A Semiblind Two-Way Training Method for Discriminatory Channel Estimation in MIMO Systems

Junjie Yang, Shengli Xie, *Senior Member, IEEE,* Xiangyun Zhou, *Member, IEEE,* Rong Yu, *Member, IEEE,* Yan Zhang, *Senior Member, IEEE*

***Abstract*—Discriminatory channel estimation (DCE) is a recently developed strategy to enlarge the performance difference between a legitimate receiver (LR) and an unauthorized receiver (UR) in a multiple-input multiple-output (MIMO) wireless system. Specifically, it makes use of properly designed training signals to degrade channel estimation at the UR which in turn limits the UR's eavesdropping capability during data transmission. In this paper, we propose a new two-way training scheme for DCE through exploiting a whitening-rotation (WR) based semiblind method. To characterize the performance of DCE, a closed-form expression of the normalized mean squared error (NMSE) of the channel estimation is derived for both the LR and the UR. Furthermore, the developed analytical results on NMSE are utilized to perform optimal power allocation between the training signal and artificial noise (AN). The advantages of our proposed DCE scheme are two folds: 1) compared to the existing DCE scheme based on the linear minimum mean square error (LMMSE) channel estimator, the proposed scheme adopts a semiblind approach and achieves better DCE performance; 2) the proposed scheme is robust against active eavesdropping with the pilot contamination attack, whereas the existing scheme fails under such an attack.**

***Index Terms*—Two-way training, discriminatory channel estimation, semiblind approach, pilot contamination attack**

I. Introduction

Eavesdropping by unauthorized receivers has become a prevalent security threat in wireless communications due to the broadcast nature of the wireless medium. Therefore, discriminating the signal reception performance between a legitimate receiver (LR) and an unauthorized receiver (UR) becomes an important issue in secure communications [1,2]. To address the issue, the concept of physical layer security [3,4] has been introduced which utilizes the physical layer properties of a wireless channel to achieve the desired discriminatory channel performance. From an information-theoretic perspective, the studies in [5-7] showed that the maximal data rate can be achieved by exploiting the difference in the channel conditions between the LR and the UR, while preventing the UR from eavesdropping any information from the received signals. Moreover, [8] investigated the secrecy improvement resulting from frequency selectivity in MIMO-OFDM systems. From a signal processing perspective, various beamforming schemes [9,10] have been developed to enhance the signal reception at the LR whilst limiting the quality of signal at the UR. The beamforming design requires the channel state information (CSI) of the LR and/or the UR priori. The physical layer security can be used in many application senarios [5-7], *e.g.,* the two-way relaying [11-13].

Several studies on physical layer security mainly focus on data transmission without the assumption of perfect CSI. The pilot transmission phase is the period to acquire CSI. It is known that channel estimation performance has a significant effect on data detection. This observation has motivated the development of a new training strategy called discriminatory channel estimation (DCE) such that the channel estimation at the UR is much worse than the channel estimation at the LR. For this, artificial noise (AN) [14-16] is inserted in the training signals to jam the UR while keeping a minimal level of interference to the LR. Chang *et al.* [17] first designed a DCE scheme by employing multiple feedback-and-training processes. This scheme requires large training overhead and high design complexity. Later, a two-way training based DCE scheme was proposed in the study [18] to reduce overhead and hence improve the efficiency of DCE over the original scheme in [17]. The two-way DCE scheme in [18] works well against passive eavesdropping attack from the UR. However, as we will show in this paper, the two-way DCE scheme is not able to achieve the desired performance under an *active* eavesdropping named the pilot contamination attack [19]. The pilot contamination attack makes use of the fixed and publicly known training sequence used by the LR in the reverse training phase in order to influence the channel estimation at the transmitter (TX). Therefore, it is important to design a robust DCE scheme against the pilot contamination attack, which does not require any fixed and known training sequence at the LR.

In this paper, we propose a new two-way training scheme via whitening-rotation (WR) based semiblind approach [20-22]. The proposed scheme includes two phases: 1) the LR transmits a sequence of stochastic signals in the reverse training phase. These signals are only known by the LR itself, facilitating CSI acquisition at the TX; 2) the TX broadcasts a new sequence of pilots inserted by AN in the forward training phase. This will enable the channel estimation at the LR while

J. Yang, S. Xie, R. Yu are with the School of Automation, Guangdong University of Technology, Guangzhou, 510006, China. (e-mail: yangjunjie1985@gmail.com, shlxie@gdut.edu.cn, yurong@gdut.edu.cn)

X. Zhou is with the Research School of Engineering, the Australian National University, Canberra, ACT 0200, Australia. (e-mail: xiangyun.zhou@anu.edu.au).

Y. Zhang is with Simula Research Laboratory, Norway; and also with Department of Informatics, University of Oslo, Norway. (email: yanzhang@simula.no)

disrupting the channel estimation at the UR. With respect to the proposed scheme, we have the following contributions.

- The proposed WR-based DCE scheme achieves a better DCE performance than the existing LMMSE-based DCE scheme in [18]. By combining the blind and training-based algorithms, the WR-based semiblind techniques can potentially enhance the quality of DCE. As shown in our numerical results, the proposed scheme outperforms the existing scheme with the same training overhead.
- Another advantage of the proposed DCE scheme is the provision of a way to protect against the pilot contamination attack due to the randomness feature in the training signal used by the LR. We present an analytical model to demonstrate effective attack protection and show that such attack has a minor impact on the DCE performance.
- Moreover, we analytically evaluate the DCE performance of the proposed scheme by deriving the NMSE of channel estimation at both the LR and the UR. The optimal power allocation between the training signals and the AN is also investigated and an efficient solution is obtained as an one-dimensional line search.

The remainder of this paper is organized as follows. First, the system model and problem description are presented in Section II. The proposed two-way training scheme using the WR-based channel estimator is presented in Section III. The performance analysis under the pilot contamination attack is discussed in Section IV. Next, simulation results are given in Section V, followed by the conclusions in Section VI. Through the paper, we adopt the following notations:

TABLE I
NOTATION LIST IN THIS PAPER

Symbols	Notations
$*$	conjugate
T	transpose
H	complex conjugate transpose
$\circ$	Hadamard product
$Tr(\cdot)$	the trace of a matrix
$\|\| \cdot \|\|_F$	Frobenius norm
$diag(\cdot)$	a stacking of the diagonal elements of the involved matrix into a vector

II. System Model and Problem description

A. System Model

As shown in Fig.1, we consider a wireless MIMO system consisting of a transmitter (TX), a legitimate receiver (LR) and an unauthorized receiver (UR). In the system, the TX, the LR and the UR have N_T, N_L, and N_U antennas ($N_T > N_L$), respectively. The TX is connected to one LR and one UR by means of two different communication channels, namely legitimate channel and wiretap channel. The legitimate channel and the wiretap channel are denoted as $\mathbf{H} \in \mathbb{C}^{N_L \times N_T}$, $\mathbf{G} \in \mathbb{C}^{N_U \times N_T}$, respectively. Besides, the channel from the LR to the UR is denoted as $\mathbf{B} \in \mathbb{C}^{N_U \times N_L}$.

To enable the LR to interpret the legitimate channel, the TX needs to emit a sequence of training pilots, but this also allows the UR to perform wiretap channel estimation. Therefore, the design of pilot signal is required to ensure a high quality channel estimation at the LR but also prevent the UR from estimating the wiretap channel.

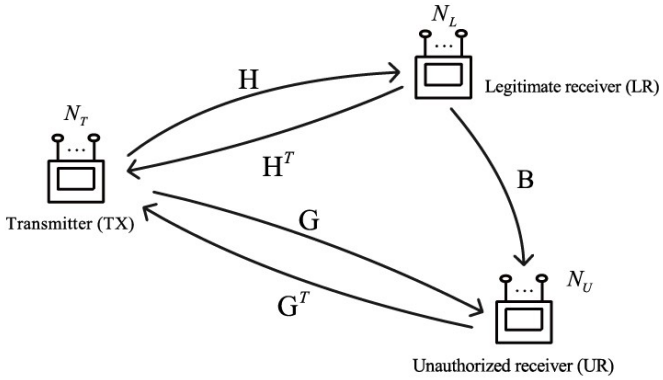


Fig. 1. A wireless MIMO system includes a multi-antennas transmitter (TX), a multi-antennas legitimate receiver (LR) and a multi-antennas unauthorized receiver (UR).

The system model is based on the following assumptions.

1) Channels are assumed to be independently distributed and have reciprocity, *e.g.*, matrix $\mathbf{H}$ represents downlink legitimate channel and $\mathbf{H}^T$ is uplink legitimate channel. Besides, matrices $\mathbf{H}$, $\mathbf{G}$ and $\mathbf{B}$ are assumed to be the Rayleigh flat fading channels.
2) The entries of channel matrices $\mathbf{H}$, $\mathbf{G}$ and $\mathbf{B}$ are assumed to be *i.i.d*, $\mathcal{CN}(0, \sigma^2_{\mathbf{H}})$, $\mathcal{CN}(0, \sigma^2_{\mathbf{G}})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{B}})$, respectively; moreover, the entries of receiver noises are assumed to be the same as independent additive white Gaussian distributed, *i.i.d*, $\mathcal{CN}(0, \sigma^2_0)$.

The reciprocal assumption indicates that the uplink and downlink channel paths are similar, which happens in time-division duplex (TDD) systems [23]. Such assumption is very critical for the two-way training, and this paper mainly focuses on the design of a DCE scheme in a TDD systems; besides, the Rayleigh flat fading channel assumption indicates that channels are relatively fixed over the transmission of symbols in one time slot but change randomly between time slots. For the second assumption of the system, it refers that the conditions of channels and noises are respectively treated as same for the sake of fair performance.

In this paper, two eavesdropping scenarios are taken into account, that is, passive eavesdropping and active eavesdropping (pilot contamination attack [19]). For the first case, the UR only silently receives signals via channels $\mathbf{G}$ and $\mathbf{B}$ during the training phase. For the latter case, the UR not only receives signals but also emits false training pilots from the uplink channel $\mathbf{G}^T$ within the training process. Such pilot contamination attack is a potential threat for the two-way training.

B. The Existing Two-way Training Scheme

The two-way training includes a reverse training phase and a forward training phase. For the reverse training phase, the LR sends a reverse training signal to the TX as

$$\mathbf{S}_0 = \sqrt{\frac{P_0}{N_L} T_0} \mathbf{C_0} \tag{1}$$

where P_0 is the power of the training pilot, and the reverse pilot matrix $\mathbf{C_0} \in \mathbb{C}^{N_\mathbf{L} \times T_1}$ satisfies an orthogonal condition $\mathbf{C_0}\mathbf{C_0^H} = \mathbf{I}_{N_L}$. The received signal at the TX is given by

$$\mathbf{X_0} = \mathbf{H}^T\mathbf{S_0} + \mathbf{E_0}, \tag{2}$$

where $\mathbf{E_0} \in \mathbb{C}^{N_T \times T_0}$ refers to the AWGN matrix. By employing the linear minimum mean-square error (LMMSE) method [24], the channel estimation at the TX is given by

$$\hat{\mathbf{H}}_\mathbf{0} = \sigma_\mathbf{H}^\mathbf{2}(\sigma_\mathbf{H}^\mathbf{2}\mathbf{S_0}\mathbf{S_0^H} + \sigma_\mathbf{0}^\mathbf{2}\mathbf{I}_{N_L})^{-\mathbf{1}}\mathbf{S_0}\mathbf{X_0^H}. \tag{3}$$

In the forward training phase, the TX transmits a sequence of forward training signals inserted with AN to enable channel estimation at the LR while degrading the channel acquisition at the UR. In particular, the AN-aided training sequence, denoted by $\mathbf{S_1}$, has the following expression

$$\mathbf{S_1} \triangleq \sqrt{\frac{P_1}{N_\mathbf{T}}T_1}\mathbf{C_1} + \mathbf{N}_{\hat{\mathbf{H}}_\mathbf{0}}\mathbf{A}, \tag{4}$$

where P_1 denotes the power of forward training pilots, T_1 is the training length, $\mathbf{C_1} \in \mathbb{C}^{N_\mathbf{T} \times T_1}$ represents the forward pilot matrix which satisfies an orthogonal condition $\mathbf{C_1}\mathbf{C_1^H} = \mathbf{I}_{N_T}$. Here, $\mathbf{N}_{\hat{\mathbf{H}}_\mathbf{0}}$ is a matrix whose column vectors form an orthogonal basis for the left null space of $\hat{\mathbf{H}}_\mathbf{0}$, that is, $\mathbf{N}_{\hat{\mathbf{H}}_\mathbf{0}}^H\hat{\mathbf{H}}_\mathbf{0} = \mathbf{0}$ and $\mathbf{N}_{\hat{\mathbf{H}}_\mathbf{0}}^H\mathbf{N}_{\hat{\mathbf{H}}_\mathbf{0}} = \mathbf{I}_{N_T - N_L}$. In addition, $\mathbf{A} \in \mathbb{C}^{(N_T - N_L) \times T_1}$ is the AN matrix with each component being *i.i.d.* $\mathcal{CN}(0, \sigma_a^2)$.

The received signals at the LR and the UR are respectively given by

$$\mathbf{X_1} = \mathbf{H}\mathbf{S_1} + \mathbf{E_1}, \tag{5}$$

$$\mathbf{Y_1} = \mathbf{G}\mathbf{S_1} + \mathbf{F_1}, \tag{6}$$

where $\mathbf{E_1} \in \mathbb{C}^{N_L \times T_1}$ and $\mathbf{F_1} \in \mathbb{C}^{N_U \times T_1}$ are the AWGN matrices. By using the LMMSE, the channel estimation at the LR can be expressed as

$$\hat{\mathbf{H}}_\mathbf{1} = \sigma_\mathbf{H}^\mathbf{2}\{(\sigma_\mathbf{H}^\mathbf{2}\mathbf{S_1}\mathbf{S_1^H} + \sigma_\mathbf{0}^\mathbf{2}\mathbf{I}_{N_T})^{-\mathbf{1}}\mathbf{S_1}\mathbf{X_1^H}\}^T. \tag{7}$$

The UR also makes use of the received signals for its channel estimation in the same manner as (7), but the channel performance at the UR would be restricted due to the AN.

III. Proposed DCE Scheme under Passive Eavesdropping

A. Preliminary of Whitening-Rotation based Channel Estimator

We first give a brief introduction of the WR-based semiblind channel approach [20-22]. The channel matrix $\mathbf{H}^T$ is firstly estimated in the reverse training phase, so we take the decomposition of channel $\mathbf{H}^T$ as an example by

$$\mathbf{H}^T = \mathbf{W}\mathbf{Q}^H, \tag{8}$$

where $\mathbf{W} \in \mathbb{C}^{N_T \times N_L}$ is a whitening matrix and $\mathbf{Q} \in \mathbb{C}^{N_L \times N_L}$ is an unitary rotation matrix, *i.e.*, $\mathbf{Q}^H\mathbf{Q} = \mathbf{Q}\mathbf{Q}^H = \mathbf{I}_{N_L}$. Besides, performing singular value decomposition (SVD) [25] on the channel $\mathbf{H}^T$ gives

$$\mathbf{H}^T = \mathbf{U}_{\mathbf{H}^T}\mathbf{\Sigma}_{\mathbf{H}^T}\mathbf{V}_{\mathbf{H}^T}^H, \tag{9}$$

where $\mathbf{diag}(\mathbf{\Sigma_H}) = [\xi_\mathbf{1}, ..., \xi_{N_L}]^T$. One possible choice of $\mathbf{W}$ and $\mathbf{Q}$ can be $\mathbf{U}_{\mathbf{H}^T}\mathbf{\Sigma}_{\mathbf{H}^T}$ and $\mathbf{V}_{\mathbf{H}^T}$, respectively. Without loss of generality, the channel estimation can be divided into two steps with the WR-based semiblind method:

1) Estimate the whitening matrix $\mathbf{W}$ in a blind fashion using the autocorrelation matrix of the received signals along with a subspace based method.
2) Estimate the unitary rotation matrix $\mathbf{Q}$ using the training pilots with the constrained maximum likelihood (ML)-based method.

The two-steps of the WR-based channel estimator provides a new training design for improving the DCE performance. Specifically, the WR-based semiblind method can be used for the channel estimation both at the LR and the UR during the two-way training.

B. Our Proposed WR-based DCE Scheme

1) Step I. reverse training phase: The LR sends the reverse training signals to the TX for the uplink channel estimation without benefiting the channel estimation process at the UR. In the proposed scheme, the design of reverse training signals has the same expression of (1). Different from the existing two-way training, these reverse training signals are randomly generated at the LR and only known by itself, therefore, the TX can not apply the LMMSE method for the channel estimation.

Here, the TX can resort to the blind part of the WR-based semiblind method for the partial acquisition of channel $\mathbf{H}^T$. Specifically, we estimate the whitening matrix of $\mathbf{H}^T$ by performing SVD on the autocorrelation matrix of the received signals, which has the following form

$$\mathbf{R}_{\mathbf{X_0}} \triangleq \frac{\mathbf{X_0}\mathbf{X_0^H}}{\frac{P_0}{N_L}T_\mathbf{0}}. \tag{10}$$

Referring to (10), we can estimate the whitening matrix of $\mathbf{H}^T$ as

$$\hat{\mathbf{W}}_\mathbf{0} = \frac{\mathbf{1}}{\sqrt{P_\mathbf{0}}}\mathbf{U}_{\mathbf{X_0}}\mathbf{\Sigma}_{\mathbf{X_0}}^{\frac{\mathbf{1}}{\mathbf{2}}} \tag{11}$$

by performing SVD on $\mathbf{R}_{\mathbf{X_0}}$. By using (2) , the autocorrelation matrix $\mathbf{R}_{\mathbf{X_0}}$ can be expressed by

$$\mathbf{R}_{\mathbf{X_0}} = \mathbf{H}^T\mathbf{H}^* + \mathbf{\Delta R}_{\mathbf{X_0}}. \tag{12}$$

From (12), the error of $\mathbf{R}_{\mathbf{X_0}}$ has the following form

$$\mathbf{\Delta R}_{\mathbf{X_0}} = \frac{N_L}{P_\mathbf{0}}(\mathbf{H}^T\mathbf{\Delta R}_{\mathbf{S_0},\mathbf{E_0}} + \mathbf{\Delta R}_{\mathbf{S_0},\mathbf{E_0}}^H\mathbf{H}^* + \mathbf{\Delta R}_{\mathbf{E_0},\mathbf{E_0}}), \tag{13}$$

where the cross correlation matrices $\mathbf{\Delta R}_{\mathbf{S_0},\mathbf{E_0}}$,$\mathbf{\Delta R}_{\mathbf{E_0},\mathbf{E_0}}$ are defined as follows, respectively

$$\mathbf{\Delta R}_{\mathbf{S_0},\mathbf{E_0}} \triangleq \frac{\mathbf{S_0}\mathbf{E_0^H}}{T_\mathbf{0}},$$

$$\mathbf{\Delta R}_{\mathbf{E_0},\mathbf{E_0}} \triangleq \frac{\mathbf{E_0}\mathbf{E_0^H}}{T_\mathbf{0}}.$$

Considering the noise interference, the error of the estimated $\hat{\mathbf{W}}_\mathbf{0}$ can be defined as

$$\mathbf{\Delta W_0} \triangleq \hat{\mathbf{W}}_\mathbf{0} - \mathbf{W}. \tag{14}$$

By using the results of (8) and (13), $\mathbf{\Delta W_0}$ can be deduced as

$$\mathbf{\Delta W_0} = \frac{N_L}{P_0}\mathbf{\Delta R}^H_{\mathbf{S_0},\mathbf{E_0}}\mathbf{Q}. \tag{15}$$

2) Step II. forward training phase: For the forward training phase, the design of forward training sequence is required to enable the LR to interpret the downlink channel information but degrade the channel performance at the UR. Here, the new forward training signal is given by

$$\mathbf{S_1} \triangleq \sqrt{\frac{P_1}{N_T}T_1}\mathbf{C_1} + \mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}}\mathbf{A}, \tag{16}$$

where $\mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}} \in \mathbb{C}^{N_L \times (N_T - N_L)}$ is the orthogonal complement space matrix of $\hat{\mathbf{W}}_\mathbf{0}$ satisfying $\mathbf{N}^H_{\hat{\mathbf{W}}_\mathbf{0}}\hat{\mathbf{W}}_\mathbf{0} = \mathbf{0}$ and $\mathbf{N}^H_{\hat{\mathbf{W}}_\mathbf{0}}\mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}} = \mathbf{I}_{N_T - N_L}$. Compared to (4), (16) utilizes the left null space of $\hat{\mathbf{W}}_\mathbf{0}$ instead of $\hat{\mathbf{H}}^T_\mathbf{0}$ for the generation of AN. In fact, the left null spaces to the matrices $\hat{\mathbf{W}}_\mathbf{0}$ and $\hat{\mathbf{H}}^T_\mathbf{0}$ are same because the matrix $\hat{\mathbf{W}}_\mathbf{0}$ has all the eigenvalues of $\hat{\mathbf{H}}^T_\mathbf{0}$. We denote the first term of (16) as

$$\tilde{\mathbf{S}}_\mathbf{1} = \sqrt{\frac{P_1}{N_T}T_1}\mathbf{C_1}.$$

The LR may suffer from the the imperfect estimation of $\mathbf{W_0}$ due to the interference of AN, thus the power allocation problem between P_1 and σ_a^2 needs to be allocated carefully.

2.1) ***Channel estimation at the LR*:** Using (5) and (16), the received signal matrix at the LR can be rewritten as follows

$$\mathbf{LR}: \mathbf{X_1} = \mathbf{H}\tilde{\mathbf{S}}_\mathbf{1} + \tilde{\mathbf{E}}_\mathbf{1}, \tag{17}$$

where

$$\tilde{\mathbf{E}}_\mathbf{1} \triangleq \mathbf{H}\mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}}\mathbf{A} + \mathbf{E_1}.$$

We apply the WR-based semiblind channel estimator for the channel estimation at the LR. First, the whitening matrix of $\mathbf{H}$ can be estimated as

$$\hat{\mathbf{W}}_\mathbf{1} = \mathbf{V}^*_{\hat{\mathbf{X}}_\mathbf{W}}\mathbf{\Sigma}^T_{\hat{\mathbf{X}}_\mathbf{W}} \tag{18}$$

by performing SVD on the matrix

$$\hat{\mathbf{X}}_\mathbf{W} \triangleq \frac{\mathbf{X_1}\tilde{\mathbf{S}}^H_\mathbf{1}}{\frac{P_1}{N_T}T_1}, \tag{19}$$

where

$$\hat{\mathbf{X}}_\mathbf{W} = \mathbf{U}_{\hat{\mathbf{X}}_\mathbf{W}}\mathbf{\Sigma}_{\hat{\mathbf{X}}_\mathbf{W}}\mathbf{V}^H_{\hat{\mathbf{X}}_\mathbf{W}}.$$

After that, the unitary rotation matrix of $\mathbf{H}$ can be obtained by solving the following optimization problem under the perturbation-free case,

$$\begin{aligned} LR: \quad & min(\mathbf{Q}) = \sum_{i=1}^{N_L} \parallel \mathbf{X_1}(i) - \sum_{j=1}^{N_T} \hat{\sigma}_j q^*_{ij}\hat{\mathbf{S}}_\mathbf{1}(j) \parallel^2_F \\ \mathbf{s.t.} \quad & \mathbf{Q}\mathbf{Q}^H = \mathbf{I}_{N_L}, \end{aligned} \tag{20}$$

where $\hat{\mathbf{S}}_\mathbf{1} = \mathbf{V}^H_{\hat{\mathbf{X}}_\mathbf{W}}\tilde{\mathbf{S}}_\mathbf{1}$, $\mathbf{X_1}(i)$ represents the ith column of $\mathbf{X_1}$ and $\hat{\mathbf{S}}_\mathbf{1}(j)$ refers to the jth column of $\hat{\mathbf{S}}_\mathbf{1}$, respectively. By using the Lagrange method (the derivation can be found in appendix A), the unitary rotation matrix can be calculated as follows

$$\hat{\mathbf{Q}}_\mathbf{1} = \mathbf{U}_{\hat{\mathbf{X}}_\mathbf{Q}}\mathbf{V}^H_{\hat{\mathbf{X}}_\mathbf{Q}} \tag{21}$$

by performing SVD on the matrix

$$\hat{\mathbf{X}}_\mathbf{Q} \triangleq \frac{\mathbf{X}^*_\mathbf{1}\tilde{\mathbf{S}}^T_\mathbf{1}\hat{\mathbf{W}}_\mathbf{1}}{\frac{P_1}{N_T}T_1}, \tag{22}$$

where

$$\hat{\mathbf{X}}_\mathbf{Q} = \mathbf{U}_{\hat{\mathbf{X}}_\mathbf{Q}}\mathbf{\Sigma}_{\hat{\mathbf{X}}_\mathbf{Q}}\mathbf{V}^H_{\hat{\mathbf{X}}_\mathbf{Q}}.$$

According to (8), the legitimate channel $\mathbf{H}$ can be calculated by $\hat{\mathbf{H}}_\mathbf{1} = \hat{\mathbf{Q}}^*_\mathbf{1}\hat{\mathbf{W}}^T_\mathbf{1}$.

2.2) ***Channel estimation at UR*:** Likewise, the wiretape channel $\mathbf{G}$ can be decomposed as

$$\mathbf{G} = \mathbf{M}\mathbf{R}^H, \tag{23}$$

where $\mathbf{M} \in \mathbb{C}^{N_U \times N_T}$ is the whitening matrix, and $\mathbf{R} \in \mathbb{C}^{N_T \times N_T}$ is the unitary rotation matrix. Besides, $\mathbf{G}$ can be decomposed by SVD as follows

$$\mathbf{G} = \mathbf{U}_\mathbf{G}\mathbf{\Sigma}_\mathbf{G}\mathbf{V}^H_\mathbf{G}, \tag{24}$$

where $\mathbf{diag}(\mathbf{\Sigma_G}) = [\gamma_\mathbf{1}, ..., \gamma_{N_U}]^T$. Without loss of generality, we can assume that $\mathbf{M} = \mathbf{U_G}\mathbf{\Sigma_G}$ and $\mathbf{R} = \mathbf{V_G}$.

When the UR employs the WR-based semiblind channel estimator for its channel estimation, the received signal matrix of (6) can be rewritten as follows

$$\mathbf{UR}: \mathbf{Y_1} = \mathbf{G}\tilde{\mathbf{S}}_\mathbf{1} + \tilde{\mathbf{F}}_\mathbf{1}, \tag{25}$$

where $\tilde{\mathbf{F}}_\mathbf{1} \triangleq \mathbf{G}\mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}}\mathbf{A} + \mathbf{F_1}$. Then, the whitening matrix of $\mathbf{G}$ can be obtained as

$$\hat{\mathbf{M}} = \mathbf{U}_{\hat{\mathbf{Y}}_\mathbf{M}}\mathbf{\Sigma}_{\hat{\mathbf{Y}}_\mathbf{M}} \tag{26}$$

by performing SVD to the matrix

$$\hat{\mathbf{Y}}_\mathbf{M} \triangleq \frac{\mathbf{Y_1}\tilde{\mathbf{S}}^H_\mathbf{1}}{\frac{P_1}{N_T}T_1}, \tag{27}$$

where

$$\hat{\mathbf{Y}}_\mathbf{M} = \mathbf{U}_{\hat{\mathbf{Y}}_\mathbf{M}}\mathbf{\Sigma}_{\hat{\mathbf{Y}}_\mathbf{M}}\mathbf{V}^H_{\hat{\mathbf{Y}}_\mathbf{M}}.$$

Next, the rotation matrix of $\mathbf{G}$ can be calculated using the training-based method [22],

$$\hat{\mathbf{R}} = \mathbf{V}_{\hat{\mathbf{Y}}_\mathbf{R}}\mathbf{U}^H_{\hat{\mathbf{Y}}_\mathbf{R}} \tag{28}$$

by performing SVD to the matrix

$$\hat{\mathbf{Y}}_\mathbf{R} \triangleq \frac{\hat{\mathbf{M}}^H\mathbf{Y_1}\tilde{\mathbf{S}}^H_\mathbf{1}}{\frac{P_1}{N_T}T_1}, \tag{29}$$

where

$$\hat{\mathbf{Y}}_\mathbf{R} = \mathbf{U}_{\hat{\mathbf{Y}}_\mathbf{R}}\mathbf{\Sigma}_{\hat{\mathbf{Y}}_\mathbf{R}}\mathbf{V}^H_{\hat{\mathbf{Y}}_\mathbf{R}}.$$

Using (26) and (28), the wiretap channel $\mathbf{G}$ can be calculated by $\hat{\mathbf{G}} = \hat{\mathbf{M}}\hat{\mathbf{R}}^H$.

C. DCE Performance Analysis

We mainly discuss the DCE performance in this Section. A quantitative analysis of power allocation is offered for the optimal DCE scheme.

1) Channel estimation performance at the LR: To analyze channel estimation performance, we define the perturbation errors of $\hat{\mathbf{W}}_\mathbf{1}$ and $\hat{\mathbf{Q}}_\mathbf{1}$, *i.e.*, $\mathbf{\Delta W_1} \triangleq \hat{\mathbf{W}}_\mathbf{1} - \mathbf{W}$ and $\mathbf{\Delta Q_1} \triangleq \hat{\mathbf{Q}}_\mathbf{1} - \mathbf{Q}$. The estimation error of $\mathbf{H}$ at the LR is given by

$$\mathbf{\Delta H_1} \triangleq \hat{\mathbf{H}}_\mathbf{1} - \mathbf{H} = \hat{\mathbf{Q}}^* \hat{\mathbf{W}}_\mathbf{1}^T - \mathbf{Q}^* \mathbf{W}_\mathbf{1}^T \approx \mathbf{Q}^* \mathbf{\Delta W}_\mathbf{1}^T + \mathbf{\Delta Q}_\mathbf{1}^* \mathbf{W}^T. \tag{30}$$

First, we derive the closed-form expression of $\mathbf{\Delta W_1}$. Similar to (15), $\mathbf{\Delta W_1}$ has the following expression

$$\mathbf{\Delta W_1} = \frac{N_T}{P_\mathbf{1}} \mathbf{Q}^T \mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}}, \tag{31}$$

where

$$\mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}} = \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{E}_\mathbf{1}} + \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} \mathbf{N}^H_{\hat{\mathbf{W}}_\mathbf{0}} \mathbf{H}^H.$$

Notice that $\mathbf{N}^T_{\hat{\mathbf{W}}_\mathbf{0}} \hat{\mathbf{W}}_\mathbf{0} = \mathbf{0}$, (31) can be rewritten as

$$\mathbf{\Delta W_1} = \frac{N_T}{P_\mathbf{1}} \mathbf{Q}^T (\mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{E}_\mathbf{1}} - \frac{\mathbf{1}}{P_\mathbf{0}} \mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} \mathbf{N}^T_{\hat{\mathbf{W}}_\mathbf{0}} \mathbf{\Delta R}^H_{\mathbf{S}_\mathbf{0}, \mathbf{E}_\mathbf{0}}). \tag{32}$$

Next, we deduce the closed-form expression of $\mathbf{\Delta Q_1}$. Using the result of [22], $\mathbf{\Delta Q_1}$ equals to

$$\mathbf{\Delta Q_1} \approx \mathbf{Q} (\mathbf{\Gamma_Q} \circ \mathbf{\Pi_Q})^H, \tag{33}$$

where

$$\mathbf{\Gamma_Q} = \begin{bmatrix} \frac{1}{2\xi_1^2}, & \cdots & , \frac{1}{\xi_1^2 + \xi_{N_L}^2} \\ \frac{1}{\xi_2^2 + \xi_1^2}, & \cdots & , \frac{1}{\xi_2^2 + \xi_{N_L}^2} \\ & .... & \\ \frac{1}{\xi_{N_L}^2 + \xi_1^2}, & \cdots & , \frac{1}{2\xi_{N_L}^2} \end{bmatrix} \tag{34}$$

and

$$\mathbf{\Pi_Q} = \mathbf{\Delta X}^H_\mathbf{Q} \mathbf{Q} - \mathbf{Q}^H \mathbf{\Delta X_Q}. \tag{35}$$

To derive the perturbation error of $\mathbf{\Delta X_Q}$, we define $\hat{\mathbf{X}}_\mathbf{Q} \triangleq \mathbf{X_Q} + \mathbf{\Delta X_Q}$. Using (5), (22) can be modified as

$$\hat{\mathbf{X}}_\mathbf{Q} = \mathbf{H}^* \mathbf{W} + \mathbf{H}^* \mathbf{\Delta W_1} + \frac{N_T}{P_\mathbf{1}} \mathbf{\Delta R}^T_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}} \mathbf{W}. \tag{36}$$

Therefore, we have

$$\mathbf{\Delta X_Q} = \mathbf{H}^* \mathbf{\Delta W_1} + \frac{N_T}{P_\mathbf{1}} \mathbf{\Delta R}^T_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}} \mathbf{W}. \tag{37}$$

Substituting (37) into (35) , we have

$$\mathbf{\Pi_Q} = \mathbf{0}. \tag{38}$$

As a result, (33) can be summarized as $\mathbf{\Delta Q_1} = \mathbf{0}$, and the perturbation error of $\hat{\mathbf{H}}_\mathbf{1}$ is given by

$$\mathbf{\Delta H_1} = \frac{P_\mathbf{1}}{N_T} (\mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{E}_\mathbf{1}} - \frac{N_L}{P_\mathbf{0}} \mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} \mathbf{N}^T_{\hat{\mathbf{W}}_\mathbf{0}} \mathbf{\Delta R}^H_{\mathbf{S}_\mathbf{0}, \mathbf{E}_\mathbf{0}}). \tag{39}$$

Similar to the derivation of [22], the NMSE criterion like [24] of the estimated matrix $\mathbf{H}$ at the LR is given by

$$\begin{aligned} \mathbf{NMSE}_L &\triangleq \frac{\mathrm{Tr}(\mathrm{E}\{\mathbf{\Delta H_1} \mathbf{\Delta H}^H_\mathbf{1}\})}{N_L N_T} \\ &= \frac{N_T \sigma_0^2}{P_1 T_1} + \frac{N_L (N_T - N_L) \sigma_a^2}{P_0 T_0} \frac{N_T \sigma_0^2}{P_1 T_1}. \end{aligned} \tag{40}$$

2) Channel estimation performance at the UR: We define the perturbation errors of $\hat{\mathbf{M}}$ and $\hat{\mathbf{R}}$, *i.e.*, $\mathbf{\Delta M} \triangleq \hat{\mathbf{M}} - \mathbf{M}$ and $\mathbf{\Delta R} \triangleq \hat{\mathbf{R}} - \mathbf{R}$. In the following, the estimation error of channel $\mathbf{G}$ can be given by

$$\mathbf{\Delta G} \triangleq \hat{\mathbf{G}} - \mathbf{G} = \hat{\mathbf{M}} \hat{\mathbf{R}}^H - \mathbf{M} \mathbf{R}^H \approx \mathbf{M} \mathbf{\Delta R}^H + \mathbf{\Delta M} \mathbf{R}^H. \tag{41}$$

First, we derive the closed-form expression of $\mathbf{\Delta M}$. Similar to (15), $\mathbf{\Delta M}$ has the following expression

$$\mathbf{\Delta M} = \frac{N_T}{P_\mathbf{1}} \mathbf{\Delta R}^H_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{F}}_\mathbf{1}} \mathbf{R}, \tag{42}$$

where

$$\mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{F}}_\mathbf{1}} \triangleq \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} \mathbf{N}^H_{\hat{\mathbf{W}}_\mathbf{0}} \mathbf{G}^H + \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{F}_\mathbf{1}}.$$

Next, we deduce the closed-form expression of $\mathbf{\Delta R}$. Similar to (33), the perturbation matrix of $\hat{\mathbf{R}}$ is given by

$$\mathbf{\Delta R} \approx \mathbf{R} (\mathbf{\Gamma_R} \circ \mathbf{\Pi_R}), \tag{43}$$

where $\mathbf{\Gamma_R}$ is

$$\mathbf{\Gamma_R} = \begin{bmatrix} \frac{1}{2\gamma_1^2}, & \cdots & , \frac{1}{\gamma_1^2 + \gamma_{N_U}^2} \\ \frac{1}{\gamma_2^2 + \gamma_1^2}, & \cdots & , \frac{1}{\gamma_2^2 + \gamma_{N_U}^2} \\ & .... & \\ \frac{1}{\gamma_{N_U}^2 + \gamma_1^2}, & \cdots & , \frac{1}{2\gamma_{N_U}^2} \end{bmatrix} \tag{44}$$

and

$$\mathbf{\Pi_R} = \mathbf{R}^H \mathbf{\Delta Y}^H_\mathbf{R} - \mathbf{\Delta Y_R R}. \tag{45}$$

To derive the perturbation error matrix $\mathbf{\Delta Y_R}$, we define $\hat{\mathbf{Y}}_\mathbf{R} \triangleq \mathbf{Y_R} + \mathbf{\Delta Y_R}$. Using (6), (29) can be approximately by

$$\hat{\mathbf{Y}}_\mathbf{R} \approx \mathbf{M}^H \mathbf{G} + \mathbf{\Delta M}^H \mathbf{G} + \frac{N_\mathbf{T}}{P_\mathbf{1}} \mathbf{M}^H \mathbf{\Delta R}^H_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{F}}_\mathbf{1}}, \tag{46}$$

Therefore,

$$\mathbf{\Delta Y_R} = \mathbf{\Delta M}^H \mathbf{G} + \frac{N_T}{P_\mathbf{1}} \mathbf{M}^H \mathbf{\Delta R}^H_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{F}}_\mathbf{1}}. \tag{47}$$

Substituting (47) into (45), we have $\mathbf{\Pi_R} = \mathbf{0}$. As a result, (43) can be summarized as $\mathbf{\Delta R} = \mathbf{0}$. Then, the perturbation matrix of $\hat{\mathbf{G}}$ can be yielded as

$$\mathbf{\Delta G} = \frac{N_T}{P_\mathbf{1}} (\mathbf{G} \mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}} \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} + \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{F}_\mathbf{1}}). \tag{48}$$

In consequence, the NMSE criterion of estimated $\mathbf{G}$ at the UR can be derived by

$$\begin{aligned} \mathbf{NMSE}_U &\triangleq \frac{\mathrm{Tr}(\mathrm{E}\{\mathbf{\Delta G} \mathbf{\Delta G}^H\})}{N_T N_U} \\ &= \frac{N_T \sigma_0^2 + N_T (N_T - N_L) \sigma_a^2 \sigma_G^2}{P_1 T_1}. \end{aligned} \tag{49}$$

Comparing (40) and (49), we find that the NMSE performance at the LR and the UR are mainly relevant to the selection of power values among the training pilots and AN. When the power of training pilots becomes stronger, the precision of the channel estimation is higher for the LR but lower for the UR. Alternatively, the estimation precision is lower for the LR while higher for the UR when the power of training pilots becomes lower. Therefore, a power allocation trade-off exists between the training pilots and AN.

3) Optimal Power Allocation between the Training Pilots and AN: One needs to allocate the available power between the training pilots and the AN carefully through minimizing the channel estimation error at the LR while restricting the estimation error at the UR. We formulate the power allocation as the following optimization problem

$$\min_{P_0,P_1>0,\sigma_a^2\geqslant 0} \mathbf{NMSE}_L \tag{50}$$

$$s.t. \quad \mathbf{NMSE}_U \geq \gamma, \tag{50a}$$

$$P_0 \leq P_{ave} \tag{50b}$$

$$P_1 + (N_T - N_L)\sigma_a^2 \leq P_{ave}, \tag{50c}$$

where $\gamma > 0$ refers to the threshold of the UR's achievable NMSE, and P_{ave} is the total energy constraint of the training signal. We define $x = \frac{P_1 T_1}{N_T}, y = (N_T - N_L)\sigma_a^2, z = P_0$. Then, the problem (50) can be reformulated as

$$\min_{x>0,y\geq 0} \frac{\sigma_0^2}{x} + \frac{yN_L\sigma_0^2}{xz} \tag{51}$$

$$s.t. \quad \frac{\sigma_0^2}{x} + \frac{y\sigma_G^2}{x} \geq \gamma, \tag{51a}$$

$$z \leq P_{ave}, \tag{51b}$$

$$\frac{xN_T}{T_1} + y \leq P_{ave}. \tag{51c}$$

The problem (51) is a convex optimization problem involving three variables (x, y, z). We will prove that the three-dimensional optimization problem can be solved by a simple one-dimensional line search [26]. (The proof can be found in the Appendix B.)

- ***Proposition 1.*** *Let $\{x^*, y^*, z^*\}$ be the optimal solution to the convex optimization problem in (51) with the constraint that $\frac{N_T\sigma_0^2}{P_{ave}T_1} \leq \gamma \leq (N_T - N_L)P_{ave}$. The optimal value of x can be solved by the following one-dimensional optimization problem*

$$\min_{x} \quad \frac{\sigma_0^2}{x} + \frac{y(x)N_L\sigma_0^2}{xz} \tag{52}$$

$$s.t. \quad \frac{\sigma_0^2}{\gamma} \leq x \leq \frac{(\sigma_G^2 P_{ave} + \sigma_0^2)T_1}{\gamma T_1 + N_T\sigma_G^2}, \tag{52a}$$

where

$$y(x^*) = \frac{x\gamma - \sigma_0^2}{\sigma_G^2},$$
$$z^* = P_{ave}.$$

The associated values of y^*,z^* are given by $y(x^*)$, P_{ave}, respectively.

With the result of Proposition 1, we can construct well designed training sequences for achieving optimal DCE performance.

IV. Proposed DCE Scheme under the Pilot Contamination Attack

In this Section, we analyze the performance of our proposed DCE scheme under the pilot contamination attack.

A. The Existing Pilot Contamination Attack

Under the existing two-way training scheme, the pilot contamination attack is possible when the reverse training pilots are known by the UR. Notice that the publicly known reverse training pilots provide an opportunity for the UR to make an adverse influence on the channel estimation at the TX. In particular, the UR sends the reverse training pilots at the same time as the LR's transmission during the reverse training phase. With the additive AWGN matrix $\mathbf{F_0} \in \mathbb{C}^{N_T \times T_0}$, the received signals at the TX are given by

$$\mathbf{X_0} = \mathbf{H}^T\mathbf{S_0} + \mathbf{E_0} + \mathbf{G}^T\bar{\mathbf{S}}_\mathbf{0} + \mathbf{F_0}, \tag{53}$$

where

$$\bar{\mathbf{S}}_\mathbf{0} = \sqrt{\frac{\bar{P}_\mathbf{0}}{N_L} T_\mathbf{0}}\bar{\mathbf{C}}_\mathbf{0},$$

$\bar{P}_0$ is the power of injected fake pilot and pilot matrix $\bar{C}_0$ satisfies that $\bar{\mathbf{C}}_\mathbf{0}\bar{\mathbf{C}}_\mathbf{0}^H = \mathbf{I}_{N_L}$. If the UR knows the reverse training pilot, then $\bar{P}_0 = P_0$ and $\bar{C}_0 = C_0$. For simplicity, we define the injected noises of (53) as

$$\bar{\mathbf{F}}_0 \triangleq \mathbf{G}^T\bar{\mathbf{S}}_\mathbf{0} + \mathbf{F_0}. \tag{54}$$

The pilot contamination attack can be viewed as a form of malicious signal injection. With the injection of false training pilot, the UR can degrade the TX's estimation of uplink channel $\mathbf{H}^T$ and also align the wiretap channel estimation for the UR. In conclusion, the impact of the pilot contamination attack on the two-way DCE scheme has two folds: it reduces the accuracy of the LR's estimation of the downlink channel due to the leakage of AN; and more seriously it increases the UR's channel performance.

B. The Impact of Pilot Contamination Attack on the Proposed Scheme

For our proposed two-way training, the reverse training pilots are randomly generated at the LR and only known by itself. Therefore, the randomness feature of the reverse training pilots provides a natural way of protecting against the pilot contamination attack. Possibly, the UR may try to exploit the received signals from channel $\mathbf{B}$ via the blind detection methods [27,28]. However, the UR would suffer from a rotation ambiguity between the estimated channel $\hat{\mathbf{B}}$ and channel $\mathbf{B}$. Therefore, it is still no use for the UR to interpret the reverse training pilot without the cooperation of the LR.

Here, we consider a scenario when the UR performs pilot contamination attack with a guessing-based way, that is, the pilots $\bar{\mathbf{C}}_\mathbf{0}$ is randomly generated by a guess way. We employ the WR-based semiblind channel estimator for the DCE performance. In order to study such attack, we mainly focus on its impact on the NMSE performance of the estimated channel $\hat{\mathbf{H}}_\mathbf{1}$ at the LR. By using (31), the perturbation error of the

whitening matrix to the estimated channel $\hat{\mathbf{H}}_\mathbf{1}$ can be rewritten as

$$\mathbf{\Delta W_1} = \frac{N_T}{P_\mathbf{1}} \mathbf{Q}^T \mathbf{\Delta R}^*_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}}, \tag{55}$$

where

$$\mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \tilde{\mathbf{E}}_\mathbf{1}} \approx$$
$$\mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{E}_\mathbf{1}} - \frac{N_L}{P_\mathbf{0}} \mathbf{\Delta R}_{\tilde{\mathbf{S}}_\mathbf{1}, \mathbf{A}} \mathbf{N}^H_{\hat{\mathbf{W}}_\mathbf{0}} (\mathbf{\Delta R}^T_{\mathbf{S_0}, \mathbf{E_0}} + \mathbf{\Delta R}^T_{\mathbf{S_0}, \bar{\mathbf{F}}_\mathbf{0}}).$$

Similar to (33), the perturbation error of the unitary rotation matrix can be deduced as $\mathbf{\Delta Q_1} = \mathbf{0}$. Hence, the perturbation error of the estimated channel $\hat{\mathbf{H}}_\mathbf{1}$ is given by

$$\mathbf{\Delta H_1} = \frac{P_1}{N_T} \{\Delta R^*_{\tilde{S}_1, E_1} - \frac{N_L}{P_0} \Delta R^*_{\tilde{S}_1, A} N^T_{\hat{W}_0} (\Delta R^H_{S_0, E_0} + \Delta R^H_{S_0, \bar{F}_0})\}. \tag{56}$$

With the result of (56), the NMSE criterion of the estimated channel $\mathbf{H_1}$ at the LR is given by

$$\begin{aligned} \mathbf{NMSE}_L \approx & \frac{N_T \sigma^2_\mathbf{0}}{P_\mathbf{1} T_\mathbf{1}} + \frac{N_L (N_T - N_L) \sigma^2_a}{P_\mathbf{0} T_\mathbf{0}} \frac{N_T \sigma^2_\mathbf{0}}{P_\mathbf{1} T_\mathbf{1}} \\ & + \frac{N_L (N_T - N_L) \sigma^2_a}{P_1 T_1} (\frac{N_T \sigma^2_0}{\bar{P}_0 T_0} + \frac{N_U \sigma^2_G}{P_0 T_0}). \end{aligned} \tag{57}$$

When we compare (57) and (40), the third term of (57) is newly introduced due to the injection of fake training pilot. The third term is significantly smaller than the first of two terms. Therefore, the pilot contamination attack only marginally increases the NMSE error at the LR. Furthermore, (57) demonstrates that the power allocation using Proposition 1 is still valid under the pilot contamination attack.

V. Numerical results

We consider a MIMO wireless system with one LR and one UR. In the system, we have $N_T = 4, N_L = 2$ and $N_U = 2$. Channel matrices $\mathbf{H}$ or $\mathbf{G}$ are *i.i.d.* complex Gaussian random variables with zero mean and unit variance ($\sigma^\mathbf{2}_\mathbf{H} = \sigma^\mathbf{2}_\mathbf{G} = \mathbf{1}$); and the additive noise matrices $\mathbf{E_0}$, $\mathbf{E_1}$ or $\mathbf{F_1}$ are *i.i.d.* AWGN ($\sigma^2_0 = 0.01$). We set the maximum transmission power as 30 dBm, *i.e.,* $P_{ave} = 1$. The reverse training pilot matrix and the forward pilot matrix satisfy that $\mathbf{C_0 C^H_0} = \mathbf{I}_{N_L}$, $\mathbf{C_1 C^H_1} = \mathbf{I}_{N_T}$, respectively. Moreover, the overall training length is given as $T = 280$, in which $T_0 = T_1 = 140$. The parameter γ is set as 0.03 or 0.1 [17]. With $P_{ave} = 1$, the criterion of signal-to-noise ratios (SNRs) at the LR and the UR can be defined as

$$\begin{aligned} \mathbf{SNR}_L &= \frac{\mathrm{E}\| \mathbf{HS_1} \|^\mathbf{2}_F}{\mathrm{E}\| \mathbf{E_1} \|^\mathbf{2}_F} = \frac{\mathbf{1}}{\sigma^\mathbf{2}_\mathbf{0}}, \\ \mathbf{SNR}_U &= \frac{\mathrm{E}\| \mathbf{GS_1} \|^\mathbf{2}_F}{\mathrm{E}\| \mathbf{F_1} \|^\mathbf{2}_F} = \frac{\mathbf{1}}{\sigma^\mathbf{2}_\mathbf{0}}, \end{aligned} \tag{58}$$

where $\mathbf{SNR}_L = \mathbf{SNR}_U$. Here, the DCE scheme based on the LMMSE channel estimator in [18] is employed as a fair comparison to the proposed DCE scheme based on the WR channel estimator. In the following, the scheme in [18] is called as LMMSE-based DCE scheme, and the proposed scheme is named as WR-based DCE scheme. The result of each DCE scheme is obtained over 100,000 Monte Carlo running. We first demonstrate the efficiency of the proposed DCE scheme. Both the LR and the UR exploit their channel estimation with the received signal samples. The optimal power value among P_1 and σ^2_a can be calculated via the optimized solution of (52). Fig.2 shows that more power is needed for the forward training pilots than the AN at all SNR levels. There is a minor variation between the powers of forward training pilots and the AN at all SNR levels. This observation indicates that the power allocation solution has a stable performance.

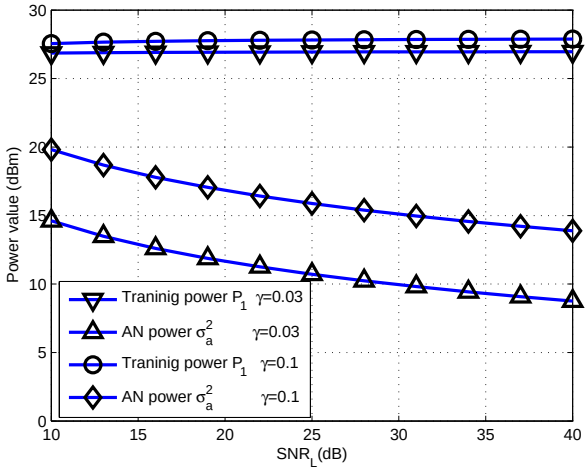
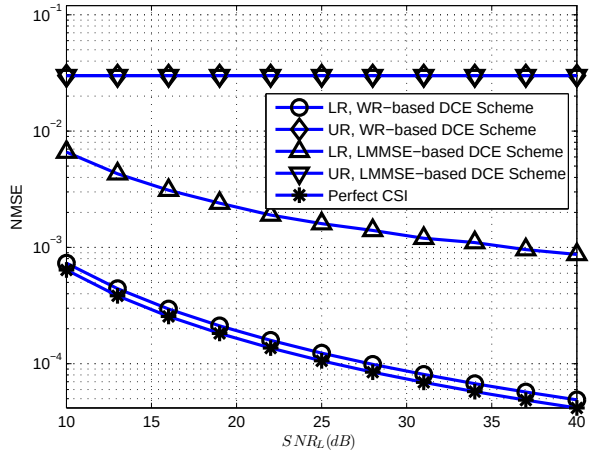


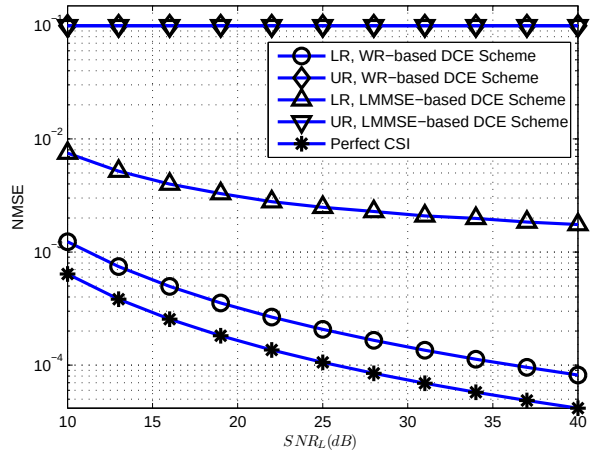
Fig. 2. Power allocation among the training signals and AN in our proposed DCE scheme

From Fig.3 (a) and Fig.3 (b), it is found that the NMSE performance at the LR with the WR-based DCE scheme achieves better DCE performance than the LMMSE-based DCE scheme. By assuming that the TX knows perfect CSI of the uplink channel, we illustrate the ideal lower bound of NMSE with the proposed DCE scheme in the figures. The gap between the ideal lower bound with perfect CSI and the NMSE error at the LR with the LMMSE-based DCE scheme is wide while it is very close to the WR-based DCE scheme. Furthermore, Fig 3.(c) shows the relationship between NMSE at the LR and the training sequence length. The NMSE performance at the LR improves the DCE performance with longer training pilots. Although our simulation results are shown for the scenario where the LR and UR are at the same distance from the TX ($\sigma^\mathbf{2}_\mathbf{H} = \sigma^\mathbf{2}_\mathbf{G}$), the proposed DCE scheme works well even if the UR is much closer to the TX as long as the transmit power is sufficiently large. The reason is that the SNR at the UR does not change much with distance when the inserted AN dominates the noise at the UR.

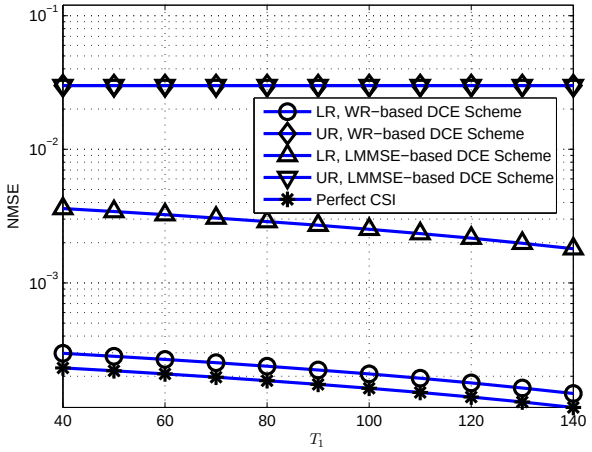
We then look into the performance of the proposed WR-based DCE scheme under a pilot contamination attack. As we have discussed in Section IV, the UR has no knowledge of the reverse training signals. In addition, we suppose that the UR sends another guess-based orthogonal signals $\bar{\mathbf{S}}_\mathbf{0}$ to attack the system, in which $\bar{P}_0 = P_{ave} = 1$. From Fig.4 (a), one can see that the NMSE performance at the LR with LMMSE-based DCE scheme has approximately reached the limitation of the UR's NMSE due to the poor channel estimation. On the



(a) $\gamma = 0.03$

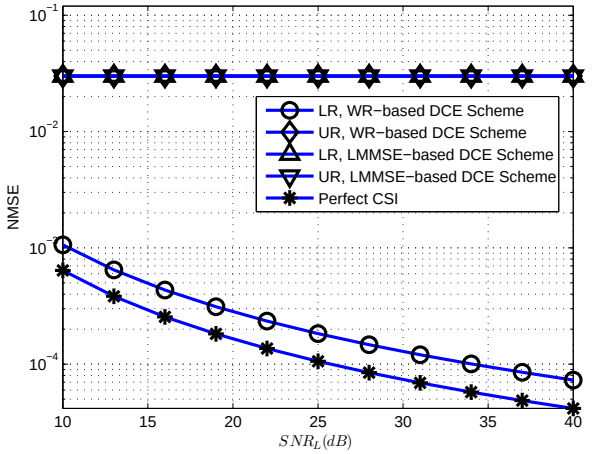


(b) $\gamma = 0.1$

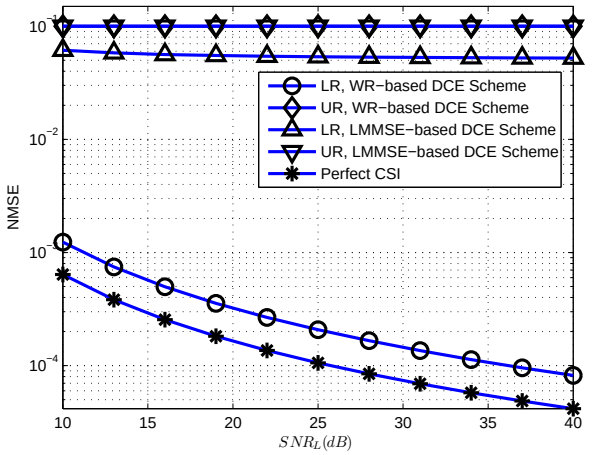


(c) Variation of T_1 when $SNR_L = 25dB$.

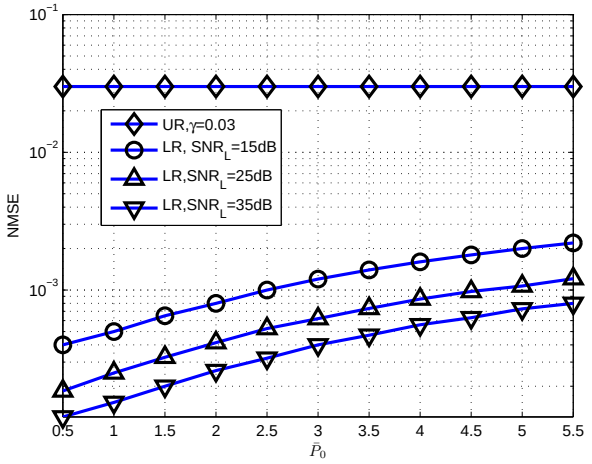
Fig. 3. NMSE performance comparison between the LMMSE-based DCE scheme and the WR-based DCE scheme



(a) $\gamma = 0.03$



(b) $\gamma = 0.1$



(c) Variation of $\bar{P}_0$ when the noise levels are set as $15dB$, $25dB$, $35dB$, respectively.

Fig. 4. NMSE performance of the LMMSE-based DCE scheme and the WR-based DCE scheme under the pilot contamination attack

contrary, the NMSE performance at the LR with the proposed DCE scheme only has a slight reduction. Similar results can be observed in Fig.4 (b) in case of $\gamma = 0.1$. As a result, the LMMSE-based DCE scheme is more sensitive to the pilot contamination attack than our proposed DCE scheme.

Fig.4 (c) shows the impact of pilot contamination attack on the performance of our proposed scheme with variation of attack power. Since the LMMSE-based DCE scheme works not very well under the pilot contamination attack, we only focus on the performance of the proposed DCE scheme. The result show that the obtained NMSE error at the LR has a slight reduction with the increasing power $\bar{P}_0$. The attack power is restricted at the UR, hence the pilot contamination attack has an ignorable impact on the performance of our proposed DCE scheme.

VI. Conclusion

In this paper, we proposed a new two-way training scheme for DCE in wireless MIMO systems. To improve the DCE performance, an efficient whitening-rotation (WR) based semi-blind approach has been employed in the two-way training. A closed-form of NMSE on the channel estimation between the LR and the UR has been developed, facilitating optimal power allocation between the training signals and AN. Furthermore, the proposed training design offers a countermeasure against the pilot contamination attack. It has been proved that the pilot contamination attack has a very limited impact on the DCE performance. Simulation results demonstrate that our proposed scheme can achieve higher performance than the existing training scheme.

Our future work includes the following directions of research: (a) We will extend the study of DCE from narrowband systems to wideband OFDM-based systems [29]. The power allocation between the training signal and AN across all pilot subcarriers will be an interesting problem to investigate. (b) We will apply the semiblind two-way training method to tackle the pilot contamination problem in multi-cell massive MIMO systems.

Appendix A
Derivation of unitary rotation matrix

According to (20), the rotation matrix $\mathbf{Q}$ can be obtained by using Lagrange method as follows,

$$\begin{aligned} LR: \quad & minf(\mathbf{Q},\lambda,\mu) = \sum_{i=\mathbf{1}}^{N_L} \parallel \mathbf{X_1}(i) - \sum_{j=\mathbf{1}}^{N_T} \hat{\sigma}_j q_{ij}^* \hat{\mathbf{S}}_\mathbf{1}(j) \parallel_F^\mathbf{2} \\ & + \sum_{i=1}^{N_L} Re\{\lambda_i(q_i^H q_i - 1)\} + \sum_{i=1}^{N_L}\sum_{j=i+1}^{N_L} Re\{\mu_{ij} q_i^H q_j\}. \end{aligned} \tag{59}$$

By differentiating (59) *w.r.t* $\mathbf{Q}$ and let it equals to 0, we have

$$\mathbf{X_1^* \tilde{S}_1^T \hat{W}_1} - \mathbf{Q \hat{W}_1^T \tilde{S}_1 \tilde{S}_1^H \hat{W}_1} = \mathbf{Q\Theta}, \tag{60}$$

where Θ is the matrix of Lagrange multipliers which satisfies $\Theta_{ii} = \lambda_i$,$\Theta_{ij} = \mu_{ij}$ when $i > j$ and $\Theta_{ij} = \mu_{ij}^*$ when $i < j$. We divide $\frac{P_1}{N_T} T_1$ on both sides of (60), and denote

$$\hat{\mathbf{X}}_\mathbf{Q} \triangleq \frac{\mathbf{X_1^* \hat{S}_1^T \hat{W}_1}}{\frac{P_1}{N_T}\mathbf{T_1}}.$$

Using the conjugate symmetry feature of Θ, we premultiply $\mathbf{Q}^H$ to (60) and post-multiply $\mathbf{Q}^H$ to the conjugate of (60). Performing a subtraction between the two new equations, we have

$$\mathbf{Q}^H \hat{\mathbf{X}}_\mathbf{Q} = \hat{\mathbf{X}}_\mathbf{Q}^H \mathbf{Q}. \tag{61}$$

According to the specific structure of (61), it holds if and only if

$$\hat{\mathbf{Q}}_\mathbf{1} = \mathbf{U}_{\hat{\mathbf{X}}_\mathbf{Q}} \mathbf{V}_{\hat{\mathbf{X}}_\mathbf{Q}}^H, \tag{62}$$

where $\mathbf{U}_{\hat{\mathbf{X}}_\mathbf{Q}}$ and $\mathbf{V}_{\hat{\mathbf{X}}_\mathbf{Q}}$ are the decomposition results after performing SVD on $\hat{\mathbf{X}}_\mathbf{Q}$, *e.g.,* $\hat{\mathbf{X}}_\mathbf{Q} = \mathbf{U}_{\hat{\mathbf{X}}_\mathbf{Q}} \mathbf{\Sigma}_{\hat{\mathbf{X}}_\mathbf{Q}} \mathbf{V}_{\hat{\mathbf{X}}_\mathbf{Q}}^H$.

Appendix B
Derivation of optimum power allocation

First, we need to develop the range of parameter γ. For the extreme case when $y = 0$, we know that

$$x \leq \frac{P_{ave} T_1}{N_T} \tag{63}$$

by using the power constraint of (51c). In this case, γ has the lower bound

$$\gamma \geq \frac{N_T \sigma_0^2}{P_{ave} T_1}. \tag{64}$$

To obtain the upper bound of γ, we need to analyze the NMSE error performance at the UR when $x = 0$. Similar to (42), the perturbation matrix of $\mathbf{M}$ can be rewritten as

$$\mathbf{\Delta M} \approx \mathbf{\Delta R}_{\mathbf{A},\mathbf{F_1}}^H \mathbf{N}_{\hat{\mathbf{W}}_\mathbf{0}}^H \mathbf{R}, \tag{65}$$

In this case, we have the result as follows

$$\mathbf{NMSE}_U \approx (N_T - N_L) P_\mathbf{ave}. \tag{66}$$

This result implies the worst MNSE performance at the UR, so we can obtain the upper bowed of γ,

$$\gamma \leq (N_T - N_L) P_{max}. \tag{67}$$

For the variable y, it satisfies the following inequations as

$$\frac{x\gamma - \sigma_0^2}{\sigma_G^2} \leq y \leq P_{ave} - \frac{x N_T}{T_1} \tag{68}$$

by using the constraints of (51a) and (51c). Besides, the inequations of (68) holds if and only if

$$P_{ave} - \frac{x N_T}{T_1} \geq \frac{x\gamma - \sigma_0^2}{\sigma_G^2}. \tag{69}$$

Thus, x satisfies

$$\frac{\sigma_0^2}{\gamma} \leq x \leq \frac{(\sigma_G^2 P_{ave} + \sigma_0^2) T_1}{\gamma T_1 + N_T \sigma_G^2}. \tag{70}$$

From the optimal problem (51), the objective function is monotonically decreasing with respect to the variable y, so the optimal value can be achieved when

$$y^* = \frac{x\gamma - \sigma_0^2}{\sigma_G^2}. \quad (71)$$

Furthermore, z is independent from x and y, thus the objective function approaches its optimization point when $z^* = P_{ave}$.

ACKNOWLEDGMENTS

The work was supported in part by programs of NSFC under Grants nos. 61322306, 61333013, U1201253, 61273192, 61370159, U1035001, 6120311761370159, U1035001 and 61203117, Guangdong Province Natural Science Foundation of under Grant S2011030002886 (team project), the Department of Science and Technology of Guangdong Province, China (nos. 2011A090100039,2011B090400360), program for New Century Excellent Talents in University under Grant NCET-11-0911 and Special Scientific Funds approved in 2011 for the Recruited Talents by Guangdong Provincial universities, and the Science and Technology Program of Guangzhou, China (grant no. 2014J2200097). The work of X. Zhou was supported by the Australian Research Council's Discovery Projects funding scheme (grant no. DP140101133). The corresponding author is Shengli Xie.

REFERENCES

[1] A. Wyner,"Wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1975.

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

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[4] X. Zhou, L. Song, and Y. Zhang, Physical Layer Security in Wireless Communications. CRC Press, 2013.

[5] N. Yang, H. Suraweera, I. Collings, C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. For. and Sec.*, pp. 254-259, Jan. 2013.

[6] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687-4698, Oct. 2008.

[7] X. Chen, L. Lei, H. Zhang, C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE Inter. Conf. Commun.(ICC)*, Sydney, Aus., 2014. [Online] Available FTP: http://arxiv.org/abs/1401.3049.

[8] N. R. Zurita, M. Ghogho, D. M. Lernon "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *Phys. Commun.*, vol. 4, no. 4, Dec. 2011, pp. 313-321.

[9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal. Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[10] X. Wang, K. Wang, and X. D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140-2155, June 2013.

[11] L. Y. Song, "Relay Selection for Two-way Relaying with Amplify-and-Forward Protocols," *IEEE Trans. Veh. Technol.*, vol. 60, no. 4, pp. 1954-1959, May 2011.

[12] L. Y. Song, Y. H. Li, and B. L. Jiao, "Differential Modulation for Bidirectional Relaying With Analog Network Coding," *IEEE Trans. Signal Process.*, vol. 58, no. 7, pp. 3933-3938, Jul. 2010.

[13] L. Y. Song, H. Guo, B. L Jiao, and M. Debbah, "Joint Relay Selection and Analog Network Coding Using Differential Modulation in Two-Way Relay Channels," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2932-2939, Jul. 2010.

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180-2189, Jun. 2008.

[15] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[16] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170-2181, Jun. 2013.

[17] T.-H. Chang, W.-C. Chiang, Y.-W. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems, " *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223-6237, 2010.

[18] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems", *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724-2738, may. 2013.

[19] X. Zhou, B. Maham, and A. Hjϕrungnes, "Pilot contamination for active eavesdropping, " *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903-907, Mar. 2012.

[20] C. R. Murthy, A. K. Jagannatham, and B. D. Rao, "Training-based and semiblind channel estimation for MIMO systems with maximum ratio transmission," *IEEE Trans. Signal Process.*, vol. 54, no. 7, pp. 2546-2558, 2006.

[21] A. K. Jagannatham and B. D. Rao, "Whitening-rotation-based semiblind MIMO channel estimation," *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 861-869, Mar. 2006.

[22] F. Wan, W. P. Zhu, and M. N. Swamy, "A signal perturbation free whitening-rotation-based semiblind approach for MIMO channel estimation," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3154-3166, Aug. 2009.

[23] H. Holma and A. Toskala,*WCDMA for UMTS*, vol. 4, New York: Wiley, 2000.

[24] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory,* New Jersey: Prentice Hall International, 1993.

[25] Golub, H. Gene, V. Loan, and F. Charles, *Matrix Computations*, 3rd edition, Johns Hopkins University Press, 1996.

[26] M. Chiang, C. W. Tan, D. P. Palomar, D. O'Neill and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640-2651, Jul. 2007.

[27] V. Buchoux, O. Capper, E. Moulines, and A. Gorokhov, "On the performance of semiblind subspace-based channel estimation," *IEEE Trans. Signal Process.*, vol. 48, no. 6, pp. 1750-1759, Jun. 2000.

[28] S. Shahbazpanahi, A. Gershman, and J. Manton, "Closed-form blind MIMO channel estimation for orthogonal space-time block codes," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4506-4517, Dec. 2005.

[29] A. Vinel, Q. Ni, D. Staehle, and A. Turlikov,"Capacity analysis of reservaion-based random access for broadband wireless access networks", *IEEE J. Sel. Areas Commun.*, vol. 27, no. 2, pp. 172-181, Feb.2009.