Code Approaches with Sparse Perfect Gaussian Integer Sequences for Physical Layer Security in Wireless Networks

Abstract:

Physical-layer (PHY) security in wireless communication deals mainly with unauthorized users, eavesdroppers, and/or jammers. It is crucial for wireless network due to its broadcast nature and the channel is easily susceptible to eavesdropping by unauthorized receivers. Recently, secrecy techniques on the initial physical layer of wireless network have drawn a renewed interest. In a Multiple Input Multiple Output (MIMO) antenna system, the increase of channel correlation may decrease the transmission security level. The eavesdropper may obtain information by estimating and reconstructing the wireless environment. Besides, to decrease the signal bit error rate (BER) between legitimate users, it is required to increase the system complexity and feedback overhead. Nearby eavesdroppers may observe the same channel as the legitimate users. In this paper, we propose an enhanced (E-MOP) security scheme for MIMO orthogonal frequency division multiplexing (MIMO-OFDM) systems by using Precoding Matrix Index (PMI) and Sparse Perfect Gaussian Integer Sequences (SPGIS) to generate private keys. This scheme relieves the MIMO channel correlation issue. Due to the designed time slot exchanging algorithm, the eavesdroppers are unlikely to reconstruct the wireless environment. The encryption complexity decreases while the BER remains low. The proposed E-MOP scheme enhances the PHY transmission security while the channel capacity is not sacrificed.

Keywords: Wireless network, physical-layer security, MIMO-OFDM, Sparse Perfect Gaussian Integer Sequences (SPGIS), code approach, eavesdropping.

I. Introduction

Traditional security in communication networks relies mainly on the upper layers of the OSI model with cryptography and authentication measures. Due to the radio frequency (RF) broadcast nature, wireless communications are easily susceptible to unauthorized receivers having eavesdropping capability. As the wireless applications are more widely used, wireless communication becomes vulnerable in the initial physical layer (PHY) of the OSI model. Research on the PHY security has drawn a great interest in recent years. The PHY security deals mainly with exploiting the inherent randomness of noise and network channels to limit information intercepted by unauthorized users.

Recent advances in wireless technology such as multi-input multi-output (MIMO) and orthogonal frequency division multiplexing (OFDM) have greatly increased the range and capacity of wireless communication. MIMO is a method for multiplying the capacity of a wireless link using multiple transmit and receive antennas to exploit multipath propagation. MIMO has become an essential element of wireless communication standards including IEEE 802.11n (Wi-Fi), IEEE 802.11ac (Wi-Fi), HSPA+ (3G), WiMAX (4G), and Long Term Evolution (4G). MIMO-OFDM is the dominant air interface for 4G and 5G broadband wireless networks because it achieves the greatest spectral efficiency and delivers the highest capacity and data throughput. An information-theoretic framework for investigating information security in wireless MIMO is proposed by Hero [1]. One of the principal conclusions is that with proper exploitation of space-time diversity at the transmitter can enhance information security and information-hiding capabilities.

To prevent the unauthorized intrusions at the initial PHY level, much research have been conducted to prevent intruders from gaining access to the wireless network.

The reported approaches to achieve PHY security can be classified into the following four categories, namely, the channel, power, signal detection, and code approaches. Firstly, the channel approaches exploit the channel characteristics to increase PHY layer security by using methods such as radio frequency (RF) fingerprinting [2], algebraic channel decomposition multiplexing (ACDM) precoding [3], and randomization of MIMO transmission coefficients [4]. The power approaches usually involve the employment of directional antennas [5] and the injection of artificial noise [6]. The signal design approach includes the training-based channel estimation scheme that enables the quality-of-service discrimination between legitimate and non-legitimate receivers in wireless networks [7]. The code approaches for PHY security consist of using error correction coding [8], spread spectrum coding [9] [10], and PHY-layer network coding scheme [11].

One remarkable way of creating effective encryption keys on the physical layer comes from the reciprocity property of the wireless channels. Received wireless RF signals due to random scattering and reflection display an effect known as the multipath interference. Channel reciprocity means that, under an impulse response, the channel remains the same if the sender and receiver are reversed. They can obtain joint randomness through the impulse response between their wireless channels. Any other eavesdropping receivers, provided they are separated sufficiently away from the legitimate receivers, will not be able to receive the precoded signals.

In this paper, we propose an enhanced E-MOP scheme by using Precoding Matrix Index (PMI) and Sparse Perfect Gaussian Integer Sequences (SPGIS) for MIMO-OFDM wireless systems. It works by preventing any eavesdropper from learning the channel state information (CSI) of the wiretap channel and decoding the information being exchanged. The encryption complexity has been reduced while the bit error rate

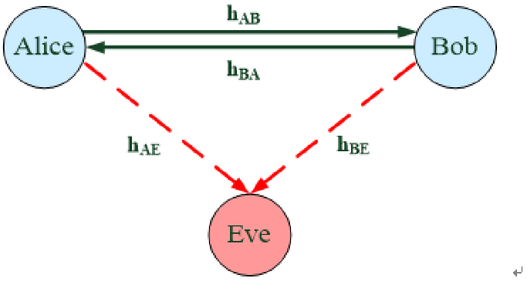

Fig 1. Position structure model

(BER) remains low. The proposed E-MOP scheme enhances the PHY transmission security while the channel capacity is not sacrificed.

II. The MOP system

A. System Model

Let’s consider three users in the environment of Wireless communication, Alice, Bob and Eve, Alice and Bob are the legitimate users and Eve is the unauthorized eavesdropper, and three communication channel $\mathbf{h}_{AB}$, $\mathbf{h}_{BA}$, $\mathbf{h}_{AE}$, and $\mathbf{h}_{BE}$. In Fig 1, the solid arrow $\mathbf{h}_{AB}$ represents the channel from Alice to Bob; conversely, $\mathbf{h}_{BA}$. The dotted arrows $\mathbf{h}_{AE}$ and $\mathbf{h}_{BE}$ represent the channel through which the message sent from Alice will be overheard by Eve. Similarly, $\mathbf{h}_{BE}$ represents the channel through which the message sent from Bob will be overheard by Eve. We adopt the Time-Division Duplexing (TDD) model. Different from Frequency-Division Duplexing (FDD), TDD uses a single frequency band for both transmit and receive. It shares that band by assigning alternating time slots to transmit and receive operations which has a bigger

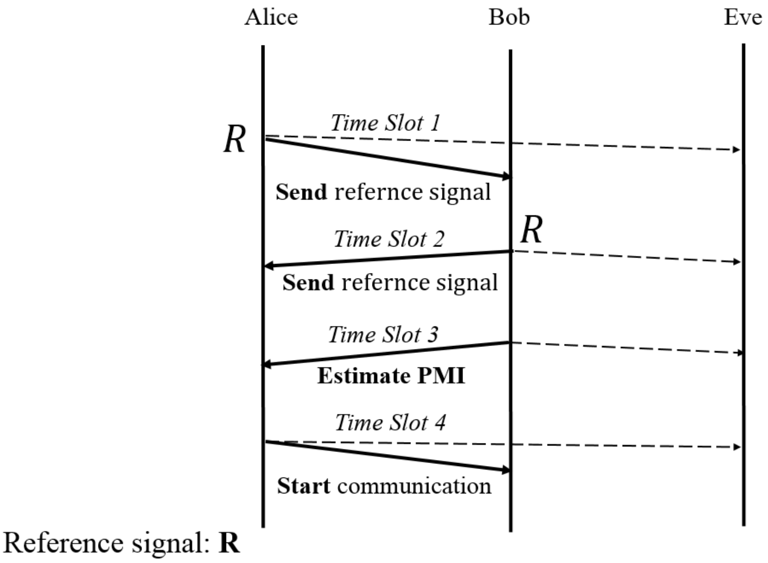

Fig. 2. Signaling procedure of the MOP scheme.

flexibility to distribute the different bandwidth to different channels. This prevents the wasting of the spectrum usage and requires less complexity and cost in forming up the system。In this way, the channel through which the message sending from Alice to Bob will equal to the channel from Bob to Alice. In other words, $\mathbf{h}_{AB} = \mathbf{h}_{BA}$.

B. Realization

In MOP, Alice first sends out a reference signal to Bob. After receiving the reference signal, Bob will use the signal to make channel estimation and find the corresponding PMI by using the estimated channel information $\mathbf{h}_{AB}$. To prevent Eve from learning the PMI and to avoid feedback overhead, Bob will send back a reference signal to Alice for Alice to make channel estimation and acquire the same PMI. Since $\mathbf{h}_{AE}$, $\mathbf{h}_{BE}$ and $\mathbf{h}_{AB}$ are pairwise independent and $\mathbf{h}_{AB} = \mathbf{h}_{BA}$, Alice and Bob are able to calculate the same PMI and prevent Eve from knowing the information. Finally, they used the PMI as the secret key.

C. Step of MOP Procedure

1) Time slot 1:

Alice sends a reference signal $\mathbf{R} \in \mathbb{C}^{N_A \times N_L}$ for Bob to make channel estimation, where N_A is the number of the antennas Alice had equipped and N_L is the length of the reference signal. After channel estimation, Bob acquired the channel information $\mathbf{h}_{AB,i} \in \mathbb{C}^{N_B \times N_A}$ in the *i*th subcarrier and calculates the averaged channel $\mathbf{h}_{AB} = \frac{1}{n}\sum_{i=1}^{n} h_i^{AB}$ for the subband containing n subcarriers, where N_B corresponds to the number of the antennas Bob had equipped. Bob then computes the PMI $k_{Bob,RSV}$ and $k_{Bob,RSV}$ by finding $\hat{F}_{Bob,RSV} = \arg\max_F C_{H_{AB,F}}$ and $\hat{F}_{Bob,LSV} = \arg\max_F C_{H_{AB,F}}$ respectively, where $\hat{F}_{Bob,RSV} \in \mathbb{C}^{N_A \times n}$, $\hat{F}_{Bob,LSV} \in \mathbb{C}^{N_B \times n}$ and $C_{H_{AB,F}} = \log_2 \det[I_n + \frac{E_s}{n_s \sigma^2} F^\dagger H^\dagger HF]$, and use them as a secret key K_{Bob}.

2) Time slot 2:

Bob sends a reference signal $\mathbf{R} = \left[R(0), R(1), \ldots, R(N-1)\right]^T$ back to Alice for Alice to make channel estimation. After channel estimation, Alice computes the corresponding PMI $k_{Alice,RSV}$ and $k_{Alice,RSV}$ by finding $\hat{F}_{Alice,RSV} = \arg\max_F C_{H_{AB,F}}$ and $\hat{F}_{Alice,LSV} = \arg\max_F C_{H_{AB,F}}$ respectively, where $C_{H_{AB,F}} = \log_2 \det[I_n + \frac{E_s}{n_s \sigma^2} F^\dagger H^\dagger HF]$ and use them as a secret key K_{Alice}.

3) Time slot 3:

The procedures in slot 1 and slot 2 are repeated for all finding the corresponding PMI for all subbands.

4) Time slot 4:

Alice encrypt a data X with K_{Alice} and send it to Bob. Bob decrypts the data with its own key K_{Bob}. After receiving the message sent by Alice, Bob checks if the message matches with X. An error of the key agreement is declared if there is a mismatch with the messages.

Ⅲ. The proposed scheme

The purpose of MOP scheme is to prevent the transmission signal from being known to the eavesdropper. However, the design of the MOP scheme only works under the assumption that the eavesdropper is somehow far away from the legitimate users. As a matter of fact, eavesdropper may be near to the legitimate users. On the other hand, the eavesdropper is able to gain the channel information between the legitimate users and itself by receiving the reference signal. To solve the weakness of MOP, we propose a scheme for the MIMO-OFDM system, enhanced-MOP (E-MOP). Using SPGIS as precoding matrices to generate private keys and design a time slot exchanging algorithm.

The signal transmitting from the transmitter (data in) to the receiver (data out) through the OFDM system are shown in fig 3. The transmitter first sends a signal in the frequency domain, and then the signal will be transformed to the time domain by using Inverse Fast Fourier Transform (IFFT). After the reference signal is encrypted by the precoding matrix, we get $\mathbf{r}_i$ and send it through channel $\mathbf{h}_{AB}$ to the receiver. By doing so, the eavesdropper will not be able to get any useful information about the transmitted

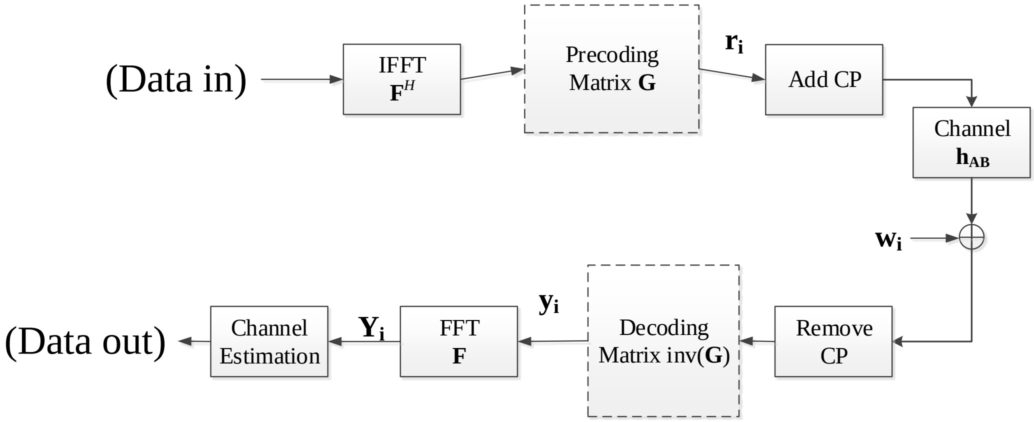

Fig 3 OFDM encryption model

signal even if she has access to encrypted signal. On the other hand, the transmitter will add Cyclic Prefix (CP) in the time domain to eliminate the Inter-Carrier Interference (ICI) and the Inter-Symbol Interference (ISI) between symbols. CP can be removed after the $\mathbf{r}_i$ passes through the channel. After removing CP, the received signal will be decoded base on different situations. Finally, we get $\mathbf{Y}_i$ on then frequency domain by doing Fast Fourier Transform (FFT) to the received signal $\mathbf{y}_i$. The receiver will then estimate the channel and receive the wanted message, and w_i is the channel noise.

A. Definition：

$F\{\cdot\}$ Fast Fourier Transformation, FFT

$(\cdot)^H$ Hermitian Transposition

$\mathbf{r}_i$ ：The encrypted time-domain input signal in Time Slot *i*

$\mathbf{y}_i$ ：The received time-domain signal after removing CP.

$\mathbf{h}_{AB}$ ：The transmission channel between Alice and Bob

$\mathbf{Y}_i$ ：The FFT of $\mathbf{y}_i$

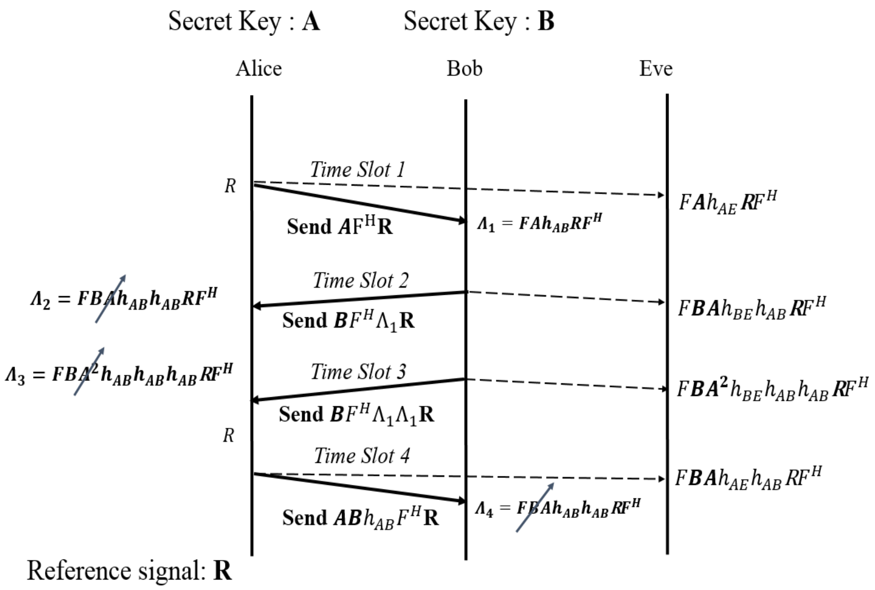
Secret Key : **A**
Secret Key : **B**
Alice
Bob
Eve
R
Time Slot 1
$F\boldsymbol{A}h_{AE}\boldsymbol{R}F^H$
Send $\boldsymbol{A}\mathrm{F}^{\mathrm{H}}\mathbf{R}$
$\Lambda_1 = F\boldsymbol{A}\boldsymbol{h}_{AB}\boldsymbol{R}F^H$
Time Slot 2
$\Lambda_2 = F\boldsymbol{B}\cancel{\boldsymbol{A}}\boldsymbol{h}_{AB}\boldsymbol{h}_{AB}\boldsymbol{R}F^H$
$F\boldsymbol{B}\boldsymbol{A}h_{BE}h_{AB}\boldsymbol{R}F^H$
Send $\boldsymbol{B}F^H\Lambda_1\mathbf{R}$
Time Slot 3
$\Lambda_3 = F\boldsymbol{B}\cancel{\boldsymbol{A}}^2\boldsymbol{h}_{AB}\boldsymbol{h}_{AB}\boldsymbol{h}_{AB}\boldsymbol{R}F^H$
$F\boldsymbol{B}\boldsymbol{A}^2h_{BE}h_{AB}h_{AB}\boldsymbol{R}F^H$
Send $\boldsymbol{B}F^H\Lambda_1\Lambda_1\mathbf{R}$
R
Time Slot 4
$F\boldsymbol{B}\boldsymbol{A}h_{AE}h_{AB}RF^H$
Send $\boldsymbol{A}\boldsymbol{B}h_{AB}F^H\mathbf{R}$
$\Lambda_4 = F\cancel{\boldsymbol{B}}\boldsymbol{A}\boldsymbol{h}_{AB}\boldsymbol{h}_{AB}\boldsymbol{R}F^H$
Reference signal: **R**

Fig 4. Signaling procedure of the MOP scheme.

$\mathbf{\Lambda}_i$ ：The final received signal in Time Slot *i*

B. Secret Key Construction

Assume a SPGIS sequence $\mathbf{g}$, every element of $\mathbf{g}$ can be shown as eq. (3.1):

$$g[n] = \sum_{u=0}^{K-1} c_u \cdot \hat{x}_u[(n - s_u)_N], \tag{1}$$

Whereas c_u, $\hat{x}_u$ and s_u are the amplitude parameter, base sequence and the parameter of cyclic shift respectively and $u = 0,1,\ldots,K$, $n = 0,1,\ldots,N$. K is the number of the bases， N is the length of the sequence.

The precoding matrix **G** in eq. (3.2) is a Circulant Matrix composed by sequence $\mathbf{g}$, and can be used as a private key. It contains three properties: (1) **G** is a circulant matrix which meets the commutative principle for multiplication; (2) **G** is a unitary matrix; (3) Most elements in each column of **G** are zero.

$$G = [\mathbf{g}[n]^{(0)}, \mathbf{g}[n]^{(1)}, \cdots, \mathbf{g}[n]^{(N-1)}], \tag{2}$$

$\mathbf{g}\left[n\right]^{(q)}$ represents the qth cyclic shift position of the sequence $\mathbf{g}$, $q = 0,1,\ldots,N-1$.

C. The E-MOP scheme

Through the exchange of pilot signals in Fig 4, the legitimate users estimates the channel and constructs the precoding matrix to prevent the threat caused by the eavesdropper. First of all, after Alice passes the reference signal R in Time Slot 1, Bob receives $\mathbf{\Lambda}_1$. Similarly, Bob send the encrypted $\mathbf{\Lambda}_1$ and $\mathbf{\Lambda}_1$ $\mathbf{\Lambda}_1$ to Alice for her to receive signal $\mathbf{\Lambda}_2$ and $\mathbf{\Lambda}_3$ in Time Slot 2 and Time Slot 3 respectively. By both $\mathbf{\Lambda}_2$ and $\mathbf{\Lambda}_3$, Alice acquires the channel information between Bob and herself. In the end, Bob receives $\mathbf{\Lambda}_4$ in Time Slot 4 and acquires the same channel information by $\mathbf{\Lambda}_3$ and $\mathbf{\Lambda}_4$. Simultaneously, Eve has received different signals through each Time Slot. The signal received by both the legitimate users and Bob will be derived as the followings.

(1) Time Slot 1：

Alice transmits the reference signal R. After Fourier transformation, Bob receives signal $\mathbf{\Lambda}_1$.

$\mathbf{\Lambda}_1$ is formed in the following deductions:

After **IFFT**($\mathbf{F}^H$) and encrypted by the private key **A,** we get $\mathbf{r}_1$ from $\mathbf{R} = \left[R(0), R(1), \ldots, R(N-1)\right]^T$ **in eq.(3).**

$$\mathbf{r}_1 = \mathbf{A}\mathbf{F}^H\mathbf{R}, \tag{3}$$

Through transmission of $\mathbf{r}_1$ in OFDM system, we get eq.(4), where $\mathbf{h}_{AB}$ is a $N \times N$ circulant matrix with channel vector $N \times 1$ in the first row and L be the channel length.

$$\left[h_{AB}(0), h_{AB}(1), \ldots, h_{AB}(L-1), 0, 0, \ldots, 0\right]^T.$$

$$\mathbf{y}_1 = \mathbf{h}_{AB}\mathbf{r}_1, \tag{4}$$

After a N-point FFT(F), we acquired signal $\mathbf{Y}_1$ shown in eq.(5).

$$\begin{aligned}\mathbf{Y}_1 &= \mathbf{F}\mathbf{y}_1 \\ &= \mathbf{F}\mathbf{h}_{AB}\mathbf{r}_1 \\ &= \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R} \\ &= \mathbf{\Lambda}_1\mathbf{R},\end{aligned} \tag{5}$$

$$\therefore \mathbf{\Lambda}_1 = \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H = diag\left\{\Lambda_1(0), \Lambda_1(1), \ldots, \Lambda_1(N-1)\right\} \tag{6}$$

where $\mathbf{\Lambda}_1$ is a $N \times N$ diagonal matrix.

(2) Time Slot 2：

Bob combines the received $\mathbf{\Lambda}_1$ from Time Slot 1 with $\mathbf{R}$ and turn it into $\mathbf{\Lambda}_1\mathbf{R}$, Alice receives the encrypted $\mathbf{\Lambda}_1\mathbf{R}$ in Time Slot 2 and acquires signal $\mathbf{\Lambda}_2$.

$\mathbf{\Lambda}_1$ is formed in the following deductions:

First of all, Bob multiplies the reference signal with $\mathbf{\Lambda}_1$ and get $\mathbf{\Lambda}_1\mathbf{R}$, transform $\mathbf{\Lambda}_1\mathbf{R}$ with IFFT and encodes it with $\mathbf{B}$ to get signal $\mathbf{r}_2$ as shown in eq.(7).

$$\begin{aligned}\mathbf{r}_2 &= \mathbf{B}\mathbf{F}^H\mathbf{\Lambda}_1\mathbf{R} \\ &= \mathbf{B}\mathbf{F}^H\mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R} \\ &= \mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R},\end{aligned} \tag{7}$$

After removing CP and secret key $\mathbf{A}$ with Hermitian $\mathbf{A}^H$, we get eq.(8).

$$\begin{aligned}\mathbf{y}_2 &= \mathbf{A}^H\mathbf{h}_{AB}\mathbf{r}_2 \\ &= \mathbf{A}^H\mathbf{h}_{AB}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R} \\ &= \mathbf{h}_{AB}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R},\end{aligned} \tag{8}$$

We get eq.(9) from transforming $\mathbf{y}_2$ into the frequency domain.

$$\begin{aligned}\mathbf{Y}_2 &= \mathbf{F}\mathbf{y}_2 \\ &= \mathbf{F}\mathbf{h}_{AB}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R} \\ &= \mathbf{\Lambda}_2\mathbf{R},\end{aligned} \tag{9}$$

$$\therefore \mathbf{\Lambda}_2 = \mathbf{F}\mathbf{h}_{AB}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H = diag\left\{\Lambda_2(0), \Lambda_2(1), \ldots, \Lambda_2(N-1)\right\} \tag{10}$$

(3) Time Slot 3：

Bob combines the received $\mathbf{\Lambda}_1$ from Time Slot 1 with $\mathbf{R}$ and turn it into $\mathbf{\Lambda}_1\mathbf{\Lambda}_1\mathbf{R}$, Alice receives the encrypted $\mathbf{\Lambda}_1\mathbf{\Lambda}_1\mathbf{R}$ in Time Slot 3 and acquires signal $\mathbf{\Lambda}_3$. By both $\mathbf{\Lambda}_2$ and $\mathbf{\Lambda}_3$, Alice acquires the channel information $\mathbf{h}_{AB}$ and private key $\mathbf{B}$.

$\mathbf{\Lambda}_3$, $\mathbf{h}_{AB}$, and precoding matrix $\mathbf{B}$ are obtained in the following deductions:

Bob transform $\mathbf{\Lambda}_1\mathbf{\Lambda}_1\mathbf{R}$ with IFFT and encodes it with $\mathbf{B}$ to get signal $\mathbf{r}_3$ as in eq.(11).

$$\begin{aligned}\mathbf{r}_3 &= \mathbf{BF}^H\mathbf{\Lambda}_1\mathbf{\Lambda}_1\mathbf{R}\\ &= \mathbf{BF}^H\mathbf{Fh}_{AB}\mathbf{AF}^H\mathbf{Fh}_{AB}\mathbf{AF}^H\mathbf{R}\\ &= \mathbf{Bh}_{AB}\mathbf{Ah}_{AB}\mathbf{AF}^H\mathbf{R},\end{aligned} \tag{11}$$

After signal transmission through $\mathbf{h}_{AB}$, Alice compensates the private key $\mathbf{AA}$ with Hermitian $\mathbf{A}^H$, and get $\mathbf{y}_3$ as show in eq.(12).

$$\begin{aligned}\mathbf{y}_3 &= \mathbf{A}^H\mathbf{A}^H\mathbf{h}_{AB}\mathbf{r}_3\\ &= \mathbf{A}^H\mathbf{A}^H\mathbf{h}_{AB}\mathbf{BAh}_{AB}\mathbf{Ah}_{AB}\mathbf{F}^H\mathbf{R}\\ &= \mathbf{h}_{AB}\mathbf{Bh}_{AB}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R},\end{aligned} \tag{12}$$

We get $\mathbf{Y}_3$ by transforming $\mathbf{y}_3$ into the frequency domain by FFT.

$$\begin{aligned}\mathbf{Y}_3 &= \mathbf{Fy}_3\\ &= \mathbf{Fh}_{AB}\mathbf{Bh}_{AB}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}\\ &= \mathbf{\Lambda}_3\mathbf{R},\end{aligned} \tag{13}$$

$$\therefore \mathbf{\Lambda}_3 = \mathbf{FBh}_{AB}\mathbf{Bh}_{AB}\mathbf{h}_{AB}\mathbf{F}^H = diag\left\{\Lambda_3(0),\Lambda_3(1),\ldots,\Lambda_3(N-1)\right\} \text{。} \tag{14}$$

To estimate channel $\mathbf{H_{AB}} = \mathbf{Fh_{AB}F}^H$ and private key $\mathbf{B}$, Alice utilizes the computation between $\mathbf{\Lambda}_2$ and $\mathbf{\Lambda}_3$ to acquire eq.(15).

$$\begin{aligned}\mathbf{\Lambda}_2^{-1}\cdot\mathbf{\Lambda}_3 &= \left(\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H\right)^{-1}\cdot\left(\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H\right)\\ &= \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H \\ &= \mathbf{H}_{\mathbf{AB}}.\end{aligned} \tag{15}$$

From eq.(14), we obtain $\mathbf{h}_{\mathbf{AB}} = \mathbf{F}^H\mathbf{H}_{\mathbf{AB}}\mathbf{F}$ (16)

After substituting eq.(16) into eq.(14), we get $\mathbf{B} = \mathbf{F}^H\mathbf{\Lambda}_2\mathbf{F}(\mathbf{h}_{\mathbf{AB}})^{-1}(\mathbf{h}_{\mathbf{AB}})^{-1}$, (17)

(4) Time Slot 4：

Alice sends a reference signal R through the OFDM precoding system for Bob to receive signal $\mathbf{\Lambda}_4$. By both $\mathbf{\Lambda}_1$ and $\mathbf{\Lambda}_4$, Alice acquires the channel information $\mathbf{h}_{BA}$, which is also $\mathbf{h}_{AB}$.

$\mathbf{\Lambda}_4$ and $\mathbf{h}_{AB}$ are obtained in the following deductions:

In Time Slot 4, the private key is set as $\mathbf{ABh}_{AB}$ which makes $\mathbf{r}_4$ becomes

$$\mathbf{r}_4 = \mathbf{h}_{AB}\mathbf{ABF}^H\mathbf{R}, \tag{18}$$

After signal transmission through $\mathbf{h}_{AB}$, Bob receives $\mathbf{y}_4$:

$$\begin{aligned}\mathbf{y}_4 &= \mathbf{B}^H\mathbf{h}_{AB}\mathbf{r}_4\\ . \quad &= \mathbf{B}^H\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}\\ &= \mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R},\end{aligned} \tag{19}$$

We get $\mathbf{Y}_4$ by transforming $\mathbf{y}_4$ into the frequency domain by FFT.

$$\begin{aligned}\mathbf{Y}_4 &= \mathbf{F}\mathbf{y}_4\\ &= \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}\\ &= \mathbf{\Lambda}_4\mathbf{R},\end{aligned} \tag{20}$$

$$\therefore \mathbf{\Lambda}_4 = \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H = diag\left\{\Lambda_4(0), \Lambda_4(1), \ldots, \Lambda_4(N-1)\right\} \text{。} \tag{21}$$

To estimate channel $\mathbf{H}_{\mathbf{AB}} = \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H$, Bob utilizes the computation between $\mathbf{\Lambda}_1$ and $\mathbf{\Lambda}_4$ which is shown from eq.(22) to eq.(24).

$$\mathbf{\Lambda}_1 = \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{A}\mathbf{F}^H, \tag{22}$$

$$\mathbf{\Lambda}_4 = \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{A}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H, \tag{23}$$

$$\begin{aligned}\mathbf{\Lambda}_1^{-1}\cdot\mathbf{\Lambda}_4 &= \left(\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{A}\mathbf{F}^H\right)^{-1}\cdot\left(\mathbf{F}\mathbf{A}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H\right)\\ &= \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{F}^H\\ &= \mathbf{H}_{\mathbf{AB}}.\end{aligned} \tag{24}$$

After acquiring the channel information $\mathbf{H}_{\mathbf{AB}}$, Alice and Bob collects the same PMI and set the PMI as precoding matrix to enhance transmission security.

After the message exchanging in the four Time Slots, the legitimate users acquires four signals respectively. Simultaneously, Eve has obtained for signals as well, shown in the followings.

$$\mathbf{F}\mathbf{h}_{AE}\mathbf{A}\mathbf{R}\mathbf{F}^H \tag{25}$$

$$\mathbf{F}\mathbf{h}_{BE}\mathbf{h}_{AB}\mathbf{B}\mathbf{A}\mathbf{R}\mathbf{F}^H \tag{26}$$

$$\mathbf{F}\mathbf{h}_{BE}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{A}^2\mathbf{B}\mathbf{R}\mathbf{F}^H \tag{27}$$

$$\mathbf{F}\mathbf{h}_{AE}\mathbf{h}_{AB}\mathbf{B}\mathbf{A}\mathbf{R}\mathbf{F}^H \tag{28}$$

D. The Transmission Security Detection

The previous chapters were focusing on signals obtained by the legitimate users through message exchanging in the Time Slots. Similarly, the eavesdropper obtains messages during the process of the message exchanging as well. Hence, in this chapter, we focus on checking the possibility of Eve gaining the access to either precoding

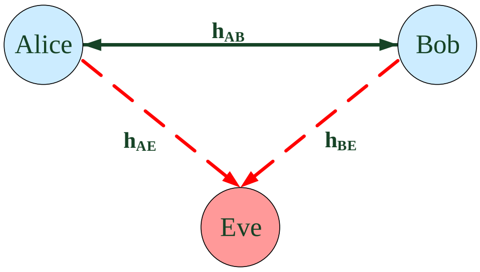
Alice
Bob
Eve
$\mathbf{h}_{\mathbf{AB}}$
$\mathbf{h}_{\mathbf{AE}}$
$\mathbf{h}_{\mathbf{BE}}$

Fig 5. Position structure model

matrix or channel information. During the procedure of communication, it is considered that the result may be different as Eve moves to different locations. Consequently, this research takes the distance between Eve and the legitimate users into consideration and comes up with three different conditions. Condition one: the wireless channels are independent by a distance of several wavelength that is the channels between the three users (Alice, Bob and Eve) are considered independent. Condition two: when Eve is near Bob, away from Alice. Condition three: when Eve is near Alice, away from Bob.

Condition 1:

By knowing the signal received by Eve through eq. (25) to (28), we compensate the reference signal $\mathbf{R}$ and simplifies the signals as follows.

$$\begin{cases} \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^{2}\mathbf{B}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \end{cases} \rightarrow \begin{cases} (\mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^{H})^{-1}\bullet(\mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H}) = \mathbf{h}_{\mathbf{AB}}\mathbf{B} \\ (\mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H})^{-1}\bullet(\mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^{2}\mathbf{B}\mathbf{F}^{H}) = \mathbf{h}_{\mathbf{AB}}\mathbf{A} \end{cases} \tag{29}$$

From eq(29), we found out the only accessible information for Eve are $\mathbf{h}_{\mathbf{AB}}\mathbf{A}$ and $\mathbf{h}_{\mathbf{AB}}\mathbf{B}$. This result shows that it will not be able for Eve to acquire both the channel information $\mathbf{h}_{\mathbf{AB}}$ and $\mathbf{h}_{AE}$, which can prevent the possibility of Eve to reconstruct the

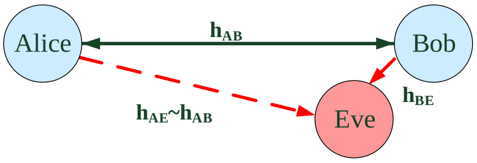

Fig 6. Position structure model

entire wireless environment in its whole surroundings and obtain the precoding matrix.

Condition 2:

As Eve approaches Bob, we consider Eve and Bob locates in the directly same position. Thus, the channel between Eve and Alice will approximates to the channel between Bob and Alice, which is $\mathbf{h}_{AE} \approx \mathbf{h}_{AB}$. The signal received by Eve will have the following form.

$$\begin{Bmatrix} \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^2\mathbf{B}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H \end{Bmatrix} \rightarrow \begin{Bmatrix} \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{A}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^2\mathbf{B}\mathbf{F}^H \\ \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H \end{Bmatrix}$$

After simplifying the four information, we obtain

$$\rightarrow \begin{cases} (\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{A}\mathbf{F}^H)^{-1} \bullet (\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H) = \mathbf{h}_{\mathbf{AB}}\mathbf{B} \\ (\mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^H)^{-1} \bullet (\mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^2\mathbf{B}\mathbf{F}^H) = \mathbf{h}_{\mathbf{AB}}\mathbf{A} \end{cases} \quad (30)$$

Under this condition, we found out the only accessible information for Eve are $\mathbf{h}_{\mathbf{AB}}\mathbf{A}$ and $\mathbf{h}_{\mathbf{AB}}\mathbf{B}$. This result shows that it will not be able for Eve to acquire both the channel information $\mathbf{h}_{\mathbf{AB}}$ and $\mathbf{h}_{AE}$, which can prevent the possibility of Eve to reconstruct

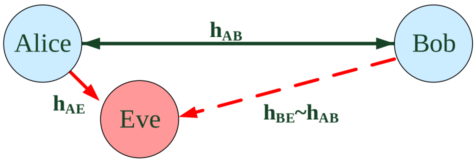

Fig 7. Position structure model

the entire wireless environment in its whole surroundings and obtain the precoding matrix as well.

Condition 3:

As Eve approaches Alice, we consider Eve and Alice locate at the same position. Thus, the channel between Eve and Bob approximates to the channel between Alice and Bob, which is $\mathbf{h}_{BE} \approx \mathbf{h}_{AB}$. The signal received by Eve will have the following form.

$$\begin{Bmatrix} \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{BE}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^{2}\mathbf{B}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \end{Bmatrix} \rightarrow \begin{Bmatrix} \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^{2}\mathbf{B}\mathbf{F}^{H} \\ \mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H} \end{Bmatrix}$$

After simplifying the four information, we obtain

$$\rightarrow \begin{cases} (\mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{A}\mathbf{F}^{H})^{-1} \bullet (\mathbf{F}\mathbf{h}_{\mathbf{AE}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H}) = \mathbf{h}_{\mathbf{AB}}\mathbf{B} \\ (\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{B}\mathbf{A}\mathbf{F}^{H})^{-1} \bullet (\mathbf{F}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{h}_{\mathbf{AB}}\mathbf{A}^{2}\mathbf{B}\mathbf{F}^{H}) = \mathbf{h}_{\mathbf{AB}}\mathbf{A} \end{cases} \tag{31}$$

Under this condition, we found out the only accessible information for Eve are $\mathbf{h}_{\mathbf{AB}}\mathbf{A}$ and $\mathbf{h}_{\mathbf{AB}}\mathbf{B}$ in eq.(31). This result shows that Eve will not be able to acquire both the channel information $\mathbf{h}_{\mathbf{AB}}$ and $\mathbf{h}_{AE}$, which can prevent the possibility of Eve to reconstruct the entire wireless environment in its whole surroundings and obtain the precoding matrix as well.

From the tests conducted above, no matter who Eve approaches, the transmission security will still be enhanced. Due to the fact that Eve is not able to know the secret keys constructed by the legitimate users in advance, the messages obtained during the four Time Slots will be considered ineffective. Simulations will be carry out in the next chapter to verify the results.

IV. Simulation Results

The proposed E-MOP scheme consists of five main processes: conduction of private keys, message exchanging, channel estimation, precoding matrix setup and the transmission security test. To observe the feasibility of the encryption scheme, we will use Normalized Mean Square Error (NMSE) and Bit Error Rate (BER) as indicators for the efficiency analysis of different Time Slots and further observations for the robustness of noise signals. At the same time, it is necessary to prove that the legitimate users acquire the same precoding matrix. On the other hand, we compare the channel capacity for different constructions of precoding matrix. Finally, we compare the E-MOP scheme with the MOP scheme.

MATLAB R2013a is used to conduct the simulation in this research under several assumptions. The number of carriers is assumed to be 128, length of CP to be 16 and the channel to be considered using the Rayleigh model with the energy decaying parameter to be 0.2. We adopt Quadrature Phase Shift Keying (QPSK) modulation in this simulation.

A. Nmse Analysis

To determine the precision of channel estimation, NMSE will be used as an indicator to perform the evaluation. The numerical number of NMSE is directly proportional to the difference between simulation and reality. In channel estimation, LS estimator is used in every Time Slot. The number of Time Slots represent the number of messages exchanging. The channel length is assumed to be 5, L=5. It is shown in Fig 8 that NMSE is approximately 0.017 when the Signal to Noise ratio (SNR) equals to 10dB in Time Slot 1; NMSE is approximately 0.02 when the SNR equals the same in Time Slot 2. It is quite obvious that as the number of the Time Slot

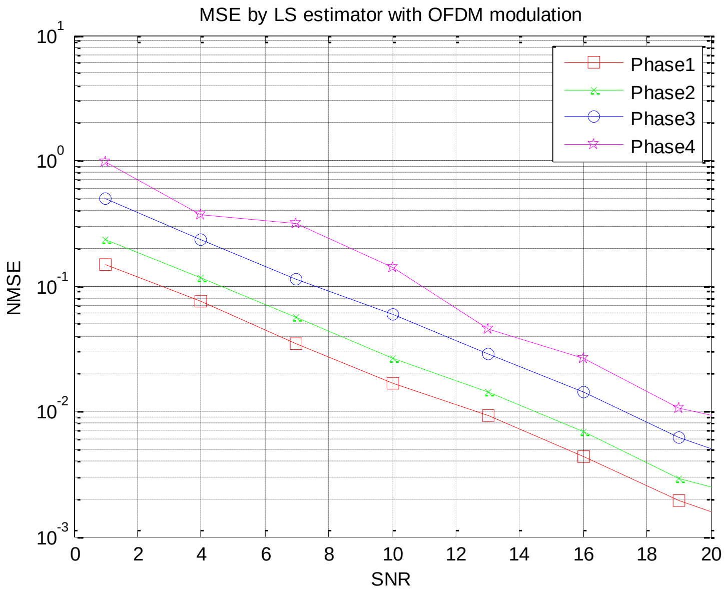

Fig 8 NMSE by LS estimator in different Time Slots

rises, the numerical number of NMSE increases as well. In other words, the more messages exchanging occurs, the higher the NMSE will be. Although it will cause bigger error when the estimation is carried out by the LS estimator rather than by other estimators, it is shown in Fig 8 that after times of message exchanging, the NMSE of the estimation is 0.15 in Time Slot 4 when SNR equals to 10dB, which is still considered small enough. The efficiency of the scheme still reaches a fairly high level.

B. Bit-Error-Rate Analysis

During the process of channel estimation, the channel variation is assumed to be small enough and the legitimate users are considered not far from each other. The squared connected line in Fig 9 shows that the BER maintains at 0.5 under different SNR condition which indicates that Eve is not able to acquire any useful information through the entire communication process. The triangular and star connected line

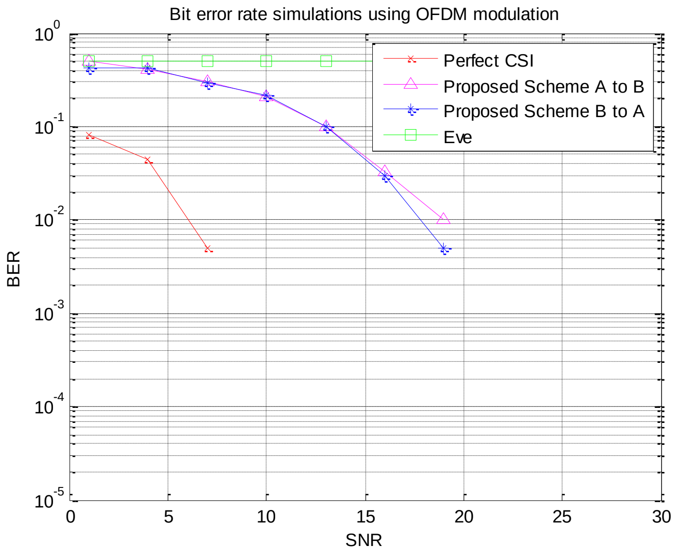

Fig 9 Bit error rate simulations using OFDM modulation

represents the BER to SNR of signal transmitting from A to B and the BER to SNR of signal transmitting from B to A respectively. As shown in Fig 9, the two decaying lines nearly overlapped each other. In other words, Alice and Bob have practically the same results of channel estimation with BER inversely proportional to SNR. It is shown that the BER is below 0.03 when SNR equals 15dB, and the channel estimation will no longer be affected by the noise, BER equals 0, when SNR equals 18dB or higher, which is good enough using the LS estimator. This indicates the high robustness to noise of the E-MOP scheme.

C. Consistency of Precoding Matrix

To ensure that both the transmitter and receiver acquire the same precoding matrix, we first send out a signal encrypted with the precoding matrix, constructed by the transmitter, to the receiver, and then the receiver decrypts the received signal with the precoding matrix, constructed by the receiver, to check if the received signal matches the transmitted signal. Since the precoding matrix is constructed based on the channel

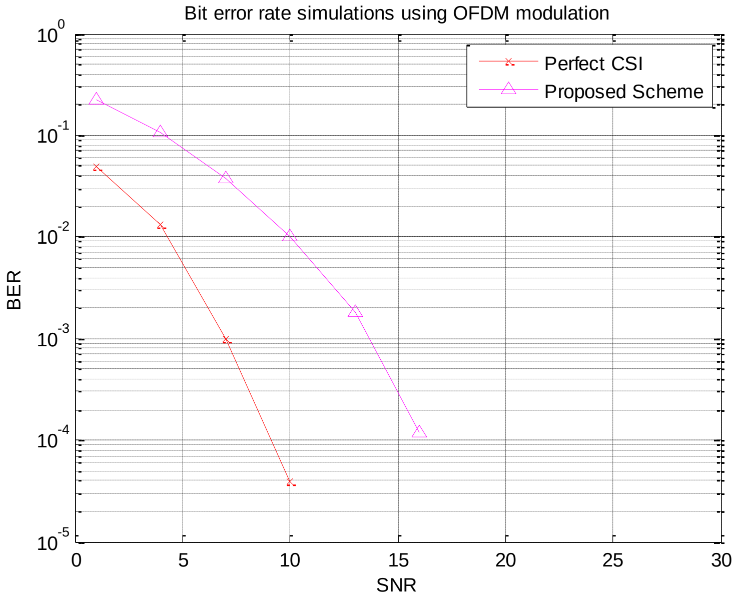

Fig 10 The comparison of BER between FCSI and estimated CSI

information, the precoding matrix acquired by both the transmitter and the receiver will be consistent.

In Fig 10 the BER to SNR curve of the received signal after decryption in the receiver is presented as the following triangle lines. The x line represents the BER to SNR curve under the condition that the precoding matrix are known by both the transmitter and the receiver in advance. In other words, the transmitter and the receiver have Full Channel State Information (FCSI). It is clear to see that the two lines are similar to each other by having the characteristic of exponential decaying, from which it can be proved that the channel estimated by the transmitter and the receiver are quite accurate. In other words, the precoding matrices constructed by the legitimate users are

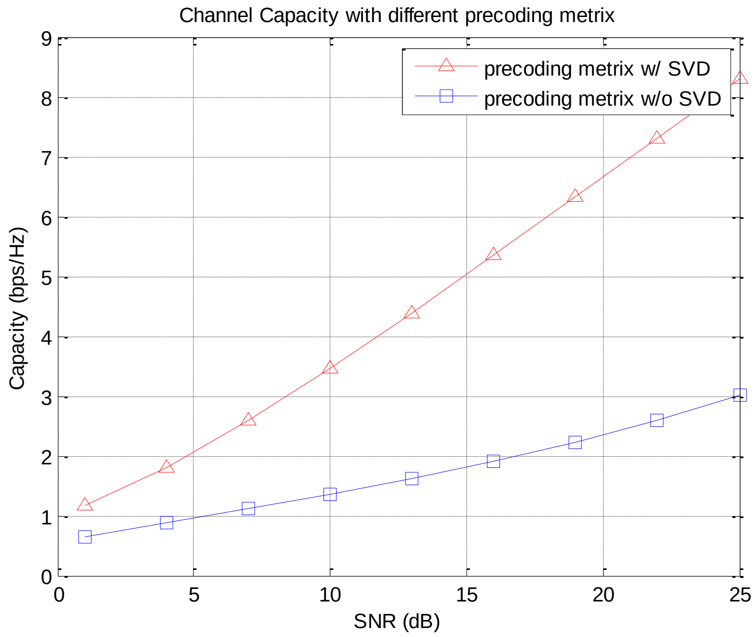

Fig 11 The comparison of channel capacity between different precoding matrices

consistent.

D. Channel Capacity

In this section, channel capacity is discussed. Since different precoding matrix may affect the channel capacity. Here we compare the difference of channel capacity using two different precoding matrices. As shown in Fig. 11, the triangular line represents the channel capacity to SNR curve when precoding matrix based on the corresponding PMI of the channel information in the universal codebook is applied. On the other hand, the square line represents the channel capacity to SNR curve when using the channel information itself as the precoding matrix. It is clearly shown that the triangular line has higher channel capacity under different SNR compare to that of the square line. Besides, the triangular line has a higher increasing rate compare to the square line as SNR increases. These two phenomena directly indicate that construct the precoding matrix find by the corresponding PMI will acquire higher channel capacity.

E. Enhanced Security in E-MOP

The proposed OFDM encryption E-MOP scheme utilizes the message exchanging Time Slot to ensure the transmission security in spite of Eve’s position. Fig 12 compares the performance of E-MOP with that of MOP。E-MOP obtains a BER equal to 0.7 in any SNR level, which is dotted by square in Fig 12. It is clear that the eavesdropper will not obtain any transmission information when nearby either Alice or Bob in the E-MOP scheme. The triangular line represents the BER to SNR curve of signal transmitting from Alice (A) to Bob (B). In contrast, the star dotted line represents the BER to SNR curve of signal transmitting from B to A. The circle dotted line represents the BER to SNR curve of signal transmission when Eve is close to Bob. The BER exponentially decays as SNR increases in the above three lines as shown in Fig 12. In MOP, the circle dotted line and the star dotted line nearly overlaps each other, which indicates that the wireless environment of Eve will become practically equivalent to Bob’s and endangers the transmission security. Similarly, when Eve approaches Alice, the BER of the transmitted signal exponentially decays as SNR increases which is nearly the same result obtained when Eve approaches Bob. Hence Eve is able to eavesdrop the transmitted signal. From the analysis above, we can see that the E-MOP scheme will ensure the transmission security and the nearby eavesdropper problem will be relieved. As mentioned in the beginning, the E-MOP scheme performs better than the MOP in transmission security.

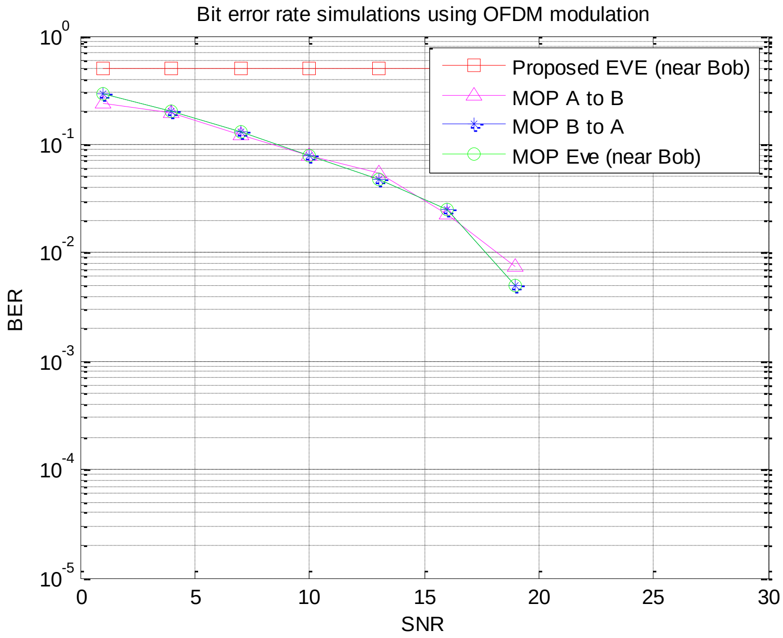

Fig 12 The performance of E-MOP and MOP when Eve is near Bob

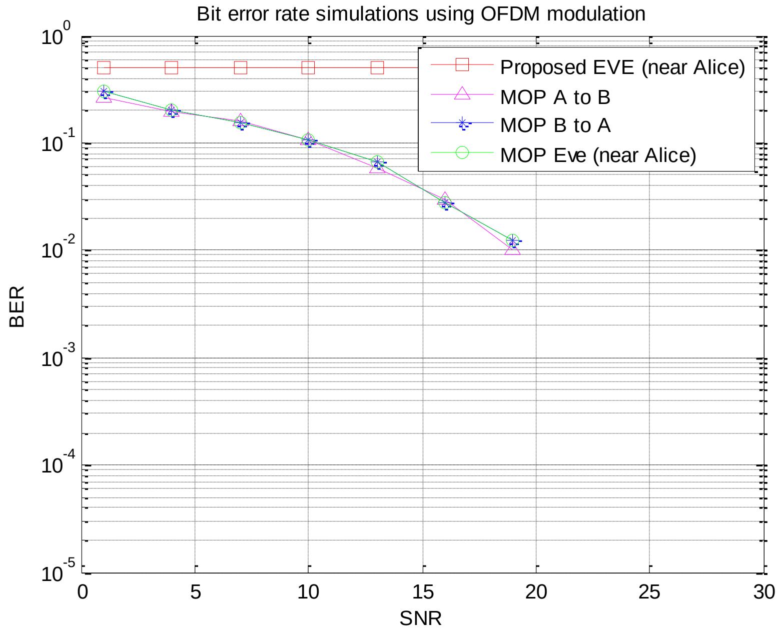

Fig 13 The performance of E-MOP and MOP when Eve is near Alice

V. Conclusions

In this research, we propose an OFDM encryption scheme E-MOP, applying SPGIS to construct private keys. It reduces the computational complexity and enhance signal transmission security in the entire (communication). On the other hand, the message exchanging algorithm is only consisted of four Time Slots and two private keys, which can not only prevent the eavesdropper to reconstruct the entire wireless environment and gain the access of the channel information, but can also prevent the nearby eavesdropping problem from happening. Finally, by constructing the precoding matrix based on the corresponding PMI of channel information will increase channel capacity and make further improvement on the efficiency of message transmission. The most important of all, the E-MOP scheme strengthens the system's capability against eavesdropping and enhance the transmission security in physical layer.

REFERENCES

[1] A. O. Hero, "Secure space–time communication", *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[2] C. Sperandio and P. Flikkema, "Wireless Physical-Layer Security via Transmit Precoding Over Dispersive Channels: Optimum Linear Eavesdropping," *Proc. MILCOM 2002*, vol. 2, pp. 1113–17, Oct. 2002.

[3] X. Li and E. Ratazzi, “Mimo Transmissions with Information-Theoretic Secrecy for Secret-Key Agreement in Wireless Networks,” *IEEE MILCOM 2005*, vol. 3, pp. 1353–59, Oct. 2005.

[4] D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, “Combination of Turbo Coding and Cryptography in Non-Geo Satellite Communication Systems,” *Int’l. Symp. Telecommun.*, pp. 27–28, Aug. 2008.

[5] S. Goel and R. Negi, “Guaranteeing Secrecy Using Artificial Noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–89, June 2008.

[6] S. Goel and R. Negi, “Secret Communication in Presence of Colluding Eavesdroppers,” *IEEE MILCOM 2005*, vol. 3, pp. 1501–06, Oct. 2005.

[7] T. H. Chang, Y. W. P. Hong, and C. Y. Chi, “Training Signal Design for Discriminatory Channel Estimation,” *IEEE GLOBECOM*, pp. 3–5, 11/30~12/4, 2009.

[8] Y. Hwang and H. Papadopoulos, “Physical-Layer Secrecy in AWGN via a Class of Chaotic DS/SS Systems: Analysis and Design,” *IEEE Trans. Sig. Proc.*, vol. 52, no. 9, pp. 2637–49, Sept. 2004.

[9] T. Li *et al.*, “Physical Layer Built-In Security Analysis and Enhancement of CDMA Systems,” *IEEE Military Commun. Conf.*, vol. 2, pp. 956–62, Oct. 2005.

[10] J.-P. Cheng, Y.-H. Li, P.-C. Yeh, and C.-M. Cheng, “MIMO-OFDM PHY Integrated (MOPI) scheme for confidential wireless transmission,” in *Proc. IEEE*

Wireless Comm. and Networking Conf. (WCNC), pp. 1–6, Apr. 2010.

[11] G. Noubir, "On Connectivity in Ad Hoc Network Under Jamming Using Directional Antennas and Mobility," *2nd Int'l. Conf. Wired and Wireless Internet Commun.*, pp. 54–62, 2004.