

Transmit Filter and Artificial Noise Design for Secure MIMO-OFDM Systems

Wenfei Liu[†], Ming Li[†], Xiaowen Tian[†], Zihuan Wang[†], and Qian Liu[‡]

[†]School of Information and Communication Engineering

Dalian University of Technology, Dalian, Liaoning 116024, China

E-mail: {liuwenfei, tianxw, wangzihuan}@mail.dlut.edu.cn, mli@dlut.edu.cn

[‡] School of Computer Science and Technology

Dalian University of Technology, Dalian, Liaoning 116024, China

E-mail: qianliu@dlut.edu.cn

Abstract—Physical layer security has been considered as an important security approach in wireless communications to protect legitimate transmission from passive eavesdroppers. This paper investigates the physical layer security of a wireless multiple-input multiple-output (MIMO) orthogonal frequency division multiplexing (OFDM) communication system in the presence of a multiple-antenna eavesdropper. **We first propose a transmit-filter-assisted secure MIMO-OFDM system which can destroy the orthogonality of eavesdropper's signals.** Our proposed transmit filter can disturb the reception of eavesdropper while maintaining the quality of legitimate transmission. Then, we propose another artificial noise (AN)-assisted secure MIMO-OFDM system to further improve the security of the legitimate transmission. The time-domain AN signal is designed to disturb the reception of eavesdropper while the legitimate transmission will not be affected. Simulation results are presented to demonstrate the security performance of the proposed transmit filter design and AN-assisted scheme in the MIMO-OFDM system.

Index Terms—Physical layer security, transmit filter, MIMO-OFDM, artificial noise, power allocation.

I. INTRODUCTION

With the rapid development of wireless communication systems, security has become a crucial issue in wireless networks due to open broadcast nature. Especially, when the important information is transmitting via the wireless medium, an eavesdropper can also receive the signals, resulting in a great threat to the security of the wireless communication systems [1]. Therefore, it is essential for the legitimate transceiver to apply security transmission schemes. Current security schemes rely on the conventional encryption mechanism. However, the cryptography algorithms are based on the computational hardness assumptions, which are still mathematically unproven. Physical layer security is now recognized as an alternative technique in achieving security transmission, which exploits the physical characteristic of wireless channels.

The main principle of physical layer security is making use of the randomness of the wireless channels to disturb eavesdropper's reception without relying on the upper-layer [2]. Many initial physical layer security techniques are investigated in an information-theoretic way. For example, a

seminal physical layer security work proposed by Wyner [3]. Wyner proved that if the wiretap channel was worse than the legitimate channel, then the communication of the legitimate receiver can achieve secure transmission. Based on the pioneering studies of physical layer security, many researches on secrecy capacity have been studied for different channel models, such as Gaussian noise channel, fading channel, Gaussian broadcast channel, etc. Beamforming and power allocation techniques are also investigated to achieve secrecy capacity [4]–[8]. Artificial noise (AN) is another physical layer security technique. AN is generated in the null space of the legitimate channel and can be canceled out at the legitimate receiver but cannot be removed at the eavesdropper.

While most of the previous researches focus on information-theoretic analysis, there is also a growing need to provide practical security solutions. Recently, OFDM has been widely used in wireless communications due to its high performance and low complexity, and the physical layer security in the application of OFDM systems is also well-noticed. Early information-theoretic based techniques utilized in OFDM systems are basically channel coding and cryptography [9]–[11]. In [12], the authors proposed a time-domain AN based physical layer security technology in OFDM systems. In MIMO systems, transmit beamforming designs have been universally utilized by exploiting the spatial degrees of freedom to enhance the physical layer security [13]–[16]. In MIMO-OFDM systems, which have both the advantages of MIMO systems and OFDM systems, physical layer security are also studied [17]–[19].

Inspired by the above studies, in this paper, we propose a transmit-filter-assisted secure scheme and AN-assisted secure scheme in MIMO-OFDM systems. We assume that the transmitter has perfect knowledge of the channel state information (CSI) of legitimate channel. Based on the diversity of the legitimate channel and wiretap channel, the transmit filter is designed based on the legitimate CSI to deliberately destroy the orthogonality of the transmitted signals. Only the legitimate receiver can recover the original signals by making use of the minimum mean square error (MMSE) filter to suppress the inter-carrier interference (ICI). Finally, we apply the AN approach to further improve the transmission security.

The following notation is used throughout this paper. $(\cdot)^T$

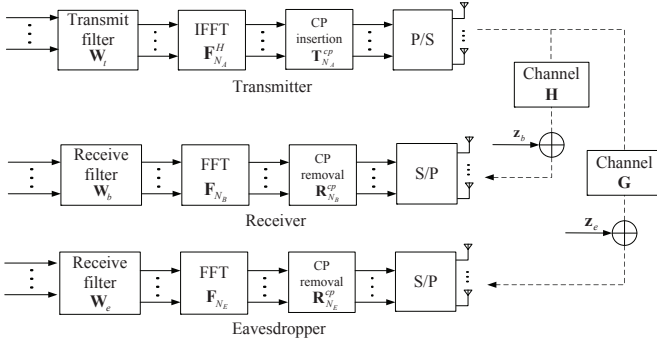


Fig. 1: The filter-assisted secure MIMO-OFDM system.

represents transpose of a matrix. $(\cdot)^H$ represents conjugate transpose of a matrix. $\mathbb{E}\{\cdot\}$ denotes statistical expectation. $\text{Tr}\{\mathbf{X}\}$ denotes the trace of matrix \mathbf{X} . $\mathbb{C}^{M \times N}$ represents $M \times N$ matrices. \mathbf{I}_N represents an $N \times N$ identity matrix. $\text{Diag}(x_1, \dots, x_M)$ represents the $M \times M$ diagonal matrix whose diagonal elements are x_1 to x_M . $\text{null}(\cdot)$ represents the orthonormal bases for the null space of a matrix. $\text{blkdiag}(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_N)$ denotes a block diagonal matrix where the enclosed elements are diagonal blocks. \otimes is the Kronecker product. The function $\min(\cdot, \cdot)$ returns the minimum among the values enclosed in brackets. $\|\cdot\|$ denotes the Enclidean norm of a vector. $[\cdot]_{i,k}$ denotes the (i, k) th entry of a matrix. $[\cdot]_k$ denotes the k th entry of a vector.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a MIMO-OFDM communication system with one transmitter (Alice), one legitimate receiver (Bob), and one eavesdropper (Eve). The number of antennas at node $m \in \{A, B, E\}$ is N_m .

In order to clearly present our MIMO-OFDM system, we first mathematically express the conventional single-input single-output (SISO)-OFDM transmission procedure. Let $\mathbf{s} \triangleq [s_1, s_2, \dots, s_N]^T$ denotes the transmitted signals, where N is the number of subcarriers. \mathbf{F} and \mathbf{F}^H denote the $N \times N$ FFT and IFFT matrices, respectively. \mathbf{T}_{cp} and \mathbf{R}_{cp} are the cyclic prefix (CP) insertion matrix and removal matrix, respectively. The legitimate channel matrix \mathbf{H} is a $(N + N_{cp}) \times (N + N_{cp})$ Toeplitz matrix which can be expressed as

$$\mathbf{H} = \begin{bmatrix} h(1) & 0 & 0 & \dots & 0 \\ \vdots & h(1) & 0 & \dots & 0 \\ h(L) & \dots & \ddots & \dots & \vdots \\ \vdots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & h(L) & \dots & h(1) \end{bmatrix}, \quad (1)$$

where $h(l), l \in \{1, \dots, L\}$, is the channel impulse response from Alice to Bob, and $L < N_{cp}$ is the maximum delay spread. At the receiver, frequency-domain signal of Bob can be expressed as

$$\mathbf{y}_b = \mathbf{F} \mathbf{R}_{cp} \mathbf{H} \mathbf{T}_{cp} \mathbf{F}^H \mathbf{P} \mathbf{s} + \mathbf{n}_b \quad (2)$$

where $\mathbf{n}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2 \mathbf{I}_N)$ is the additive white Gaussian noise (AWGN) vector at the legitimate receiver.

After explicitly explaining the mathematical model of the conventional SISO-OFDM system, we turn to present the wiretap MIMO-OFDM system model as shown in Fig. 1. As for a MIMO-OFDM system, the original signal is firstly processed by a transmit beamformer/filter \mathbf{W}_t , and then transformed to the time domain by IFFT. After CP insertion, the transmitted signal arrives at the receiver through the multipath Rayleigh fading channel. Then, Bob and Eve will remove CP and convert it to the frequency-domain signal by FFT. After that both Bob and Eve use receive filters to recover the original signals.

To mathematically express the MIMO-OFDM system, let $\mathbf{s} \triangleq [s_{1,1}, \dots, s_{1,N}, \dots, s_{N_s,1}, \dots, s_{N_s,N}]^T$ represent the symbol vector to be transmitted via the corresponding subcarriers, $\mathbb{E}\{\|s_{i,j}\|^2\} = 1$, N is the number of orthogonal subcarriers, N_s is the number of data streams of per subcarrier with $N_s \leq N_A$. Let $\mathbf{F}_{N_m} = \mathbf{I}_{N_m} \otimes \mathbf{F} \in \mathbb{C}^{N_m N \times N_m N}$ denote the FFT operation at a node with N_m antennas. $\mathbf{F}_{N_B} = \text{blkdiag}(\mathbf{F}, \mathbf{F}, \dots, \mathbf{F})$ is the FFT matrix and $\mathbf{F}_{N_A}^H = \text{blkdiag}(\mathbf{F}^H, \mathbf{F}^H, \dots, \mathbf{F}^H)$ is the IFFT matrix. The matrix for CP insertion is denoted by $\mathbf{T}_{N_A}^{cp} \in \mathbb{C}^{N_A(N+N_{cp}) \times N_A N}$, where $\mathbf{T}_{N_A}^{cp} = \text{blkdiag}(\mathbf{T}_{cp}, \dots, \mathbf{T}_{cp})$. $\mathbf{R}_{N_B}^{cp} \in \mathbb{C}^{N_B(N+N_{cp}) \times N_B N}$ is the CP removal matrix, and $\mathbf{R}_{N_B}^{cp} = \text{blkdiag}(\mathbf{R}_{cp}, \dots, \mathbf{R}_{cp})$. $\mathbf{W}_t \in \mathbb{C}^{N_A N \times N_s N}$ is the transmit beamformer/filter which has a power constraint, i.e. $\text{Tr}(\mathbf{W}_t \mathbf{W}_t^H) \leq P_t$, where P_t is the total transmit power. $\mathbf{H} \in \mathbb{C}^{N_B(N+N_{cp}) \times N_A(N+N_{cp})}$ is the Alice-to-Bob MIMO multipath channel matrix which is constructed by

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{1,1} & \dots & \mathbf{H}_{1,N_A} \\ \vdots & \ddots & \vdots \\ \mathbf{H}_{N_B,1} & \dots & \mathbf{H}_{N_B,N_A} \end{bmatrix}, \quad (3)$$

$\mathbf{H}_{k,i} \in \mathbb{C}^{(N+N_{cp}) \times (N+N_{cp})}$ is the channel impulse response between the i th antenna of Alice and the k th antenna of Bob, which has a form of

$$\mathbf{H}_{k,i} = \begin{bmatrix} h_{k,i}(1) & 0 & 0 & \dots & 0 \\ \vdots & h_{k,i}(1) & 0 & \dots & 0 \\ h_{k,i}(L) & \dots & \ddots & \dots & \vdots \\ \vdots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & h_{k,i}(L) & \dots & h_{k,i}(1) \end{bmatrix}. \quad (4)$$

The received frequency-domain signal at all antennas of the legitimate receiver can be expressed as

$$\begin{aligned} \mathbf{y}_b &= \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{s} + \mathbf{z}_b \\ &= \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{s} + \mathbf{z}_b, \end{aligned} \quad (5)$$

where $\mathbf{y}_b \in \mathbb{C}^{N_B N \times 1}$ is the received signal vector at Bob, $\mathbf{z}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2 \mathbf{I}_{N_B N})$ is the AWGN vector at Bob, the effective channel matrix

$$\begin{aligned} \tilde{\mathbf{H}} &\triangleq \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \\ &= \text{blkdiag}(\tilde{\mathbf{H}}_1, \tilde{\mathbf{H}}_2, \dots, \tilde{\mathbf{H}}_{N_A}) \end{aligned} \quad (6)$$

is block-diagonal, where $\tilde{\mathbf{H}}_n \in \mathbb{C}^{N_B \times N_A}$ represents the frequency-domain channel matrix of the n th subcarrier from the transmitter to the legitimate receiver.

The Alice-to-Eve channel matrix \mathbf{G} , whose size is $N_E(N + N_{cp}) \times N_A(N + N_{cp})$, has similar constructure as (3), and the received signals at Eve can be given as

$$\begin{aligned} \mathbf{y}_e &= \mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{s} + \mathbf{z}_e \\ &= \tilde{\mathbf{G}} \mathbf{W}_t \mathbf{s} + \mathbf{z}_e, \end{aligned} \quad (7)$$

where $\mathbf{y}_e \in \mathbb{C}^{N_E N \times 1}$ is the received signal vector at Eve. $\mathbf{F}_{N_E} \in \mathbb{C}^{N_E N \times N_E N}$ is the FFT matrix of Eve. $\mathbf{R}_{N_E}^{cp} \in \mathbb{C}^{N_E N \times N_E(N + N_{cp})}$ is the CP removal matrix performed at Eve. $\mathbf{z}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2 \mathbf{I}_{N_E N})$ is the AWGN vector at Eve. The equivalent channel matrix

$$\begin{aligned} \tilde{\mathbf{G}} &\triangleq \mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \\ &= \text{blkdiag}(\tilde{\mathbf{G}}_1, \tilde{\mathbf{G}}_2, \dots, \tilde{\mathbf{G}}_N) \end{aligned} \quad (8)$$

is also block-diagonal, where $\tilde{\mathbf{G}}_n \in \mathbb{C}^{N_E \times N_A}$ represents the frequency-domain channel matrix of the n th subcarrier from the transmitter to the eavesdropper.

After describing the above system model, we can see that the equivalent channel matrix $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{G}}$ have similar structures. This will threaten the MIMO-OFDM systems because Eve can recover the transmitted signals after some demodulation processes. In order to prevent eavesdropping, we propose a transmit-filter-assisted secure MIMO-OFDM technique to maintain the communication security. The transmit filter aims to disturb the received signal of Eve while maintaining the Alice-to-Bob transmission, as will be presented in Section III.

Eve also adopts MMSE

III. TRANSMIT FILTER DESIGN IN MIMO-OFDM SYSTEM

This section is devoted to design the transmit filter in secure MIMO-OFDM system to disturb the reception of Eve. We assume that Alice knows the CSI of the Alice-to-Bob channel link while Eve does not. Based on the diversity between the legitimate channel and wiretap channel, Alice designs the transmit filter to deliberately destroy the orthogonality of the transmitted signals. Both Bob and Eve adopt the MMSE filter to suppress the ICI. However, Eve cannot recover the destroyed signals as what Bob does and then the transmission security can be maintained.

After employing the transmit filter in the frequency-domain, the received MIMO-OFDM signals at Bob and Eve are not orthogonal, i.e. $\tilde{\mathbf{H}} \mathbf{W}_t$ and $\tilde{\mathbf{G}} \mathbf{W}_t$ are not diagonal matrixes. At the receiver, Bob uses the MMSE receive filter to suppress the inter-subcarrier interference. The recovered signal can be expressed as

$$\hat{\mathbf{s}}_b = \mathbf{W}_b^H \mathbf{y}_b, \quad (9)$$

where \mathbf{W}_b is the MMSE receive filter at Bob which is well known as

$$\begin{aligned} \mathbf{W}_b &= (\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H + \sigma_{z_b}^2 \mathbf{I})^{-1} \tilde{\mathbf{H}} \mathbf{W}_t \\ &= (\mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{W}_t^H \mathbf{F}_{N_A} \mathbf{T}_{N_A}^{cp} \mathbf{H}^H \mathbf{F}_{N_B}^H \\ &\quad \mathbf{R}_{N_B}^{cp} \mathbf{F}_{N_B}^H + \sigma_{z_b}^2 \mathbf{I})^{-1} \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t. \end{aligned} \quad (10)$$

Then, with the above MMSE receive filter \mathbf{W}_b , the mean squared error (MSE) at Bob is

$$\begin{aligned} \Gamma_b &= \mathbb{E}\{\|\hat{\mathbf{s}}_b - \mathbf{s}\|^2\} \\ &= \mathbb{E}\{\|\mathbf{W}_b^H \mathbf{y}_b - \mathbf{s}\|^2\} \\ &= \text{Tr}\{\mathbf{W}_b \mathbf{W}_b^H \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H\} + \sigma_{z_b}^2 \text{Tr}\{\mathbf{W}_b \mathbf{W}_b^H\} \\ &\quad - \text{Tr}\{\mathbf{W}_b^H \tilde{\mathbf{H}} \mathbf{W}_t\} - \text{Tr}\{\mathbf{W}_t^H \tilde{\mathbf{H}}^H \mathbf{W}_b\} + N_s N. \end{aligned} \quad (11)$$

Submitting the MMSE receive filter (10) in (11), we can rewrite the MSE at Bob as

$$\begin{aligned} \Gamma_b &= \text{Tr}\{(\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H + \sigma_{z_b}^2 \mathbf{I})^{-1} \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H\}^2 \\ &\quad + \sigma_{z_b}^2 \text{Tr}\{(\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H + \sigma_{z_b}^2 \mathbf{I})^{-1} \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H \\ &\quad (\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H + \sigma_{z_b}^2 \mathbf{I})^{-1}\} - 2 \text{Tr}\{(\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H \\ &\quad + \sigma_{z_b}^2 \mathbf{I})^{-1} \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H\} + N_s N. \end{aligned} \quad (12)$$

Our purpose is to design the transmit filter \mathbf{W}_t which minimizes the MSE (Γ_b). Obviously, this problem is too difficult to be solved. Therefore, we turn to find a suboptimal solution to design \mathbf{W}_t . Since the effective channel $\tilde{\mathbf{H}}$ is available to Alice, we can make the singular value decomposition (SVD) of $\tilde{\mathbf{H}}$ as $\tilde{\mathbf{H}} = \mathbf{U} \mathbf{\Sigma} \mathbf{V}^H$. The columns of $\mathbf{U} \in \mathbb{C}^{N_B N \times N_B N}$ are the left-singular vector of $\tilde{\mathbf{H}}$ and the columns of $\mathbf{V} \in \mathbb{C}^{N_A N \times N_A N}$ are the right-singular vector of $\tilde{\mathbf{H}}$. $\mathbf{\Sigma} = \text{Diag}(\sigma_1, \dots, \sigma_\alpha) \in \mathbb{C}^{N_B N \times N_A N}$ contains the singular values, where $\alpha = \min(N_A N, N_B N)$, and $\sigma_1 \geq \dots \geq \sigma_\alpha$. To transmit $N_s N$ symbols, we simply select the first $N_s N$ columns of \mathbf{V} as \mathbf{V}_t .

Then, the term $\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H$ in (12) can be rewritten as

$$\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H = \mathbf{U} \mathbf{\Sigma} \mathbf{V}_t^H \mathbf{W}_t \mathbf{W}_t^H \mathbf{V}_t \mathbf{\Sigma}^H \mathbf{U}^H. \quad (13)$$

For simplification design purpose, let

$$\mathbf{W}_t = \mathbf{V}_t \mathbf{P} \quad (14)$$

be the transmit filter design, where \mathbf{P} denotes the transmit power matrix and $\mathbf{P} = \text{Diag}(\sqrt{p_1}, \dots, \sqrt{p_{N_s N}})$. The equation (13) can be further simplified as

$$\tilde{\mathbf{H}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{H}}^H = \mathbf{U} \mathbf{\Lambda} \mathbf{U}^H, \quad (15)$$

where $\mathbf{\Lambda} = \mathbf{\Sigma} \mathbf{P}^2 \mathbf{\Sigma}^H = \text{Diag}(\lambda_1, \dots, \lambda_{N_s N})$. Substituting (15) in the original objective function (12), Γ_b can be further expressed as

$$\begin{aligned} \Gamma_b &= \text{Tr}\{((\mathbf{\Lambda} + \sigma_{z_b}^2 \mathbf{I})^{-1} \mathbf{\Lambda})^2\} + \sigma_n^2 \text{Tr}\{(\mathbf{\Lambda} + \sigma_{z_b}^2 \mathbf{I})^{-1} \mathbf{\Lambda} \\ &\quad (\mathbf{\Lambda} + \sigma_{z_b}^2 \mathbf{I})^{-1}\} - 2 \text{Tr}\{(\mathbf{\Lambda} + \sigma_{z_b}^2 \mathbf{I})^{-1} \mathbf{\Lambda}\} + N_s N \\ &= \sum_{i=1}^{N_s N} \frac{\sigma_{z_b}^2}{\sigma_i^2 p_i + \sigma_{z_b}^2}. \end{aligned} \quad (16)$$

After the above equation transform, we turn to solve the power allocation problem for subcarriers instead of the original optimization problem. The final transmit filter design problem can be expressed as

$$\begin{aligned} \min \quad & \sum_{i=1}^{N_s N} \frac{\sigma_{z_b}^2}{\sigma_i^2 p_i + \sigma_{z_b}^2} \\ \text{s.t.} \quad & \sum_{i=1}^{N_s N} p_i \leq P_t, \\ & p_i \geq 0, i = 1, \dots, N_s N. \end{aligned} \quad (17)$$

This power allocation problem can be easily solved by some existing solvers such as CVX solvers. After working out the power allocation of different subcarriers, we can obtain the transmit filter $\mathbf{W}_t = \mathbf{V}_t \mathbf{P}$.

As for Eve, she also uses MMSE receive filter to recover the transmit signals. Similarly as Bob, the recovered signal of Eve can be expressed as

$$\hat{\mathbf{s}}_e = \mathbf{W}_e^H \mathbf{y}_e, \quad (18)$$

where \mathbf{W}_e is the MMSE receive filter which has a similar form as (10)

$$\begin{aligned} \mathbf{W}_e &= (\tilde{\mathbf{G}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{G}}^H + \sigma_{z_e}^2 \mathbf{I})^{-1} \tilde{\mathbf{G}} \mathbf{W}_t \\ &= (\mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{W}_t^H \mathbf{F}_{N_A} \mathbf{T}_{N_A}^{cp} \mathbf{H}^H \mathbf{H} \\ &\quad \mathbf{R}_{N_E}^{cp} \mathbf{H}^H \mathbf{F}_{N_E}^H + \sigma_{z_e}^2 \mathbf{I})^{-1} \mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t. \end{aligned} \quad (19)$$

The MSE at Eve is

$$\begin{aligned} \Gamma_e &= \text{Tr}\{\mathbf{W}_e \mathbf{W}_e^H \tilde{\mathbf{G}} \mathbf{W}_t \mathbf{W}_t^H \tilde{\mathbf{G}}^H\} + \sigma_{z_e}^2 \text{Tr}\{\mathbf{W}_e \mathbf{W}_e^H\} \\ &\quad - \text{Tr}\{\mathbf{W}_e^H \tilde{\mathbf{G}} \mathbf{W}_t\} - \text{Tr}\{\mathbf{W}_t^H \tilde{\mathbf{G}}^H \mathbf{W}_e\} + N_s N. \end{aligned} \quad (20)$$

Based on the fact that the transmit filter \mathbf{W}_t is designed to minimize Γ_b by the use of legitimate CSI \mathbf{H} , Bob can efficiently recover the original signals by employing the receive filter. However, due to the diversity between the wiretap channel \mathbf{G} and the legitimate channel \mathbf{H} , the MSE at Eve Γ_e is much higher than Γ_b . Therefore, after applying the transmit filter, the received signals at Eve will be disturbed and the security will be enhanced.

IV. ARTIFICIAL NOISE DESIGN IN MIMO-OFDM SYSTEM

After developing the transmit-filter-assisted secure scheme, we find that the transformed power allocation problem in section III is intriguing. And it is sensible to adopt another AN-assisted scheme utilizing the residual power to further guarantee the security of the transmission.

Let γ_b denote the MSE threshold of Alice-to-Bob transmission. When $\Gamma_b \leq \gamma_b$, the quality of legitimate transmission can be maintained to a certain extend according to γ_b . Let P_t represent the total transmit power. Denote $P_c = \sum_{i=1}^{N_s N} p_i$ as the consumed power of all symbols utilized to satisfy the MSE constraint $\Gamma_b \leq \gamma_b$. $P_a = P_t - P_c$ represents the residual power after power allocation for different subcarriers. When the MSE constraint is met, i.e., $\Gamma_b \leq \gamma_b$, there exists a minimum power consumption P_c which not only satisfying the legitimate transmission quality, but also has the largest residual power P_a in generating AN. Therefore, the task of the AN-assisted scheme is to minimize the power of all subcarriers P_c under the constraint of Alice-to-Bob transmission quality. The optimal problem can be formulated as follows:

$$\begin{aligned} \min \quad & \sum_{i=1}^{N_s N} p_i \\ \text{s.t.} \quad & \sum_{i=1}^{N_s N} \frac{\sigma_{z_b}^2}{\sigma_i^2 p_i + \sigma_{z_b}^2} \leq \gamma_b, \\ & \sum_{i=1}^{N_s N} p_i \leq P_t, \\ & p_i \geq 0, i = 1, \dots, N_s N. \end{aligned} \quad (21)$$

The solution of this optimal problem can be easily obtained by CVX solvers. After solving this restrained power allocation problem, the residual power is $P_a = P_t - P_c$. Alice generates AN in the time-domain with residual power P_a to interfere the reception of the eavesdropper with the legitimate transmission not affected. AN is applied to the transmission after inserting CP, the received symbols of Bob can be represented as

$$\begin{aligned} \mathbf{y}_b &= \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} (\mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{s} + \mathbf{z}_a) + \mathbf{z}_b \\ &= \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{s} + \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{z}_a + \mathbf{z}_b, \end{aligned} \quad (22)$$

where $\mathbf{z}_a \in \mathbb{C}^{N_A(N+N_{cp}) \times 1}$ is the generated AN vector. $P_a = \text{Tr}\{\mathbb{E}\{\mathbf{z}_a \mathbf{z}_a^H\}\}$ is the power of AN.

In this AN-assisted scheme, AN should be laid in the null space of the Alice-to-Bob channel link so that AN will not influence Bob's reception. Therefore, AN can be generated as

$$\mathbf{z}_a = \mathbf{Q}_a \mathbf{d}, \quad (23)$$

where $\mathbf{Q}_a = \text{null}(\mathbf{R}_{N_B}^{cp} \mathbf{H})$ is an $N_A(N+N_{cp})$ -by- $N(N_A - N_s) + N_{cp} N_A$ matrix, i.e.

$$\mathbf{R}_{N_B}^{cp} \mathbf{H} \mathbf{Q}_a = \mathbf{0}, \quad (24)$$

$$\mathbf{Q}_a \mathbf{Q}_a^H = \mathbf{I}_{N_A(N+N_{cp})}, \quad (25)$$

\mathbf{d} is $(N(N_A - N_s) + N_{cp} N_A) \times 1$ zero-mean complex Gaussian random vector which has the variance of σ_d^2 . Then, the received symbols of Bob in (22) can be rewritten as

$$\begin{aligned} \mathbf{y}_b &= \mathbf{F}_{N_B} \mathbf{R}_{N_B}^{cp} \mathbf{H} (\mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{s} + \mathbf{z}_a) + \mathbf{z}_b \\ &= \tilde{\mathbf{H}} \mathbf{W}_t \mathbf{s} + \mathbf{z}_b. \end{aligned} \quad (26)$$

As for Eve, due to the diversity of channel characteristic, Eve cannot eliminate the affect of AN. The received signal at Eve can be expressed as

$$\begin{aligned} \mathbf{y}_e &= \mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} (\mathbf{T}_{N_A}^{cp} \mathbf{F}_{N_A}^H \mathbf{W}_t \mathbf{s} + \mathbf{z}_a) + \mathbf{z}_e \\ &= \tilde{\mathbf{G}} \mathbf{W}_t \mathbf{s} + \mathbf{F}_{N_E} \mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{z}_a + \mathbf{z}_e. \end{aligned} \quad (27)$$

Since the legitimate channel \mathbf{H} is different from the eavesdropping channel \mathbf{G} , i.e. $\mathbf{R}_{N_E}^{cp} \mathbf{G} \mathbf{z}_a \neq \mathbf{0}$, Eve cannot cancel out AN as Bob does. Therefore, the proposed AN-assisted scheme can further prevent Eve from eavesdropping and increase the security capacity of the MIMO-OFDM systems.

V. SIMULATION RESULTS

In this section, we examine the performance of the proposed transmit-filter-assisted and AN-assisted secure MIMO-OFDM systems. We evaluate the average bit-error-rate (BER) of both Bob and Eve for various total transmit power, the number of subcarriers, the number of antennas at Alice and MMSE constraints. The simulation results are experienced over 10^5 channel realizations.

In this simulation, Alice tries to establish a secure transmission between herself and Bob in the presence of Eve, using a MIMO-OFDM wireless communication system which has $N = 64$ subcarriers and $N_{cp} = 16$. The number of antennas at Alice is $N_A = 4$, and $N_B = N_E = 2$, $N_s = 2$. Fig. 2 shows the BERs of Bob and Eve under different

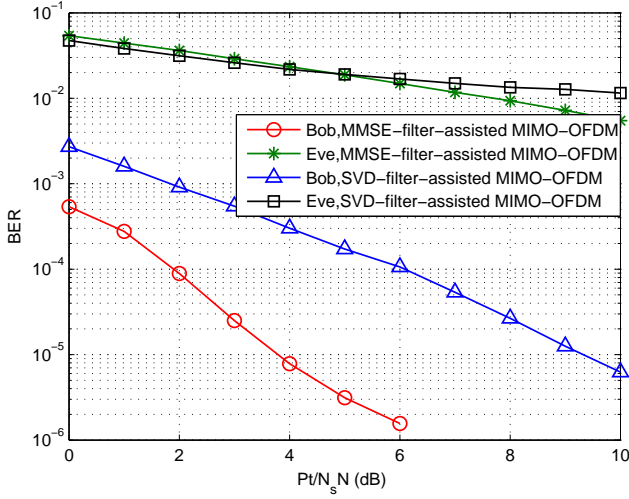


Fig. 2: BER versus transmit power ($N = 64$ subcarriers, length of CP $N_{cp} = 16$, $N_A = 4$, $N_B = N_E = N_s = 2$).

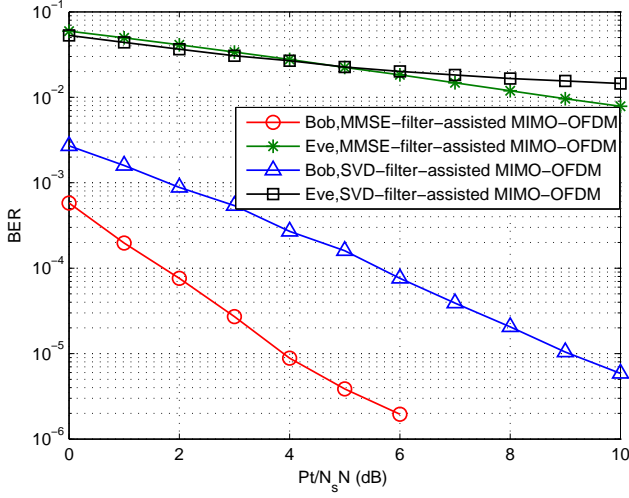


Fig. 3: BER versus transmit power ($N = 128$ subcarriers, length of CP $N_{cp} = 32$, $N_A = 4$, $N_B = N_E = N_s = 2$).

total transmit power constraints. For comparison purpose, we compare the SVD-filter-based scheme [20] with our proposed algorithm. For the proposed transmit-filter-assisted scheme, the BER of Bob is much lower than the conventional SVD-filter-based MIMO-OFDM system. However, the BERs of Eve in both our proposed system and SVD-filter-based system are merely the same and very high, which means that Eve's reception has been significantly degraded. We can also observe from Fig. 2 that the BER gap between Bob and Eve in our proposed scheme is significantly enlarged comparing with the conventional SVD scheme, which demonstrates that our proposed MMSE-filter-assisted MIMO-OFDM system has better security performance.

Then, the simulation results for a MIMO-OFDM system with $N = 128$ subcarriers and $N_{cp} = 32$ are shown in Fig. 3, which has the similar performance as Fig. 2. The BER of Bob

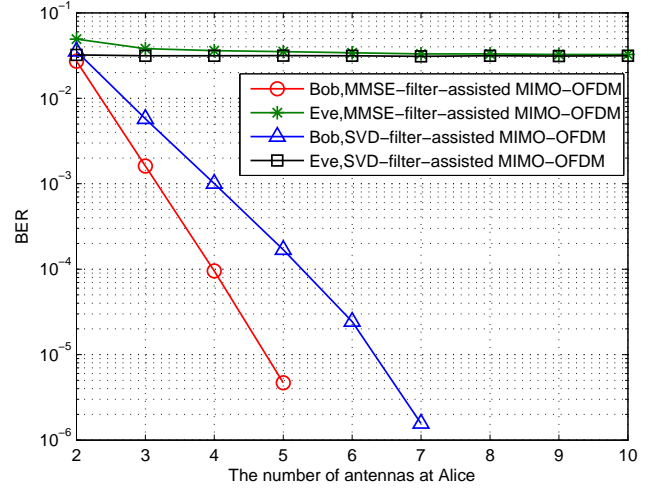


Fig. 4: BER versus the numbers of antennas at Alice ($N = 64$ subcarriers, $N_{cp} = 16$, $N_B = N_E = N_s = 2$).

in MMSE-filter-assisted system can achieve (by all practical measures) errorless transmission at SINR 6dB, while Eve has much higher error rate. These findings demonstrate that the proposed MMSE-filter-assisted scheme can significantly ensure the security of MIMO-OFDM systems.

Fig. 4 shows the BERs of Bob and Eve for various numbers of antennas at Alice. We evaluate the number of N_A from 2 to 10 and fix $N_B = N_E = N_s = 2$. The number of subcarriers $N = 64$ and the length of CP $N_{cp} = 16$. From Fig. 4 we can notice that with the increase of the number of antennas at Alice, the BERs of Bob will decrease to a large extent while the BERs of Eve remains unchanged. The reason is that the larger antennas of Alice, the more degrees of freedom (DoF) to design signals for anti-eavesdropping. In Fig. 4, the BER of Bob with the proposed approach is much lower than the SVD scheme which illustrates our proposed scheme can achieve much better performance in the MIMO-OFDM wireless communications.

Next, we present the performance of the AN-assisted secure MIMO-OFDM scheme in Fig. 5. We fix the MMSE constraint as $\gamma_b = 10$ and show the BERs of Bob and Eve as a function of $P_t/N_s N$. In Fig. 5, the BER gap between Bob and Eve in the proposed AN-assisted secure MIMO-OFDM system is enlarged comparing with no AN scheme. With the MMSE constraint, the BER of Bob nearly keeps in a straight line. Moreover, the BER of Bob remains unchanged when adding AN which illustrates that AN will be canceled out at Bob and can further disturb the reception of Eve.

In Fig. 6, the total transmit power is fixed as $P_t = 50$ dB and the horizontal axis is the MMSE constraint γ_b of Γ_b at Bob (i.e. $\Gamma_b \leq \gamma_b$). Fig. 6 shows that the BER of Eve is higher when adding AN while the BER of Bob remains unchanged. It illustrates that AN can prevent Eve from eavesdropping and maintain the security of Alice-to-Bob transmission. Fig. 6 also shows that with the increase of γ_b , the performance of Bob will be worse which demonstrates that our proposed MMSE-filter-assisted MIMO-OFDM scheme can influence the performance

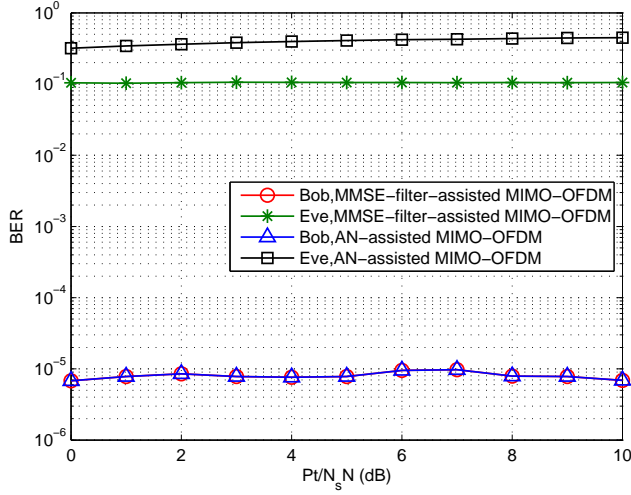


Fig. 5: BER versus total transmit power ($N = 64$, $N_{cp} = 16$, $N_A = 4$, $N_B = N_E = N_s = 2$, MMSE constraint $\gamma_b = 10$).

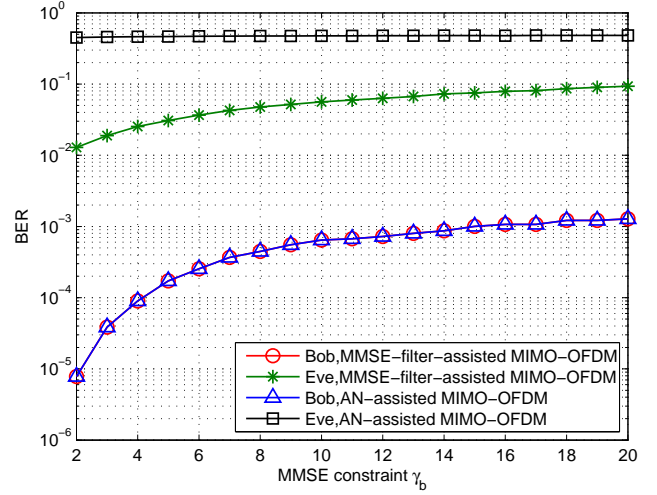


Fig. 6: BER versus MMSE constraint γ_b ($N = 64$, $N_{cp} = 16$, $N_A = 4$, $N_B = N_E = N_s = 2$, transmit power $P_t = 50$ dB).

of Bob. The numerical results show that the proposed AN-assisted secure MIMO-OFDM scheme can achieve better security transmission than the MIMO-OFDM system without AN.

VI. CONCLUSION

In this paper, we considered the problem of securing the MIMO-OFDM wireless transmission between the transmitter and the legitimate receiver in the presence of an eavesdropper. We proposed two novel schemes to improve physical layer security for MIMO-OFDM wireless communication systems. The MMSE-filter-assisted secure MIMO-OFDM system aims to disturb the orthogonality of the received signals at Eve to enhance the security of the Alice-to-Bob transmission. To further improve the performance, we proposed another AN-assisted scheme to enhance the physical layer security in MIMO-OFDM systems. Simulation results shown that the proposed schemes can significantly improve the physical layer security for the MIMO-OFDM wireless communication systems.

REFERENCES

- [1] Y. S. Shiu, S. Y. Chang, and H. C. Wu, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, April 2011.
- [2] A. Mukherjee, S. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Aug. 2014.
- [3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [4] U. Hamid, R. A. Qamar, and K. Waqas, "Performance comparison of time-domain and frequency-domain beamforming techniques for sensor array processing," *Int. Bhurban Conference on Appl. Sci. & Technology*, Islamabad, Pakistan, Jan. 2014, pp. 379-385.
- [5] Y. Chen, X. Hu, and Z. Tan, "Power allocation for OFDM-DF cooperative communication," *Commun. and Mobile Computing*, Qingdao, China, April 2011, pp. 319-322.
- [6] E. Amankwa, M. Look, and E. Kritzing, "A conceptual analysis of information security education, information security training and information security awareness definitions," *Internet Technol. and Secured Trans.*, London, UK, Dec. 2014, pp. 248-252.
- [7] Z. Wang, L. Li, and H. Wang, "Beamforming design in relay-based full-duplex MISO wireless powered communication networks," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2047-2050, Oct. 2016.
- [8] H. M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285-6298, Dec. 2015.
- [9] W. J. Lin and J. C. Yen, "An integrating channel coding and cryptography design for OFDM based WLANs," *IEEE Int. Symp. Consumer Electronics*, Kyoto, Japan, May 2009, pp. 657-660.
- [10] H. Taha, and E. Alsusa, "A MIMO precoding based physical layer security technique for key exchange encryption," in *proc. IEEE Veh. Technol. Conf.*, Glasgow, Scotland, May 2015, pp. 1-5.
- [11] P. Cao, X. Hu, and J. Wu, "Physical layer encryption in OFDM-PON employing time-variable keys from ONUs," *IEEE Photonics J.*, vol. 6, no. 2, pp. 1-7, April 2014.
- [12] H. Qin, Y. Sun, T. H. Chang, X. Chen, C. Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717-2729, June 2013.
- [13] H. M. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545, July 2012.
- [14] X. Huang, J. Wu, and Y. Wen, "Rate-adaptive feedback with bayesian compressive sensing in multiuser MIMO beamforming systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 1536-1576, July 2016.
- [15] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687-1700, Aug. 2013.
- [16] H. M. Wang, M. Luo, X. G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdroppers CSI," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 39-42, Jan. 2013.
- [17] D. J. R. Chisaguano, Y. Higashino, and T. Hou, "Low-complexity channel estimation and detection for MIMO-OFDM receiver with ESPAR antenna," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8297-8308, Oct. 2016.
- [18] A. E. Shafie, D. Niyato, and N. A. Dahir, "Artificial-noise-aided secure MIMO full-duplex relay channels with fixed-power transmissions," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1591-1594, Aug. 2016.
- [19] D. Lee, "MIMO OFDM channel estimation via block stagewise orthogonal matching pursuit," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2115-2118, Oct. 2016.
- [20] T. Akitaya, S. Asano, and T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," in *proc. IEEE Int. conference on commun. workshops*, Sydney, Australia, Aug. 2014, pp. 807-812.