Secure MIMO Transmission via Compressive Sensing

Chia-Hua Lin, Shang-Ho (Lawrence) Tsai and Yuan-Pei Lin
Department of Electrical Engineering National Chiao Tung University, Hsinchu, Taiwan
E-mails: chlin.ece98g@nctu.edu.tw, shanghot@alumni.usc.edu, and ypl@mail.nctu.edu.tw

***Abstract*—In this paper, we propose a MIMO precoding transceiver to achieve data secrecy at the physical layer. The proposed system exploits the Restricted Isometry Property (RIP) widely used in compressive sensing to encrypt the data. Because the channels at the legitimate receiver and the eavesdropper are inherently different, the corresponding sensing matrices are different. Thus the eavesdropper cannot decode the data successfully. More specifically, when full channel state information (CSI) at the legitimate receiver is known to the transmitter, the proposed precoder can simultaneously maximize receive SNR and attain secrecy. Simulation results corroborate theoretical results, and show that the proposed system enjoys different advantages when different recovery algorithms are used.**

Index Terms — Physical layer secrecy, precoder, transceiver design, compressive sensing (CS), MIMO wiretap channel.

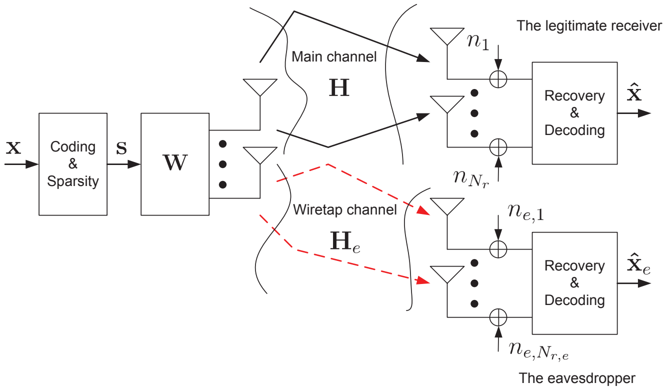

Fig. 1. The proposed system with MIMO wiretap channel.

I. Introduction

In wireless communications, security issue becomes more pronounced because the transmitted data can be accessed by some unauthorized users. Nowadays most of the communications systems encrypt data at the network layer, where key-based encryption techniques are adopted to protect data from stealing. Recently there have been several interesting results on attaining security at the *physical layer*. A main motivation for physical-layer security is that the channels for different users are generally different. The channel discrepancy can be used to encrypt data in a natural way. That is, the channel characteristics of individual users can be treated as "unique key" to encrypt confidential information. The number of keys is theoretically infinite, because the coefficients of the baseband channel are complex numbers. First of all, Wyner investigated the scenario that the transmitter sends information to the legitimate receiver but the information is intercepted by an eavesdropper through a so called wiretap channel. Extending Wyner's results, the authors in [2] characterized the secrecy capacity for the non-degraded discrete memoryless wiretap channel. Several existing precoding techniques for secrecy over MIMO wiretap channels were reviewed in [3].

In this paper, we assume that the transmitter knows only the CSI information of the legitimate user. In addition, the key or the precoding information is known only to the transmitter and the legitimate user, but not to the eavesdroppers, as in [4]. We propose a MIMO precoding system that can achieve the goals. The proposed system can be modeled as an underdetermined linear system. Thus the recovery algorithms designed for Compressive Sensing (CS) can be used to reconstruct the transmitted signals. More specially, when the transmitter knows full CSI of the legitimate receiver (CSI of the eavesdroppers is not needed), we propose an optimal precoder for maximizing the instantaneous SNR. That is, the proposed precoder can simultaneously maximize the SNR as well as attain secrecy. Combining the analysis for both the legitimate receiver and the eavesdroppers, we use two recovery algorithms, which are the simplest Orthogonal Matching Pursuit (OMP) [6] and the most complicated Dantzig selector [7] with the better recovery performance, are conducted to explain these advantages. Simulation results corroborate the theoretical results.

II. System Model and Problem Formulation

A. Problem Formulation for the Legitimate Receiver

The block diagram of the proposed system is shown in Fig. 1. At the first stage, each of the elements of a $K \times 1$ symbol vector $\mathbf{x}$ is randomly allocated to K elements of an $L \times 1$ vector $\mathbf{s}$; the other $L - K$ elements are inserted zeros. Assume $L > K$, $\mathbf{s}$ is therefore a sparse vector. For example, let $K = 3$ and the elements of the symbol vector $\mathbf{x} \in \{-1, 1\}$. If $L = 35$ and $\mathbf{x} = \begin{bmatrix} 1 & -1 & -1 \end{bmatrix}^T$, by randomly allocating the elements of $\mathbf{x}$ to $\mathbf{s}$, a possible $\mathbf{s}$ can be $\mathbf{s} = \begin{bmatrix} 0 & 1 & 0 & -1 & 0 & \cdots & 0 & -1 \end{bmatrix}^T$. A vector $\mathbf{s}$ which only has K nonzero elements is usually called K-sparsity, *i.e.*, $\|\mathbf{s}\|_0 = K$. The bit rate of $\mathbf{s}$ is defined as

$$I_r = \frac{\log_2 2^K \binom{L}{K}}{L} = \frac{K + \log_2 \binom{L}{K}}{L}. \tag{1}$$

Let N_t and N_r be the numbers of transmit and receive antennas respectively, and let $N_t > N_r$. The complex MIMO channel $\mathbf{H}_c \in \mathbb{C}^{N_r \times N_t}$ is assumed to be independent and identically distributed (i.i.d.) $\mathcal{CN}(0, 1)$; therefore, the magnitude of

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

the channel coefficients is Rayleigh distributed. Additionally, we assume that the channel is quasi-stationary so that it does not change for several symbols, *e.g.,* see [5], [8], and [9]. The encryption problem for the legitimate receiver can then be formulated as

$$\mathbf{y}_c = \mathbf{H}_c\mathbf{W}_c\mathbf{s} + \mathbf{n}_c, \tag{2}$$

where $\mathbf{n}_c \in \mathbb{C}^{N_r\times 1}$ is a complex noise vector whose entries are i.i.d. $\mathcal{CN}(0, \sigma_n^2)$, and $\mathbf{W}_c \in \mathbb{C}^{N_t\times L}$ is a complex precoder. For the proposed system, we choose $L > 2N_r$ so that (2) becomes an underdetermined linear model and $\mathbf{\Psi} = \mathbf{H}_c\mathbf{W}_c \in \mathbb{C}^{N_r\times L}$ is called the *sensing matrix*. Since $\mathbf{s}$ is a sparse signal and (2) is an underdetermined linear model, $\mathbf{s}$ can be recovered by using the CS recovery techniques if the sensing matrix $\mathbf{\Psi}$ satisfies the RIP (see [10]), which is defined as follows,

Definition 1: Given the index sets $\mathcal{I} \subset \{1, 2, \ldots, L\}$, a vector $\mathbf{a} \in \mathbb{R}^{|\mathcal{I}|}$ and a matrix $\mathbf{\Psi} \in \mathbb{R}^{M\times L}$, the matrix $\mathbf{\Psi}$ is said to satisfy the Restricted Isometry Property (RIP) with parameter (K, δ) and $K \leq M$, if the following inequality holds.

$$(1-\delta)\|\mathbf{a}\|_2^2 \leq \|\mathbf{\Psi}_{\mathcal{I}}\mathbf{a}\|_2^2 \leq (1+\delta)\|\mathbf{a}\|_2^2,$$

where $0 \leq \delta \leq 1$, and $\mathbf{\Psi}_{\mathcal{I}}$ consists of the columns of $\mathbf{\Psi}$ with indices $\mathcal{I}$ and $|\mathcal{I}| \leq K$.

For systems satisfying the RIP, the recovery algorithm such as linear programming (LP) can be used for solving the ℓ_1 optimization problem, and yielding an exact solution in noiseless channels. A popular family of sensing matrices is the $M \times L$ (real- or complex-valued) random matrices, which satisfy the RIP and lead to a high probability of recovery rate. This paper uses random matrices with i.i.d. entries. The distribution of the entries can be Gaussian or Bernoulli distribution with zero mean and variance $1/L$. It is mentioned in [10] that if the entries of the sensing matrices are generated in this way, the RIP holds and the underdetermined linear model can be perfectly recovered using the ℓ_1 optimization solutions whenever

$$K \leq \beta\frac{M}{\ln(L/M)}, \tag{3}$$

where β is a constant, and now $M = N_r$. In current communication systems, the number N_r of receive antennas is generally not large enough to make $\mathbf{\Psi}$ meet the RIP in (3) for a moderate K. From (3), the number K of sparsity increases as M increases. To increase M, we first convert the complex-valued system into an equivalent real-valued system and then repeatedly transmit the vector $\mathbf{s}$ by T times, which are described separately as follows:

We reformulate the complex-valued system into a real-valued system. More specifically, by rearranging (2), we have

$$\underbrace{\begin{bmatrix} \Re\{\mathbf{y}_c\} \\ \Im\{\mathbf{y}_c\} \end{bmatrix}}_{\mathbf{y}} = \underbrace{\begin{bmatrix} \Re\{\mathbf{H}_c\} & -\Im\{\mathbf{H}_c\} \\ \Im\{\mathbf{H}_c\} & \Re\{\mathbf{H}_c\} \end{bmatrix}}_{\mathbf{H}} \underbrace{\begin{bmatrix} \Re\{\mathbf{W}_c\} \\ \Im\{\mathbf{W}_c\} \end{bmatrix}}_{\mathbf{W}} \mathbf{s} + \underbrace{\begin{bmatrix} \Re\{\mathbf{n}_c\} \\ \Im\{\mathbf{n}_c\} \end{bmatrix}}_{\mathbf{n}}, \tag{4}$$

where $\mathbf{y} \in \mathbb{R}^{2N_r\times 1}$, $\mathbf{H} \in \mathbb{R}^{2N_r\times 2N_t}$, $\mathbf{W} \in \mathbb{R}^{2N_t\times L}$ and $\mathbf{n} \in \mathbb{R}^{2N_r\times 1}$. Now the sensing matrix is $\mathbf{\Phi} = \mathbf{HW} \in \mathbb{R}^{2N_r\times L}$, and its number of rows is doubled compared to the complex-valued system. As a result, the number of sparsity K increases. Herein our designs and performance analysis are based on the real-valued system in (4). The real-valued precoder $\mathbf{W}$ in (4) can be expressed as

$$\mathbf{W} = \begin{bmatrix} \mathbf{P}_1 & \mathbf{P}_2 & \cdots & \mathbf{P}_\alpha \end{bmatrix}, \tag{5}$$

where $\mathbf{P}_i \in \mathbb{R}^{2N_t\times R}$, $1 \leq i \leq \alpha$ is a sub-precoder and R is the rank of the channel matrix $\mathbf{H}$. α is a positive constant and is defined as

$$\alpha = \left\lfloor \frac{L}{R} \right\rfloor.$$

Note that α should be designed to satisfy the RIP in (3), and we will explain later once $\mathbf{P}_1$ is determined, the other sub-precoders $\mathbf{P}_i$, $i \neq 1$, can be determined from $\mathbf{P}_1$ easily. Assume that $\mathbb{E}\{\mathbf{ss}^H\} = (K/L)\sigma_s^2\mathbf{I}_L$, where σ_s^2 is the variance of the sparse vector $\mathbf{s}$. From (4), the instantaneous signal-to-noise ratio (SNR) γ is defined as

$$\gamma = \frac{1}{\sigma_n^2}\frac{\mathbb{E}\{\|\mathbf{HWs}\|_2^2\}}{KN_t}. \tag{6}$$

Moreover, we can repeatedly transmit the same sparse vector using different precoders to increase the number of rows of the sensing matrix. Due to the variant nature of wireless channels, each of the repeated sparse vector experiences different MIMO channels. Let the repeating number be T. From (4), the proposed system with repeated transmission can be formulated as follows,

$$\begin{aligned} \bar{\mathbf{y}} = \begin{bmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_T \end{bmatrix} &= \begin{bmatrix} \mathbf{H}_1 & & \\ & \ddots & \\ & & \mathbf{H}_T \end{bmatrix} \begin{bmatrix} \mathbf{W}_1 \\ \vdots \\ \mathbf{W}_T \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{n}_1 \\ \vdots \\ \mathbf{n}_T \end{bmatrix} \\ &= \overline{\mathbf{H}}\overline{\mathbf{W}}\mathbf{s} + \bar{\mathbf{n}} = \overline{\mathbf{\Phi}}\mathbf{s} + \bar{\mathbf{n}}, \end{aligned} \tag{7}$$

where $\overline{\mathbf{H}} \in \mathbb{R}^{2TN_r\times 2TN_t}$ is a block diagonal matrix with different $2N_r \times 2N_t$ real channel matrices on the diagonal, $\overline{\mathbf{W}} \in \mathbb{R}^{2TN_t\times L}$ is an equivalent precoder with repeating factor T, and $\overline{\mathbf{\Phi}} \in \mathbb{R}^{2TN_r\times L}$ is an equivalent sensing matrix. In a slow fading environment, the repeated sparse vectors of $\mathbf{s}$ may experience similar MIMO channels. This does not affect the RIP of the proposed system, and may not affect the long-term time average recovery performance. However this may affect the short-term time average performance, *e.g.,* channel with serious fading and thus resulting in poor performance during this period. The penalty is that the decoding latency becomes long, which is limited by the channel coherent time. Now $M = 2TN_r$, by properly choosing T, the sensing matrix satisfies (3) and can recover a sparse vector with high probability. Due to the repeating transmission, the equivalent instantaneous SNR Γ can be expressed as

$$\Gamma = \frac{1}{\sigma_n^2}\frac{\mathbb{E}\{\|\overline{\mathbf{H}}\overline{\mathbf{W}}\mathbf{s}\|_2^2\}}{TKN_t}. \tag{8}$$

Similar to (1), the bit rate with repeating transmission then becomes

$$I_R = \frac{I_r}{T} = \frac{\log_2 2^K \binom{L}{K}}{TL} = \frac{K + \log_2 \binom{L}{K}}{TL}. \tag{9}$$

B. Problem Formulation for Eavesdropper

The wiretap channel may be applied to the proposed system and the overall system is shown in Fig. 1, where the communications is eavesdropped. To steal data, the eavesdroppers need to know the repetition number T, and the numbers of transmit and receive antennas, *i.e.* N_t and N_r respectively. This increases the decoding effort for eavesdroppers to obtain these parameters before reconstructing the received signals. If the eavesdropper knows T, N_t and N_r, the received signal $\mathbf{y}_e \in \mathbb{R}^{2N_r \times 1}$ of the eavesdroppers can be represented as

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{W} \mathbf{s} + \mathbf{n}_e = \mathbf{\Phi}_e \mathbf{s} + \mathbf{n}_e, \tag{10}$$

where $\mathbf{\Phi}_e = \mathbf{H}_e \mathbf{W}$ is the equivalent sensing matrix to the eavesdroppers. The subscription 'e' is added to reflect the fact that the experienced channels of the eavesdroppers are not the same as the legitimate receiver. When T is known to the eavesdroppers, the problem after repetition can be formulated as follows,

$$\bar{\mathbf{y}}_e = \bar{\mathbf{H}}_e \bar{\mathbf{W}} \mathbf{s} + \bar{\mathbf{n}}_e = \bar{\mathbf{\Phi}}_e \mathbf{s} + \bar{\mathbf{n}}_e, \tag{11}$$

where $\bar{\mathbf{\Phi}}_e \in \mathbb{R}^{2TN_r \times L}$ is the overall equivalent sensing matrix of the eavesdropper. The secrecy of the proposed system is attained as explained as follows: The CSI of individual users is different unless they positions are very close in distance, *i.e.,* within one half distance of the wavelength. For instance letting the carrier frequency be 2.3 GHz, the distance is $\lambda/2 = c/(2f) = 3 \times 10^{10}/(2 \times 2.3 \times 10^9) \approx 6.5$ cm. However if the distance is only 6.5 cm, the legitimate receiver is alert to the eavesdroppers easily. Therefore, it is reasonable to assume $\bar{\mathbf{H}}_e \neq \bar{\mathbf{H}}$. Since the precoding matrix $\bar{\mathbf{W}}$ is highly related to the $\bar{\mathbf{H}}$, and is used as the sensing matrix for decoding, it is very unlikely that the eavesdroppers can reconstruct the signals without knowing the CSI of the legitimate receiver. In addition, later we will discuss that the optimal design of the precoder is not unique, and thus a channel-independent random matrix can be included into the precoder without affecting the optimality. This random matrix can be generated by a unique key (or seed) known only to the transmitter and the legitimate receiver. As a result, this property further enhances the encryption, and the eavesdroppers do not have chance to steal data without knowing the generation key (seed) or the CSI of the legitimate receiver $\bar{\mathbf{H}}$.

III. Proposed Precoder

We describe how to design the precoders to encrypt the transmitted information. The design criterion for the precoder is to maximize the received SNR.

A. Precoder Design for Maximizing Received SNR

The goal of designing the precode is to simultaneously achieve high receive SNR and attain encryption in wiretap channel. Now we show how to design the sub-precoders $\mathbf{P}_i$ to maximize the instantaneous SNR γ, and the equivalent instantaneous SNR Γ defined in (6) and (8), respectively. Letting $\varepsilon_s^2 = \mathbb{E}\{\mathbf{s}\mathbf{s}^H\}$, the instantaneous SNR γ in (6) can be shown to be

$$\gamma = \frac{1}{L}\frac{\varepsilon_s^2}{\sigma_n^2}\frac{\|\mathbf{H}\mathbf{W}\|_F^2}{N_t} == \frac{1}{L}\frac{\varepsilon_s^2}{\sigma_n^2}\frac{\sum_{i=1}^{\alpha}\|\mathbf{H}\mathbf{P}_i\|_F^2}{N_t}. \tag{12}$$

From (12), maximizing γ is equivalent to maximizing the following objective function:

$$\max \gamma = \max \|\mathbf{H}\mathbf{W}\|_F^2 = \max \sum_{i=1}^{\alpha} \|\mathbf{H}\mathbf{P}_i\|_F^2.$$

If $\mathbf{P}_i$, $1 \le i \le \alpha$, are designed independently (we will explain this is true later), the terms $\|\mathbf{H}\mathbf{P}_i\|_F^2$ and $\|\mathbf{H}\mathbf{P}_j\|_F^2$ can be maximized independently; that is, the maximization problem does not need to be solved jointly. Also, since $\|\cdot\|_F^2$ is positive, it yields $\max \sum_{i=1}^{\alpha} \|\mathbf{H}\mathbf{P}_i\|_F^2 = \sum_{i=1}^{\alpha} \max \|\mathbf{H}\mathbf{P}_i\|_F^2$. From the above results, the instantaneous SNR in (6) can be maximized by designing the sub-precoders $\mathbf{P}_i$ using the following relationships:

$$\max \gamma = \max \|\mathbf{H}\mathbf{P}_i\|_F^2. \tag{13}$$

Next we show that the equivalent instantaneous SNR Γ in (8) is maximized if the instantaneous SNR γ for every transmission is maximized. For notational convenience, let $\gamma^{(j)}$ be the instantaneous SNR at the jth transmission. From (8), Γ is expressed as

$$\Gamma = \frac{K}{L}\frac{\varepsilon_s^2}{\sigma_n^2}\frac{\|\bar{\mathbf{H}}\bar{\mathbf{W}}\|_F^2}{TKN_t} = \frac{1}{L}\frac{\varepsilon_s^2}{\sigma_n^2}\frac{\sum_{j=1}^{T}\|\mathbf{H}_j\mathbf{W}_j\|_F^2}{TN_t}. \tag{14}$$

From (13), $\max \sum_{j=1}^{T} \|\mathbf{H}_j \mathbf{W}_j\|_F^2 \equiv \max \sum_{j=1}^{T} \gamma^{(j)}$ for $\{\gamma^{(j)}, 1 \le j \le T\}$. Moreover, individual transmissions are assumed to be independent because channels are independent. Since $\|\cdot\|_F^2$ are positive value, $\max \sum_{j=1}^{T} \gamma^{(j)} \equiv \sum_{j=1}^{T} \max \gamma^{(j)}$. Thus we obtain the following relationships:

$$\max \Gamma \equiv \sum_{j=1}^{T} \max \gamma^{(j)}. \tag{15}$$

From (13) and (15), we have the following proposition.

Proposition 1: The SNR Γ in (8) is maximized if the sub-precoder $\{\mathbf{P}_i, 1 \le i \le \alpha\}$ in (5) is designed to maximize γ for every transmission. That is, Γ is maximized if $\mathbf{P}_i$ is designed to maximize the following value

$$\sum_{i=1}^{\alpha} \max \|\mathbf{H}\mathbf{P}_i\|_F^2, \tag{16}$$

for all T transmissions.

The result in Proposition 1 shows that the proposed precoder is to maximize the Frobenius norm of $\mathbf{\Phi}$. This result is similar to that in [11], where the authors shows that a lower bound on the mean-squared error is achieved when $\|\mathbf{\Phi}\|_F^2$ is maximized. Next let us explain how to design the precoders when the transmitter side knows full CSI.

B. Design Strategy for Full CSI

If the transmitter side has full CSI, we discuss how to design the optimal precoder $\mathbf{P}_i$ to maximize the SNR Γ. From (16), $\max \|\mathbf{HP}_i\|_F^2 = \max \operatorname{tr}(\mathbf{P}_i^H\mathbf{H}^H\mathbf{HP}_i)$, where $\mathbf{P}_i^H\mathbf{H}^H\mathbf{HP}_i$ is a Hermitian matrix. Since $\mathbf{H}$ is not a square matrix, we need to do a little trick to obtain the optimal solution. Letting $\mathbf{Q}$ be an $N_t \times N_t$ unitary matrix and $\mathbf{Q} = [\mathbf{P}_i \ \mathbf{Q}_0]$, we can formulate $\operatorname{tr}\left(\mathbf{Q}^H\mathbf{H}^H\mathbf{HQ}\right)$ as

$$\operatorname{tr}\left(\mathbf{Q}^H\mathbf{H}^H\mathbf{HQ}\right) = \operatorname{tr}\left(\mathbf{P}_i^H\mathbf{H}^H\mathbf{HP}_i\right) + \operatorname{tr}\left(\mathbf{Q}_0^H\mathbf{H}^H\mathbf{HQ}_0\right). \tag{17}$$

From (17), we have the inequality

$$\operatorname{tr}\left(\mathbf{P}_i^H\mathbf{H}^H\mathbf{HP}_i\right) \leq \operatorname{tr}\left(\mathbf{Q}^H\mathbf{H}^H\mathbf{HQ}\right) = \left(\mathbf{H}^H\mathbf{H}\right).$$

Performing the SVD for $\mathbf{H}$, *i.e.,* $\mathbf{H} = \mathbf{U\Sigma\hat{V}}^H$, we have

$$\operatorname{tr}\left(\mathbf{P}_i^H\mathbf{H}^H\mathbf{HP}_i\right) \leq \operatorname{tr}(\mathbf{\Sigma}^2). \tag{18}$$

Equality holds if and only if $\mathbf{P}_i = \hat{\mathbf{V}}\mathbf{U}_i$, *i.e.,* a column orthonormal matrix. Thus $\mathbf{P}_i = \hat{\mathbf{V}}\mathbf{U}_i$ for $i = 1, \ldots, \alpha$, where $\hat{\mathbf{V}} \in \mathbb{R}^{2N_t \times R}$ is the right singular vectors corresponding to the R largest singular values of $\mathbf{H}$, and $\mathbf{U}_i$ is an $R \times R$ unitary matrix.

***Proposition** 2:* The optimal sub-precoder $\mathbf{P}_i$ for maximizing the instantaneous SNR of the proposed system is of the form $\mathbf{P}_i = \hat{\mathbf{V}}\mathbf{U}_i$, and $\hat{\mathbf{V}}$ is the right singular vectors corresponding to the $R = \operatorname{rank}(\mathbf{H})$ largest singular values of $\mathbf{H}$. Moreover, the resulting SNR is $\operatorname{tr}\left(\mathbf{\Sigma}^2\right)$ where $\mathbf{\Sigma}$ is the singular value matrix of $\mathbf{H}$. The solutions can be obtained by letting $\mathbf{P}_i = \hat{\mathbf{V}}\mathbf{U}_i$ for $i = 1, \ldots, \alpha$ and the optimal precoder $\mathbf{W}$ in (5) can be designed by

$$\mathbf{W} = \hat{\mathbf{V}} \begin{bmatrix} \mathbf{U}_1 & \mathbf{U}_2 & \cdots & \mathbf{U}_\alpha \end{bmatrix}. \tag{19}$$

***Remark** 1:* The unitary matrices $\mathbf{U}_i$ where $1 \leq i \leq \alpha$ can be obtained by performing the QR decomposition for several random square Gaussian matrices, *i.e.,* $\|\mathbf{H}\hat{\mathbf{V}}\mathbf{U}_i\|_F^2 = \operatorname{tr}(\mathbf{U}_i^H\hat{\mathbf{V}}^H\mathbf{H}^H\mathbf{H}\hat{\mathbf{V}}\mathbf{U}_i) = \operatorname{tr}(\hat{\mathbf{V}}^H\mathbf{H}^H\mathbf{H}\hat{\mathbf{V}})$, which does not destroy the optimality in Proposition 2.

Now consider the precoders used for repeatedly transmitting the sparse vector by T times so as to satisfy the RIP in (3). The equivalent received signal in (7) can be rewritten as

$$\begin{aligned}\bar{\mathbf{y}} &= \bar{\mathbf{H}} \begin{bmatrix} \hat{\mathbf{V}}_1 & & \\ & \ddots & \\ & & \hat{\mathbf{V}}_T \end{bmatrix} \begin{bmatrix} \mathbf{U}_{11} & \cdots & \mathbf{U}_{1\alpha} \\ \vdots & \ddots & \\ \mathbf{U}_{T1} & & \mathbf{U}_{T\alpha} \end{bmatrix} \mathbf{s} + \bar{\mathbf{n}} \\ &= \bar{\mathbf{H}}\bar{\mathbf{V}}\bar{\mathbf{U}}\mathbf{s} + \bar{\mathbf{n}} = \bar{\mathbf{\Phi}}\mathbf{s} + \bar{\mathbf{n}},\end{aligned} \tag{20}$$

where $\bar{\mathbf{V}}$ is the overall precoder, which is a $2TN_t \times TR$ block diagonal matrix, $\hat{\mathbf{V}}_i$ is the singular vectors corresponding to the R largest singular values of $\mathbf{H}_i$ for $i = 1, \ldots, T$, and $\bar{\mathbf{U}}$ is the encryption matrix that is a $TR \times \alpha R$ block matrix with every sub-block being an $R \times R$ unitary matrix obtained by using Remark 1.

***Remark** 2:* According to (20), encryption is attained via two aspects. First, according to Remark 1, the encryption matrix $\bar{\mathbf{U}}$ is independent of channels, and can be generated from random matrices with a unique key (or seed) known only to the transmitter and the legitimate receiver. Without knowing this key (or seed), it is very unlikely that the eavesdroppers can recover the received signals. Secondly with full CSI, the proposed system can achieve the maximum SNR by using the optimal precoder. Meanwhile the system is automatically encrypted because $\hat{\mathbf{V}}_i$ is from the unique CSI between the transmitter and the legitimate receiver.

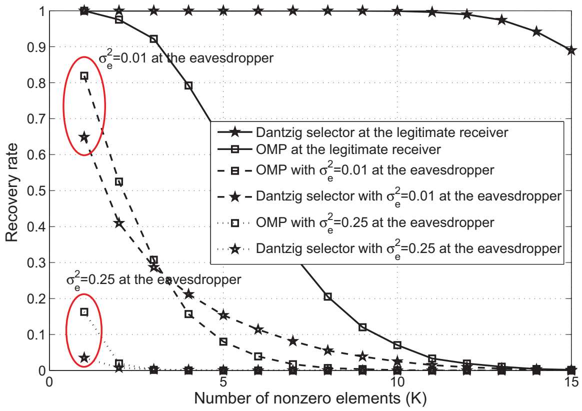

Fig. 2. The eavesdropper estimates the different levels of full CSI at the transmitter.

IV. Simulation Results

In all experiments, the data information is encoded into sparse vectors with length $L = 64$, and the nonzero elements are ± 1. More than 100000 iterations were conducted to compute the recovery rate. The MIMO antennas are $N_r = 4$ and $N_t = 7$. The 16 unitary matrices, *i.e.,* $\mathbf{U}_i$ were generated by conducting the QR decomposition for 16 4×4 square Gaussian random matrices. Three recovery algorithms were used to reconstruct the signals including the Orthogonal Matching Pursuit (OMP) and the Dantzig selector. Note that the Dantzig selector with the most powerful recovery algorithm in CS currently can be regarded as a benchmark.

Experiment 1. The eavesdroppers knew $\bar{\mathbf{U}}$ and different levels of CSI. Consider the worst case that the eavesdroppers know $\bar{\mathbf{U}}$ and also different levels of noisy CSI. The channel known to the eavesdropper is $\mathbf{H}_e = \mathbf{H}_c + \sigma_e\delta$, where δ is assumed to be i.i.d. $\mathcal{CN}(0,1)$ and σ_e^2 is the mean squared estimation error. Since the eavesdropper uses $\mathbf{H}_e$ to obtain the precoder $\bar{\mathbf{V}}_e$, which is very different from the true precoder $\bar{\mathbf{V}}$. Consequently, it results in very different equivalent sensing matrix and the recovery performance of eavesdroppers degrades significantly. Let the SNR be 30 dB. Fig. 2 shows the simulation results. Observe that the recovery rate is low for the eavesdropper. With $\sigma_e^2 = 0.01$, the recovery rate is only 65% for one sparsity using the benchmark Dantzig selector. This shows that the Dantzig selector is very sensitive to the accuracy of the CSI. For $\sigma_e^2 = 0.25$, the eavesdroppers can hardly reconstruct any data with either OMP or the Dantzig selector. Therefore, recovery performance is poor for the eavesdroppers if they do not know the exact CSI.

Experiment 2. Recovery rate for different SNR. Let $T = 5$, Fig. 3 shows the recovery performance for SNR = 10, 20 and 30 dB. Observe from the figure, the Dantzig selector can

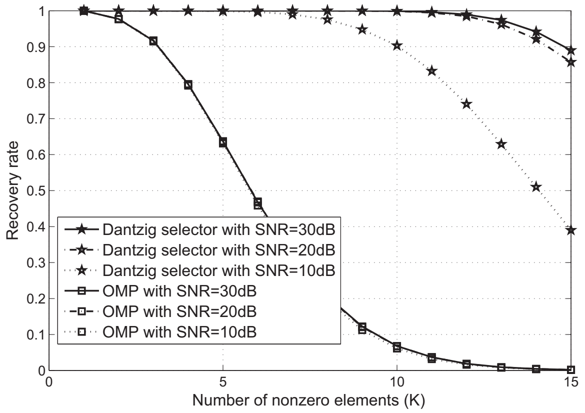

Fig. 3. Recovery rate with different SNR.

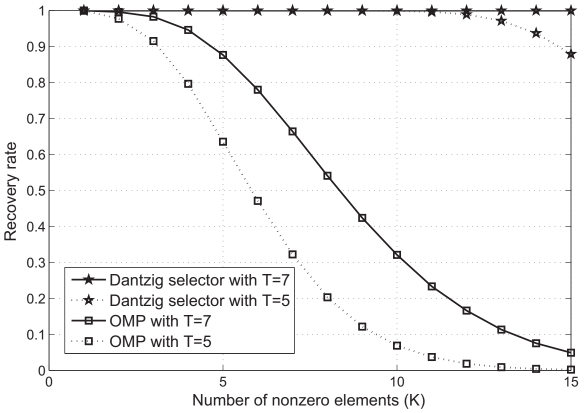

Fig. 4. Recovery rate for different T.

perfectly recover the sparse vector with $K \leq 10$ when SNR is greater than 20 dB. On the other hand, although the OMP algorithm is simple but its recovery performance is far worse than that of the Dantzig selector.

Experiment 3. Recovery rate for different repeating numbers T. Let the SNR be 25 dB, Fig. 4 shows the recovery performance for $T = 5$ and 7. Observe that for the Dantzig selector, decreasing T from 7 to 5 does not degrade the performance seriously. On the other hand, for the OMP algorithm, increasing T improves the performance significantly. In addition, the Dantzig selector with $T = 5$ outperforms the OMP algorithm with $T = 7$. Since increasing T would decrease the bit rate, this example shows that using powerful recovery algorithm can improve bit rate for the proposed system efficiently.

Experiment 4. Recovery rate using the proposed precoder. The performance using the proposed precoder is shown in Fig. 5. From the figure, although the Dantzig selector needs high computational complexity, it is not that sensitive to the precoder compared to the OMP algorithm. Moreover, at $K = 12$ the recovery rate of the Dantzig selector is degraded as 8% approximately. For OMP algorithm, Fig. 5 shows that if $K = 3$ for the randomized precoder, then the recovery rate is approximately 80%. In other words, the eavesdropper using OMP algorithm and does not obtain the truly precoder, so the eavesdropper desires to obtain the information hardly.

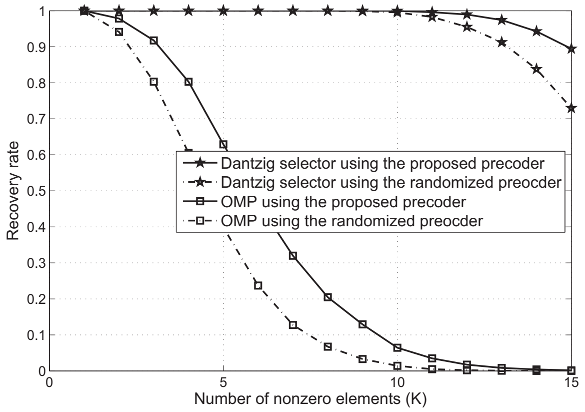

Fig. 5. Recovery rate using the precoder and the randomized precoder.

V. Conclusion

In this paper, we have proposed a precoding to achieve data secrecy at the physical layer. The precoding procedure makes the proposed system an underdetermined linear system. Thus recovery algorithms for compressive sensing can be used to reconstruct the transmitted signals. When full CSI is available, the proposed precoder can maximize the receive SNR. At the same time, the proposed precoder can be regarded as a key to encrypt the signals. If the eavesdroppers do not know the key, it is almost unlikely for eavesdroppers to reconstruct the data.

References

[1] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[2] I. Csisžar and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: survey," 2010, arXiv:1011.3754.

[4] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-Key Agreement With Channel State Information at the Transmitter," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 672-681, Sept. 2011.

[5] D. J. Love and R. W. Heath, Jr., "Limited feedback unitary precoding for spatial multiplexing systems," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2967-2976, Aug. 2005.

[6] J. A. Tropp, "Greed is good: algorithmic results for sparse approximation," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2231-2242, Oct. 2004.

[7] E. J. Candès and T. Tao, "The Dantzig selector: Statistical estimation when p is much larger than n," *Ann. Statist.*, vol. 35, no. 6, pp. 2313-2351, Dec. 2007.

[8] J. C. Roh and B. D. Rao, "Transmit beamforming in multiple-antenna systems with finite rate feedback: a VQ-based approach," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1101-1112, Mar. 2006.

[9] P. Xia and G. B. Giannakis, "Design and analysis of transmit-beamforming based on limited-rate feedback," *IEEE Trans. Signal Process.*, vol. 54, no. 5, pp. 1853-1863, May 2006.

[10] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?," *IEEE Trans. Inf. Theory*, vol. 52, pp. 5406-5425 , Dec. 2006.

[11] E. J. Candès and M. A. Davenport, "How well can we estimate a sparse vector?," *Appl. Comput. Harmon. Anal.*, available online Aug. 2012.