPE outperforms amplitude based PCPPE method, which is due to having different distributions for amplitude and phase. Amplitude has Rayleigh distribution, while phase has uniform distribution, in which the probability of occurrence of each event is the same (independent events), resulting in more randomness compared to amplitude based method. Fig. 6 exhibits the BER performance of PCPPE method under imperfect channel estimation (ICE) and imperfect channel

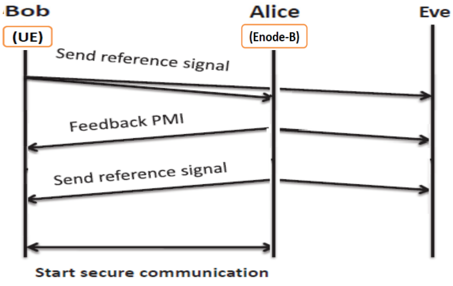

Fig. 4. Signaling procedure of the proposed PCPPE method.

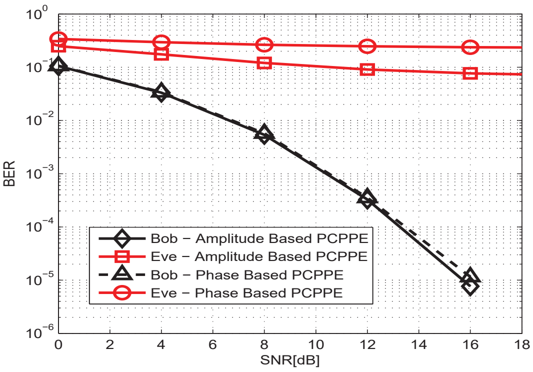

Fig. 5. BER performance comparison between amplitude based PCPPE method and phase based PCPPE with 4QAM.

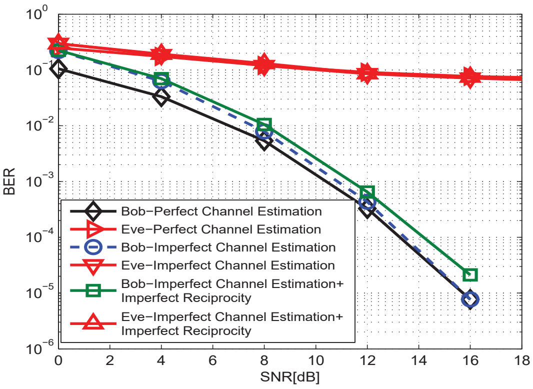

Fig. 6. BER performance of PCPPE method with 4QAM under imperfect channel estimation and imperfect channel reciprocity.

reciprocity (ICR). ICE is modeled by introducing intentional errors according to the mean square error (MSE) values of a least square estimator (LSE). More accurately, the following equation is used $MSE = \varDelta H = 10^{\frac{-SNR}{10}}$ at both the receiver and the transmitter. On the other hand, ICR is modeled by adding a constant value α, which is added to the estimated MSE value over all SNRs i.e. $MSE = \varDelta H = 10^{\frac{-SNR}{10}} + \alpha$. In our simulation, α is considered to be 0.1. As depicted in Fig. 6, ICE and ICR lead to a small degradation due to the mismatch of the generated modified precoders at both sides. It is observed that ICE creates a decaying degradation in the BER performance since MSE value at high SNR becomes very low, while ICR produces a constant degradation over all SNR since α is independent of SNR. However, this small degradation can be overcome by increasing the training sequence length, where better channel estimation can be obtained. In all of our simulation experiments, the worst security scenario is taken into account, where Eve is considered to be fully knowledgeable of the implemented security method as well as the selected PMI. This assumption is closer to the practical systems, in which PMI is fed back to the transmitter. Based on the obtained results and from both security and reliability perspectives, it is demonstrated that the security performance of PCPPE outperforms POSTBC scheme. This enhancement is achieved without sacrificing any of the precious resources such as spectral bandwidth or transmit power. Therefore, it is highly recommended to use PCPPE method for providing secure OSTBC-MISO systems in green wireless networks.

VI. CONCLUSION

The security performance obtained by employing POSTBC in wireless networks has been investigated. The worst practical security scenario, where Eve has knowledge on the selected PMI is considered. The obtained results have depicted that there is a security gap region in the resulting BER performance as a consequence of using POSTBC. Moreover, the security performance is enhanced more by developing a new robust and hybrid security method called PCPPE, where the original precoder is re-designed to take security requirements into account. This method is performed without sacrificing any communication resources, thus it is considered to be a green and power efficient security technique that can be integrated with current and future wireless systems such as 4G and 5G.

ACKNOWLEDGMENT

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

REFERENCES

[1] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, pp. 1355–1387, 1975.

[3] A. Hero, Secure space-time communication, IEEE Trans. Inf. Theory,vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[4] S. Shafiee and S. Ulukus, Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel, IEEE Trans. Inf. Theory, vol. 55, pp. 4033–4039, Sept. 2009.

[5] J. Li, On ergodic secrecy rate for Gaussian MISO wiretap channels, IEEE Trans. Wireless Commun., vol. 10, no.4, pp. 1176–1187, Apr. 2011.

[6] A. Khisti and G. W. Wornell, Secure transmission with multiple antennas I,II:The MISOME wiretap channel, IEEE Trans. Inf. Theory, vol. 56, no.11, pp. 3088–3104, July 2010.

[7] S. Goel and R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun., vol. 7, no.6, pp. 21802189, June 2008.

[8] Jun Zhu; Schober, R.; Bhargava, V.K., "Secure transmission in multi-cell massive MIMO systems," Globecom Workshops (GC Wkshps), 2013 IEEE, pp.1286–1291, 9-13 Dec. 2013.

[9] Goel, S.; Negi, R., "Secret communication in presence of colluding eavesdroppers," Military Communications Conference, 2005. MILCOM 2005. IEEE, pp.1501,1506 Vol. 3, 17-20 Oct. 2005.

[10] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach, IEEE Trans. Signal Proc., vol. 59, no.3, pp. 1202-1216, Mar. 2011.

[11] A. Mukherjee and A. L. Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI, IEEE Trans. Signal Processing, vol. 59, no. 1, pp. 351361, 2011.

[12] Chenxi Liu; Geraci, G.; Nan Yang; Jinhong Yuan; Malaney, R., "Beamforming for MIMO Gaussian wiretap channels with imperfect channel state information," Global Communications Conference (GLOBECOM), 2013 IEEE, pp.3253,3258, 9-13 Dec. 2013.

[13] Xiaoming Chen; Chau Yuen; Zhaoyang Zhang, "Exploiting large-scale MIMO techniques for physical layer security with imperfect channel state information," Global Communications Conference (GLOBECOM), 2014 IEEE, pp.1648-1635, 8-12 Dec. 2014.

[14] Rezki, Z.; Alomair, B.; Alouini, M.-S. "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation", Global Communications Conference (GLOBECOM), 2014 IEEE, On page(s):1602-1607.

[15] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, PHY layer security based on protected zone and artificial noise, IEEE Signal Process. Lett., vol. 20, no. 5, pp. 487-490, May 2013.

[16] S. Gerbracht, C. Scheunert, and E. Jorswieck, Secrecy outage in MISO systems with partial channel information, IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 704-716, Apr. 2012.

[17] S. A. Fakoorian and A. L. Swindlehurst, Optimal power allocation for GSVD-based beamforming in the MIMO wiretap channel, in Proc. IEEE ISIT, pp. 2321-2325, Boston, MA, 2012.

[18] Mukherjee, A.; Fakoorian, S.A.A.; Jing Huang; Swindlehurst, A.L., "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," Communications Surveys and Tutorials, IEEE , vol.16, no.3, pp.1550,1573, Third Quarter 2014.

[19] Allen, T.; Cheng, J.; Al-Dhahir, N., "Secure Space-Time Block Coding without Transmitter CSI," Wireless Communications Letters, IEEE , vol.3, no.6, pp.573,576, Dec. 2014.

[20] Mahdi Nouri; Abolfazl Falahati, "Securing MIMO Space-Time Block Coding Technique over Wireless Communication Links", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2012.

[21] Fakoorian, S.A.A.; Jafarkhani, Hamid; Swindlehurst, A.L., "Secure space-time block coding via artificial noise alignment,"2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), pp.651,655, 6-9 Nov. 2011.

[22] H. Jafarkhani, Space-Time Coding: Theory and Practice. Cambridge University Press, 2005.

[23] Chih-Yao Wu; Pang-Chang Lan; Ping-Cheng Yeh; Chia-Han Lee; Chen-Mou Cheng, "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices," Selected Areas in Communications, IEEE Journal on , vol.31, no.9, pp.1687,1700, September 2013.

[24] Yong Soo Cho, Jaekwon Kim, Won Young Yang, Chung G.Kang; MIMO-OFDM WIRELESS COMMUNICATIONS WITH MATLAB; November 16, 2010.

[25] Love, D.J. and Heath, R.W. Jr (2005) Limited feedback unitary precoding for orthogonal space-time block codes. IEEE Trans. Signal. Proc., 53(1), 64-73.

[26] Hochwald, B.M., Marzetta, T.L., Richardson, T.J. et al. (2000) Systematic design of unitary space-time constellations. IEEE Trans. Info. Theory, 46 (6), 1962-1973.