Training Signal Design for Discriminatory Channel Estimation

Tsung-Hui Chang, Y.-W. Peter Hong, and Chong-Yung Chi
Institute of Communications Engineering
National Tsing Hua University, Hsinchu, Taiwan
Email: changth@mx.nthu.edu.tw; {ywhong, cychi}@ee.nthu.edu.tw

***Abstract*— A training-based channel estimation scheme is proposed in the paper to enable the quality-of-service discrimination between legitimate and non-legitimate receivers in wireless networks. This method has applications ranging from user discrimination in wireless TV broadcast systems to the prevention of eavesdropping in secret communications. Specifically, by considering a network that consists of a multiple-antenna transmitter and two single-antenna receivers (i.e., the legitimate and non-legitimate receivers), we propose a multi-stage training-based channel estimation scheme that minimizes the normalized mean-squared error of the channel estimate at the legitimate receiver subject to a constraint on the estimation performance attainable by the non-legitimate receiver. The key idea is to exploit channel feedback from the legitimate receiver at the beginning of each stage to enable the use of artificial noise in the training signal, which allows us to effectively degrade the channel estimation performance at the non-legitimate receiver. The channel estimate obtained by the legitimate receiver in earlier stages are restricted due to constraints on the performance of the non-legitimate receiver, but may improve rapidly in later stages owing to the help of artificial noise and more accurate knowledge of the legitimate receiver's channel. Simulation results are presented to demonstrate the efficacy of the proposed channel estimation scheme.**

I. Introduction

Consider the problem of discriminating between the quality-of-service (QoS) achievable by different receivers in a downlink wireless system. This problem appears in many wireless applications, such as the QoS discrimination between paid and unpaid users in TV broadcast systems or the prevention of eavesdropping in secure communication systems. Conventionally, these issues have been addressed with the use of application level cryptography [1] or through authentication mechanisms [2], which typically requires large message overhead and may become vulnerable in the future as the computation power of unauthorized receivers increases. In recent years, the fundamental notion of physical-layer secrecy [3]–[5] has drawn much attention from the information theory community. Most of these works focus on the study of the so called secrecy capacity, that is, the maximum rate achievable between the legitimate transmitter-receiver pair subject to constraints on the information attainable by the unauthorized receiver. In this paper, we instead investigate these issues from a signal processing perspective through the design of training signals for discriminatory channel estimation at the receivers.

The main contribution of this work is to propose a multi-stage training-based channel estimation scheme that minimizes the normalized mean square error (NMSE) of the channel estimate at the legitimate receiver subject to a constraint on the estimation performance attainable by the unauthorized receiver or eavesdropper[1]. Specifically, consider a network that consists of a multiple-antenna transmitter and two single-antenna receivers (i.e., the legitimate receiver and the eavesdropper). Inspired by the work of Goel and Negi [6], discriminatory channel estimation is performed by utilizing artificial noise (AN) in the left null space of the legitimate receiver's channel to degrade the estimation performance of the eavesdropper. This requires transmitter's knowledge of the channel to the legitimate receiver that, however, can be obtained through feedback. The quality of the channel estimate obtained by the eavesdropper is constrained due to the use of AN while the estimate at the legitimate receiver can be refined after each stage. Consequently, QoS discrimination can be achieved by using high-order modulations or high-rate error correction codes for information data broadcasting since this will lead to poor symbol error performance at the eavesdropper.

Specifically, the proposed training-based channel estimation scheme consists of two phases. In Phase 1, the transmitter first broadcasts a training signal, as in conventional training schemes [7], to perform preliminary training on the legitimate receiver's channel. Because of the broadcast nature of the wireless medium, the training signal power in Phase 1 must be restricted in order to constrain the channel estimation performance at the eavesdropper, but this also limits the estimation performance at the legitimate receiver. By having the legitimate receiver feedback its preliminary channel estimate, the transmitter then sends another sequence of training signals which contains AN in the left null space of the legitimate receiver's channel. This special training sequence will degrade the eavesdropper's channel estimation performance while allowing the legitimate receiver to retrain its channel. Multiple stages of this feedback-and-retraining process can be

This work was supported in part by the National Science Council, Taiwan, under Grants NSC-96-2628-E-007-012-MY2, NSC-97-3114-E-007-002, NSC-97-2219-E-007-001, NSC-97-2221-E-007-037, and NSC-97-2221-E-007-073-MY3.

[1]Following the terminology of the secret communications literature [3], we shall refer to the unauthorized user as the eavesdropper throughout the remainder of this paper. However, this terminology may differ depending on the specific application.

978-1-4244-4148-8/09/$25.00 ©2009

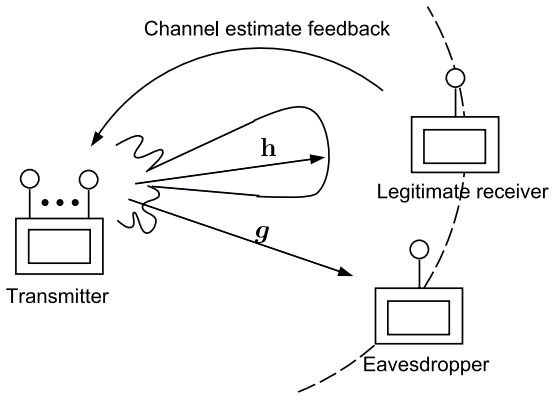

Figure 1. A network diagram consisting of a multi-antenna transmitter, a single-antenna legitimate receiver and eavesdropper.

performed in Phase 2 to further refine the channel estimate at the legitimate receiver. We show that the transmitter must be more conservative when utilizing AN in early stages, since the lack of precise knowledge of the legitimate receiver's channel will cause noise leakage into its channel [8] and further corrupt its channel estimate. Therefore, we propose to judiciously design the power allocation between the training data and the AN by minimizing the NMSE performance of the legitimate receiver subject to a performance constraint on the eavesdropper. Simulation results will show that the proposed discriminatory channel estimation scheme can render the legitimate receiver to acquire an accurate channel estimate while retaining the NMSE of the eavesdropper at a high value.

II. Problem Statement and Signal Model

We consider a wireless network that consists of a multi-antenna transmitter and two single-antenna receivers (i.e. the legitimate receiver and the eavesdropper) as shown in Figure 1. The transmitter emits a sequence of training signals to enable channel estimation at the legitimate receiver. To prevent the eavesdropper from benefiting from the training sequence, we propose a discriminatory multi-stage channel estimation scheme as described in the following:

- **Phase 1 (Preliminary training)**: The transmitter emits a sequence of regular training signals (that consists of only training data and no AN) for preliminary channel estimation at the legitimate receiver.
- **Phase 2 (Feedback-and-retraining)**: The legitimate receiver sends back its preliminary channel estimate to the transmitter. To degrade the channel estimation performance at the eavesdropper, the transmitter broadcasts another sequence of training signals which contains artificial noise (AN) in the left null space of the estimated channel. Both the legitimate receiver and the eavesdropper will make use of the training signals in both phases to refine their channel estimates. The feedback-and-retraining process can be repeated multiple times, if necessary.

Denote by N_t the number of transmit antennas at the transmitter. Assume that the feedback-and-retraining process in Phase 2 is performed K times such that there is a total of $K+1$ stages in the training process. Let $\mathbf{X}_k \in \mathbb{C}^{T_k \times N_t}$ denote the transmitted training signal matrix in stage k, with the signal length equal to T_k. The signals received by the legitimate receiver and the eavesdropper are respectively given by

$$\text{Legitimate receiver}: \boldsymbol{y}_k = \mathbf{X}_k \mathbf{h} + \boldsymbol{w}_k, \tag{1}$$

$$\text{Eavesdropper}: \mathbf{z}_k = \mathbf{X}_k \boldsymbol{g} + \boldsymbol{v}_k, \tag{2}$$

for $k = 1, 2, \ldots, K+1$, where

$\mathbf{h}, \boldsymbol{g} \in \mathbb{C}^{N_t}$: channel vectors from the transmitter to the legitimate receiver and the eavesdropper, respectively. The elements of $\mathbf{h}$ and $\boldsymbol{g}$ are assumed to be independent identically distributed (i.i.d.) complex Gaussian with zero mean and unit variance;

$\boldsymbol{w}_k, \boldsymbol{v}_k \in \mathbb{C}^{T_k}$: AWGN vectors at the legitimate receiver and the eavesdropper, with the powers per entry equal to σ_w^2 and σ_v^2, respectively.

The training signal matrices $\mathbf{X}_k$, $k = 1, \ldots, K+1$, are designed as follows. In Phase 1 (i.e., stage $k = 1$), the transmitter employs regular training techniques for preliminary channel estimation at the legitimate receiver. Assuming that the average transmission power in Phase 1 is P_1, we can write $\mathbf{X}_1$ as

$$\mathbf{X}_1 = \sqrt{\frac{P_1 T_1}{N_t}} \mathbf{C}_1 \tag{3}$$

where $\mathbf{C}_1 \in \mathbb{C}^{T_1 \times N_t}$ is the training data matrix satisfying $\mathbf{C}_1^H \mathbf{C}_1 = \mathbf{I}_{N_t}$ and $\mathbf{I}_{N_t}$ is an N_t-by-N_t identity matrix. We assume that the legitimate receiver uses the received signal $\boldsymbol{y}_1$ and the training signal $\mathbf{X}_1$ to obtain a preliminary estimate of $\mathbf{h}$, denoted by $\hat{\mathbf{h}}_1$, and sends $\hat{\mathbf{h}}_1$ back to the transmitter.

With $\hat{\mathbf{h}}_1$, we can then design the training signals that contain AN in the left null space of $\hat{\mathbf{h}}_1$ in an attempt to corrupt the eavesdropper's channel estimate [6]. Specifically, we set

$$\mathbf{X}_2 = \sqrt{\frac{P_2 T_2}{N_t}} \mathbf{C}_2 + \mathbf{A}_2 \cdot \mathbf{N}_{\hat{h},1}^H \tag{4}$$

where $P_2 > 0$, $\mathbf{C}_2 \in \mathbb{C}^{T_2 \times N_t}$ represents the training data matrix satisfying $\mathbf{C}_2^H \mathbf{C}_2 = \mathbf{I}_{N_t}$, $\mathbf{N}_{\hat{h},1} \in \mathbb{C}^{N_t \times (N_t - 1)}$ spans the left null space of $\hat{\mathbf{h}}_1$ satisfying $\mathbf{N}_{\hat{h},1}^H \mathbf{N}_{\hat{h},1} = \mathbf{I}_{N_t - 1}$, and $\mathbf{A}_2 \in \mathbb{C}^{T_2 \times (N_t - 1)}$ is an AN matrix, with each entry being i.i.d. complex Gaussian with zero mean and variance equal to $\sigma_{a,2}^2$. It is worthwhile to notice that, the legitimate receiver may also suffer from the AN added in (4) since the estimate $\hat{\mathbf{h}}_1$ is in general not perfect [8]. Therefore, the allocation between the training data power P_2 and the AN power $\sigma_{a,2}^2$ should be designed carefully.

The training design rule used in (4) also applies to $\mathbf{X}_k$ for $k = 3, \ldots, K+1$ if the feedback-and-retraining process in Phase 2 is performed multiple times. We will discuss this multiple-feedback-retraining case in detail in Section IV. In the next section, we focus on the case of $K = 1$ (one feedback-and-retraining process) and present a design criterion for the discrimination between the estimation performance of the legitimate receiver and that of the eavesdropper.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

III. Discriminatory Channel Estimation for $K = 1$

In the section, we first analyze the NMSE performances of the legitimate receiver and the eavesdropper considering that the training signal design mentioned in the previous section is used. Then, we find the optimal set of training powers P_1, P_2 and the AN power $\sigma_{a,2}^2$ that minimizes the NMSE of the legitimate receiver subject to an NMSE lower bound on the eavesdropper.

A. NMSE Analysis and Design Criterion

We assume that both the legitimate receiver and the eavesdropper employ the best linear unbiased estimator (BLUE) [9] for channel estimation. In that case, the preliminary channel estimate of $\mathbf{h}$ at the legitimate receiver in Phase 1 is given by

$$\hat{\mathbf{h}}_1 = (\mathbf{X}_1^H \mathbf{X}_1)^{-1} \mathbf{X}_1^H \boldsymbol{y}_1 \tag{5}$$

$$\triangleq \mathbf{h} + \Delta\mathbf{h}_1, \tag{6}$$

where $\Delta\mathbf{h}_1 \in \mathbb{C}^{N_t}$ is the estimation error vector which has the correlation matrix given by [9]

$$\mathrm{E}\{\Delta\mathbf{h}_1(\Delta\mathbf{h}_1)^H\} = \sigma_w^2 \left(\mathbf{X}_1^H \mathbf{X}_1\right)^{-1} = \left(\frac{N_t \sigma_w^2}{P_1 T_1}\right) \mathbf{I}_{N_t}. \tag{7}$$

We then obtain the associated normalized MSE (NMSE) of $\Delta\mathbf{h}_1$ as

$$\mathrm{NMSE}_{\mathrm{r}}^{(1)} = \frac{\mathrm{Tr}\left(\mathrm{E}\{\Delta\mathbf{h}_1(\Delta\mathbf{h}_1)^H\}\right)}{N_t} = \frac{N_t \sigma_w^2}{P_1 T_1}. \tag{8}$$

In Phase 2, the legitimate receiver can make use of both $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ as well as knowledge of $\hat{\mathbf{h}}_1$ to refine its channel estimate. Specifically, by (1), (3) and (4), we have

$$\boldsymbol{y} \triangleq \begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{P_1 T_1}{N_t}} \mathbf{C}_1 \\ \sqrt{\frac{P_2 T_2}{N_t}} \mathbf{C}_2 \end{bmatrix} \mathbf{h} + \begin{bmatrix} \boldsymbol{w}_1 \\ \mathbf{A}_2 \mathbf{N}_{\hat{h},1}^H \mathbf{h} + \boldsymbol{w}_2 \end{bmatrix}$$

$$= \begin{bmatrix} \sqrt{\frac{P_1 T_1}{N_t}} \mathbf{C}_1 \\ \sqrt{\frac{P_2 T_2}{N_t}} \mathbf{C}_2 \end{bmatrix} \mathbf{h} + \begin{bmatrix} \boldsymbol{w}_1 \\ -\mathbf{A}_2 \mathbf{N}_{\hat{h},1}^H \Delta\mathbf{h}_1 + \boldsymbol{w}_2 \end{bmatrix} \tag{9}$$

$$\triangleq \bar{\mathbf{C}}\mathbf{h} + \bar{\boldsymbol{w}}, \tag{10}$$

where we have applied (6) and the fact that $\mathbf{N}_{\hat{h},1}^H \hat{\mathbf{h}}_1 = \mathbf{0}$ in obtaining (9). Applying the BLUE to (10), we obtain the associated NMSE as [9]

$$\mathrm{NMSE}_{\mathrm{r}}^{(2)} = \frac{\mathrm{Tr}\left(\left(\bar{\mathbf{C}}^H \mathbf{R}_{\bar{w}}^{-1} \bar{\mathbf{C}}\right)^{-1}\right)}{N_t}, \tag{11}$$

where $\mathbf{R}_{\bar{w}} = \mathrm{E}\{\bar{\boldsymbol{w}}\bar{\boldsymbol{w}}^H\}$. By the independence between $\boldsymbol{w}_1$, $\boldsymbol{w}_2$ and $\mathbf{A}_2$, one can show that

$$\mathbf{R}_{\bar{w}} = \begin{bmatrix} \sigma_w^2 \mathbf{I}_{T_1} & \mathbf{0} \\ \mathbf{0} & \left(\mathrm{E}\{\|\mathbf{N}_{\hat{h},1}^H \Delta\mathbf{h}_1\|^2\}\sigma_{a,2}^2 + \sigma_w^2\right) \mathbf{I}_{T_2} \end{bmatrix}. \tag{12}$$

Since $\mathbf{N}_{\hat{h},1}$ and $\Delta\mathbf{h}_1$ are statistically independent conditioned on $\hat{\mathbf{h}}_1$, by (7), (8) and the fact that $\mathbf{N}_{\hat{h},1}^H \mathbf{N}_{\hat{h},1} = \mathbf{I}_{N_t-1}$, we can show that

$$\mathrm{E}\{\|\mathbf{N}_{\hat{h},1}^H \Delta\mathbf{h}_1\|^2\} = (N_t - 1) \cdot \mathrm{NMSE}_{\mathrm{r}}{}^{(1)}. \tag{13}$$

Substituting (12) and (13) into (11), we obtain

$$\mathrm{NMSE}_{\mathrm{r}}^{(2)} = \frac{\mathrm{Tr}\left(\left(\frac{P_1 T_1}{\sigma_w^2 N_t} + \frac{P_2 T_2 / N_t}{\mathrm{NMSE}_{\mathrm{r}}^{(1)} \cdot (N_t - 1)\sigma_{a,2}^2 + \sigma_w^2}\right)^{-1} \mathbf{I}_{N_t}\right)}{N_t}$$

$$= \left(\frac{1}{\mathrm{NMSE}_{\mathrm{r}}^{(1)}} + \frac{P_2 T_2 / N_t}{\mathrm{NMSE}_{\mathrm{r}}^{(1)} \cdot (N_t - 1)\sigma_{a,2}^2 + \sigma_w^2}\right)^{-1}. \tag{14}$$

The NMSE performance of the eavesdropper can be analyzed as follows. By (2), (3) and (4), we have the received signal at the eavesdropper as

$$\mathbf{z} \triangleq \begin{bmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{P_1 T_1}{N_t}} \mathbf{C}_1 \\ \sqrt{\frac{P_2 T_2}{N_t}} \mathbf{C}_2 \end{bmatrix} \boldsymbol{g} + \begin{bmatrix} \boldsymbol{v}_1 \\ \mathbf{A}_2 \mathbf{N}_{\hat{h},1}^H \boldsymbol{g} + \boldsymbol{v}_2 \end{bmatrix}$$

$$\triangleq \bar{\mathbf{C}}\boldsymbol{g} + \bar{\boldsymbol{v}}, \tag{15}$$

The covariance matrix of $\bar{\boldsymbol{v}}$ can be shown to be

$$\mathbf{R}_{\bar{v}} = \mathrm{E}\{\bar{\boldsymbol{v}}\bar{\boldsymbol{v}}^H\} = \begin{bmatrix} \sigma_v^2 \mathbf{I}_{T_1} & \mathbf{0} \\ \mathbf{0} & \left((N_t - 1)\sigma_{a,2}^2 + \sigma_v^2\right) \mathbf{I}_{T_2} \end{bmatrix}. \tag{16}$$

Hence, the NMSE of the eavesdropper is obtained as

$$\mathrm{NMSE}_{\mathrm{e}}^{(2)} = \frac{\mathrm{Tr}\left(\left(\frac{P_1 T_1}{\sigma_v^2 N_t} + \frac{P_2 T_2 / N_t}{(N_t - 1)\sigma_{a,2}^2 + \sigma_v^2}\right)^{-1} \mathbf{I}_{N_t}\right)}{N_t}$$

$$= \left(\frac{1}{\mathrm{NMSE}_{\mathrm{e}}^{(1)}} + \frac{P_2 T_2 / N_t}{(N_t - 1)\sigma_{a,2}^2 + \sigma_v^2}\right)^{-1}, \tag{17}$$

where

$$\mathrm{NMSE}_{\mathrm{e}}^{(1)} = \frac{N_t \sigma_v^2}{P_1 T_1} \tag{18}$$

stands for the NMSE of the eavesdropper when using only the training signal in Phase 1 for channel estimation. It is worthwhile to notice from (14) and (17) that

$$\mathrm{NMSE}_{\mathrm{r}}^{(2)} \leq \mathrm{NMSE}_{\mathrm{r}}^{(1)}, \quad \mathrm{NMSE}_{\mathrm{e}}^{(2)} \leq \mathrm{NMSE}_{\mathrm{e}}^{(1)}, \tag{19}$$

as long as $P_2 T_2 > 0$, implying that both the legitimate receiver and the eavesdropper should always use the training signals in both phases for channel estimation.

With (14) and (17), we can then find the optimal set of training powers P_1, P_2 and AN power $\sigma_{a,2}^2$ by solving the following optimization problem:

$$\min_{P_1, P_2, \sigma_{a,2}^2 \geq 0} \quad \mathrm{NMSE}_{\mathrm{r}}^{(2)} \tag{20a}$$

$$\text{s.t.} \quad \mathrm{NMSE}_{\mathrm{e}}^{(2)} \geq \gamma_e, \tag{20b}$$

$$\frac{\mathrm{E}\{\|\mathbf{X}_1\|_F^2\} + \mathrm{E}\{\|\mathbf{X}_2\|_F^2\}}{T_1 + T_2} \leq P_{\mathrm{ave}}, \tag{20c}$$

where $0 < \gamma_e < 1$ is the preassigned NMSE lower bound on the eavesdropper, and $P_{\mathrm{ave}} > 0$ is the maximum average power. Equation (20c) represents an average power budget constraint on the training signals over both phases. Notice that, by (3) and (4), we can write

$$\mathrm{E}\{\|\mathbf{X}_1\|_F^2\} + \mathrm{E}\{\|\mathbf{X}_2\|_F^2\} = P_1 T_1 + (P_2 + (N_t - 1)\sigma_{a,2}^2) T_2. \tag{21}$$

978-1-4244-4148-8/09/$25.00 ©2009

One can see that criterion (20) aims to minimize the NMSE of the legitimate receiver while enforcing an NMSE lower bound on the eavesdropper.

It is interesting to remark that, by (17), (18) and (20b),

$$\gamma_e \leq \mathrm{NMSE}_{\mathrm{e}}^{(2)} \leq \mathrm{NMSE}_{\mathrm{e}}^{(1)} = \frac{N_t \sigma_v^2}{P_1 T_1}. \tag{22}$$

Since $P_1 T_1 \leq P_{\mathrm{ave}}(T_1 + T_2)$ by (20c) and (21), we have that

$$0 \leq P_1 T_1 \leq \min\left\{ \frac{N_t \sigma_v^2}{\gamma_e}, P_{\mathrm{ave}}(T_1 + T_2) \right\}. \tag{23}$$

However, it is reasonable to choose

$$\gamma_e \geq \frac{N_t \sigma_v^2}{P_{\mathrm{ave}}(T_1 + T_2)} \tag{24}$$

where the right hand side of (24) stands for the minimum NMSE achievable at the eavesdropper without adding any AN. If $\gamma_e < N_t \sigma_v^2 / (P_{\mathrm{ave}}(T_1 + T_2))$, then a straightforward optimal solution to (20) is given by $P_1 = P_2 = P_{\mathrm{ave}}$ and $\sigma_{a,2}^2 = 0$. Hence, by (23) and (24), we conclude with

$$0 \leq P_1 T_1 \leq \tilde{\gamma}_e \triangleq \frac{N_t \sigma_v^2}{\gamma_e} \tag{25}$$

as an additional constraint for (20).

B. Optimal Power Allocation

We now show that, with the additional constraint in (25), the nonconvex optimization problem in (20) can be solved via a simple method based on the one-dimensional line search. For notational simplicity, we define $a = P_1 T_1$, $b = P_2 T_2$ and $c = (N_t - 1)\sigma_{a,2}^2$. Together with the constraint in (25), one can reformulate (20) into the following maximization problem

$$\max_{a,b,c \geq 0} \; a + \frac{a \cdot b}{N_t \cdot c + a} \tag{26a}$$

$$\text{s.t. } a + \frac{b \cdot \sigma_v^2}{c + \sigma_v^2} \leq \tilde{\gamma}_e, \tag{26b}$$

$$a + T_2 \cdot c + b \leq P_{\mathrm{ave}}(T_1 + T_2), \tag{26c}$$

$$a \leq \tilde{\gamma}_e. \tag{26d}$$

By close inspection of the problem structure of (26), it can be shown that solving (20) is equivalent to solving the following problem with only a as the variable:

$$\max_{a} \; a + \frac{a \cdot b(a)}{N_t \cdot c(a) + a} \tag{27a}$$

$$\text{s.t. } N_t \sigma_v^2 \leq a \leq \tilde{\gamma}_e, \tag{27b}$$

where

$$c(a) = \frac{P_{\mathrm{ave}} \cdot (T_1 + T_2) - \tilde{\gamma}_e}{T_2 + \left(\frac{\tilde{\gamma}_e - a}{\sigma_v^2} \right)}, \tag{28}$$

$$b(a) = \left(\frac{\tilde{\gamma}_e - a}{\sigma_v^2} \right) c(a) + \tilde{\gamma}_e - a. \tag{29}$$

Therefore, (27) can be solved via line searching with respect to a over the interval $[N_t \sigma_v^2, \tilde{\gamma}_e]$, and the associated optimal c and b can be obtained by (28) and (29), respectively. The proof of equivalence of (20) and (26) is omitted here due to space limitations.

IV. Discriminatory Channel Estimation for $K > 1$

It is worthwhile to notice that, even with the optimal power allocation, the NMSE performance of the legitimate receiver may be restricted (and may even be worse than that of the eavesdropper) if we are only allowed to perform one stage of feedback-and-retraining process in Phase 2. This is true especially when γ_e is set at a high value or when the eavesdropper has a much higher signal-to-noise ratio (SNR) than the legitimate receiver (e.g., when $\sigma_v^2 \ll \sigma_w^2$). In either of these cases, the training energy $P_1 T_1$ in Phase 1 must be small in order to meet the constraint in (22), which then degrades the quality of the preliminary channel estimate in Phase 1. The lack of precision in the preliminary channel estimate (i.e., the large value of $\mathrm{NSME}_{\mathrm{r}}^{(1)}$) will restrict the use of AN in Phase 2 and thereby limit the ability of the training scheme to discriminate between performance of the legitimate receiver and that of the eavesdropper [see also (14)]. Fortunately, this problem can be resolved by performing multiple stages of feedback and retraining in Phase 2.

We consider the case that the channel estimate feedback and retraining in Phase 2 is repeated K times ($K > 1$) so that there is a total of $K + 1$ stages of training. For $k > 2$, let $\hat{\mathbf{h}}_{k-1}$ be the channel estimate obtained at the legitimate receiver from the observations $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{k-1}$ and training data $\mathbf{C}_1, \ldots, \mathbf{C}_{k-1}$. In the kth stage of training, the discriminatory training signal $\mathbf{X}_k$ is given by

$$\mathbf{X}_k = \sqrt{\frac{P_k T_k}{N_t}} \mathbf{C}_k + \mathbf{A}_k \mathbf{N}_{\hat{h},k-1}^H, \tag{30}$$

where $\mathbf{C}_k \in \mathbb{C}^{T_k \times N_t}$ is the training data matrix satisfying $\mathbf{C}_k^H \mathbf{C}_k = \mathbf{I}_{N_t}$, $\mathbf{N}_{\hat{h},k-1} \in \mathbb{C}^{N_t \times (N_t - 1)}$ spans the left null space of $\hat{\mathbf{h}}_{k-1}$ satisfying $\mathbf{N}_{\hat{h},k}^H \mathbf{N}_{\hat{h},k} = \mathbf{I}_{N_t - 1}$, and $\mathbf{A}_k \in \mathbb{C}^{T_k \times (N_t - 1)}$ consists of i.i.d. complex Gaussian random variables with zero mean and variance equal to $\sigma_{a,k}^2$. Denote by

$$\Delta \mathbf{h}_{k-1} = \hat{\mathbf{h}}_{k-1} - \mathbf{h} \tag{31}$$

the estimation error vector at stage $k-1$. For $K > 1$, one can rewrite the received signal at the legitimate receiver in (10) as follows

$$\boldsymbol{y}_1 = \sqrt{\frac{P_1 T_1}{N_t}} \mathbf{C}_1 \mathbf{h} + \boldsymbol{w}_1, \tag{32}$$

$$\begin{aligned} \boldsymbol{y}_k &= \sqrt{\frac{P_k T_k}{N_t}} \mathbf{C}_k \mathbf{h} + \mathbf{A}_k \mathbf{N}_{\hat{h},k-1}^H \mathbf{h} + \boldsymbol{w}_k \\ &= \sqrt{\frac{P_k T_k}{N_t}} \mathbf{C}_k \mathbf{h} - \mathbf{A}_k \mathbf{N}_{\hat{h},k-1}^H \Delta \mathbf{h}_{k-1} + \boldsymbol{w}_k \end{aligned} \tag{33}$$

for $k = 2, \ldots, K+1$. Following the analysis presented in Section III-A, we can show that the NMSE at the legitimate receiver with K feedback-and-retraining processes can be expressed in the following recursive form

$$\mathrm{NMSE}_{\mathrm{r}}^{(\mathrm{K}+1)} = \left(\frac{1}{\mathrm{NMSE}_{\mathrm{r}}^{(\mathrm{K})}} + \frac{P_{K+1} T_{K+1} / N_t}{\mathrm{NMSE}_{\mathrm{r}}^{(\mathrm{K})} \cdot (N_t - 1)\sigma_{a,K+1}^2 + \sigma_w^2} \right)^{-1}, \tag{34}$$

978-1-4244-4148-8/09/$25.00 ©2009

with the $\mathrm{NMSE}_{\mathrm{r}}^{(1)}$ given in (8). Similarly, the NMSE at the eavesdropper by $(K+1)$-stage training can be shown to be

$$\mathrm{NMSE}_{\mathrm{e}}^{(\mathrm{K}+1)} = \left(\frac{1}{\mathrm{NMSE}_{\mathrm{e}}^{(\mathrm{K})}} + \frac{P_{K+1}T_{K+1}/N_t}{(N_t-1)\sigma_{a,K+1}^2 + \sigma_v^2} \right)^{-1} = \left(\frac{P_1 T_1}{N_t \sigma_v^2} + \sum_{k=2}^{K+1} \frac{P_k T_k / N_t}{(N_t-1)\sigma_{a,k}^2 + \sigma_v^2} \right)^{-1}. \quad (35)$$

With (34) and (35), one can jointly optimize the power values of P_1, and P_k and $\sigma_{a,k}^2$ for $k = 2, \ldots, K+1$, by using a design criterion as in (20). Specifically, we consider the following optimization problem:

$$\min_{\substack{P_1, P_k, \sigma_{a,k}^2 \geq 0, \\ k=2,\ldots,K+1}} \quad \mathrm{NMSE}_{\mathrm{r}}^{(\mathrm{K}+1)} \quad (36a)$$

$$\text{s.t.} \quad \mathrm{NMSE}_{\mathrm{e}}^{(\mathrm{K}+1)} \geq \gamma_e, \quad (36b)$$

$$0 \leq P_1 T_1 \leq \tilde{\gamma}_e, \quad (36c)$$

$$\sum_{k=1}^{K+1} \mathrm{E}\{\|\mathbf{X}_k\|_F^2\} \leq P_{\mathrm{ave}} \left(\sum_{k=1}^{K+1} T_k \right), \quad (36d)$$

where (36c) is due to (25), and (36d) is the energy budge constraint. In comparison with (20), the optimization problem (36) is much more involved due to the recursive structure in (34). In fact, (36) is nonconvex and the global optimum solution is completely intractable. However, (36) can be suboptimally handled using the monomial approximation and condensation method (a successive convex approximation method) in the context of geometric programming (GP) [10]. This method basically involves solving a sequence of convex GPs, and hence an approximate solution of (36) can be efficiently obtained by interior point methods. Due to space limitations, the application of the condensation method to (36) is omitted here. In the next section, it will be shown by computer simulations that the discriminatory channel estimation performance can be greatly improved when the multiple-feedback-retraining process and the design criterion in (36) are used.

V. Simulation Results and Discussion

In the section, computer simulation results are presented to demonstrate the efficacy of the proposed discriminatory channel estimation scheme. A network system as shown in Figure 1 was considered. We set $N_t = 4$ and set the elements of the channel vectors $\mathbf{h}$ and $\boldsymbol{g}$ as i.i.d. complex Gaussian random variables with zero mean and unit variance. The training data matrices $\mathbf{C}_k$, $k = 1, \ldots, K+1$, were randomly drawn from semi-unitary $T_k \times N_t$ matrices. The average power budget P_{ave} was set to 30 dBm and the training signal length per phase was set to

$$T_k = \left\lfloor \frac{300}{K+1} \right\rfloor \quad (37)$$

for all $k = 1, \ldots, K+1$. It is worthwhile to note from (37) that we have fixed the total training length (which was 300) and thus also fixed the total energy consumed for training for any choice of K. In the simulation, we considered an "NMSE lower bound" which is given by

$$\text{NMSE lower bound} = \frac{N_t \sigma_w^2}{P_{\mathrm{ave}} \sum_{k=1}^{K+1} T_k}. \quad (38)$$

This lower bound represents the best NMSE performance achievable by the legitimate receiver and the eavesdropper when $\sigma_{a,k}^2 = 0$ for all k (no discrimination). The SNRs at the legitimate receiver and at the eavesdropper were respectively defined as

$$\mathrm{SNR}_{\mathrm{r}} = \frac{P_{\mathrm{ave}}}{\sigma_w^2}, \quad \mathrm{SNR}_{\mathrm{e}} = \frac{P_{\mathrm{ave}}}{\sigma_v^2}. \quad (39)$$

Each simulation result was obtained by averaging over 100 channel realizations.

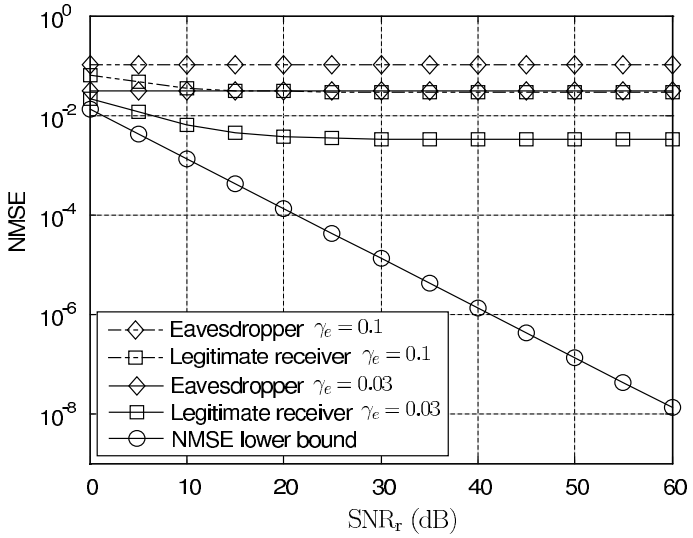

Figure 2. Simulation results of NMSE performance when only one feedback-and-retraining process is performed in Phase 2 ($K = 1$) for $\mathrm{SNR}_{\mathrm{r}} = \mathrm{SNR}_{\mathrm{e}}$.

We first consider the scenario when the legitimate receiver and the eavesdropper are equally distant from the transmitter (i.e., $\mathrm{SNR}_{\mathrm{r}} = \mathrm{SNR}_{\mathrm{e}}$) and only one feedback-and-retraining process was performed in Phase 2 ($K = 1$). In Figure 2, we show the NMSE performance of the legitimate receiver and that of the eavesdropper for $\gamma_e = 0.1$ and $\gamma_e = 0.03$, respectively. The power values P_1, P_2 and $\sigma_{a,2}^2$ were obtained according to (20). First, one can see from this figure, that NMSEs of the eavesdropper are well constrained to 0.1 and 0.03, respectively, and we see that the discrimination between the legitimate receiver and the eavesdropper is significant only for $\mathrm{SNR}_{\mathrm{r}} \geq 20$ dB, implying that a sufficient amount of power is required for discriminatory channel estimation. Second, we observe that the NMSE difference between the legitimate receiver and the eavesdropper for $\gamma_e = 0.1$ is quite limited and is larger for $\gamma_e = 0.03$, demonstrating a tradeoff between the value of γ_e and the achievable NMSE of the legitimate receiver. Finally, one can see from Figure 2 that the NMSE attainable by the legitimate receiver is far away from the NMSE lower bound.

In Figure 3, we display the results when 15 feedback-and-retraining processes were performed in Phase 2 ($K = 15$). The

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

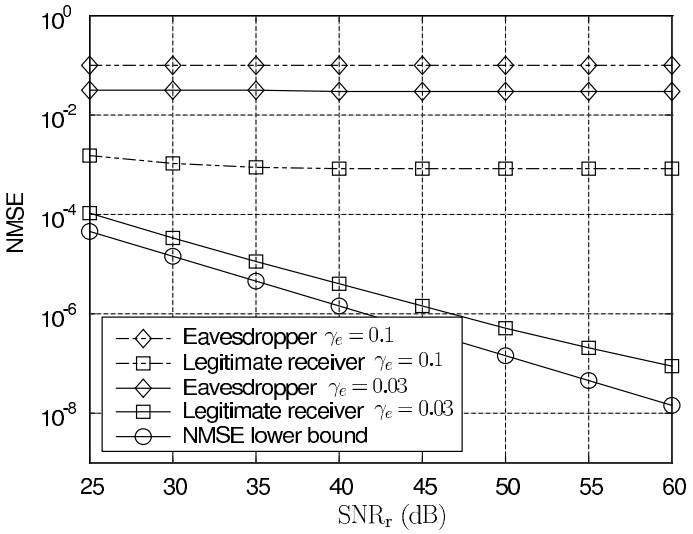

Figure 3. Simulation results of NMSE performance for $K = 15$ and $\mathrm{SNR_r} = \mathrm{SNR_e}$.

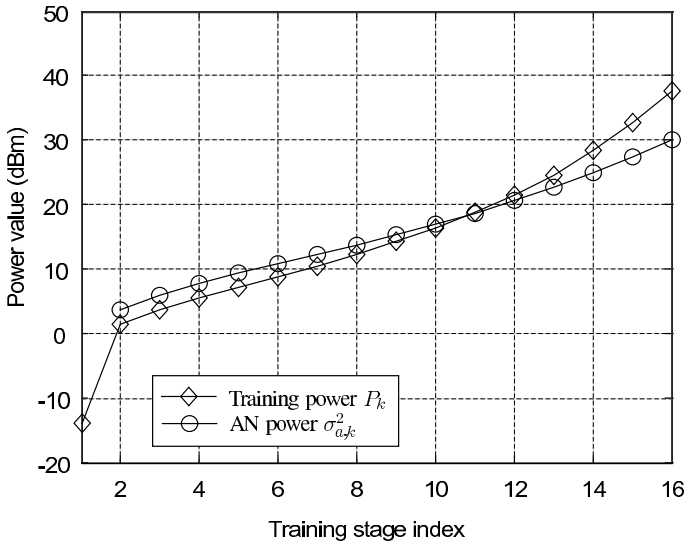

Figure 4. Distributions of $\{P_k\}_{k=1}^{K+1}$ and $\{\sigma^2_{a,k}\}_{k=2}^{K+1}$ for $\gamma_e = 0.03$, $K = 15$ and $\mathrm{SNR_r} = \mathrm{SNR_e} = 40$ dB.

values of $\{P_k\}_{k=1}^{16}$ and $\{\sigma^2_{a,k}\}_{k=2}^{16}$ were calculated according to (36). By comparing Figure 3 with Figure 2, one can see that the NMSE performance of the legitimate receiver either for $\gamma_e = 0.1$ or for $\gamma_e = 0.03$ is greatly improved, whereas the NMSEs of the eavesdropper are still well controlled. In particular, we can see that the NMSE of the legitimate receiver can be close to the NMSE lower bound for $\gamma_e = 0.03$ and for all $\mathrm{SNR_r} \geq 25$ dB, showing the efficacy of the proposed discriminatory channel estimation scheme. To understand how the multiple-feedback-retraining approach can improve the discriminatory channel estimation performance, we plot the distributions of optimized $\{P_k\}_{k=1}^{16}$ and $\{\sigma^2_{a,k}\}_{k=2}^{16}$ in Figure 4 for $\gamma_e = 0.03$ and $\mathrm{SNR_r} = \mathrm{SNR_e} = 40$ dB. We can see that the optimized P_1 is relatively very small in order to limit the eavesdropper's best NMSE performance to 0.03. After the first phase of training, the optimized P_k as well as AN powers $\sigma^2_{a,k}$ monotonically increase since the $\mathrm{NMSE_r^{(k)}}$ can gradually decrease from one training stage to another [see (34)].

We also considered the scenario that the eavesdropper is much closer to the transmitter than the legitimate receiver (i.e., $\mathrm{SNR_e} \gg \mathrm{SNR_r}$). We set $\mathrm{SNR_r} = 25$ dB and $\mathrm{SNR_e} = 45$ dB. Figure 5 shows the results for $\gamma_e = 0.03$ and $\gamma_e = 0.02$. We can observe from this figure that for $K \leq 2$, the NMSE performance of the legitimate receiver can be even worse than the eavesdropper. However, if there were more than 3 feedback-and-retraining processes performed in Phase 2, the adverse situation can be turned around and the NMSE performance of the legitimate receiver eventually gets close to the NMSE lower bound.

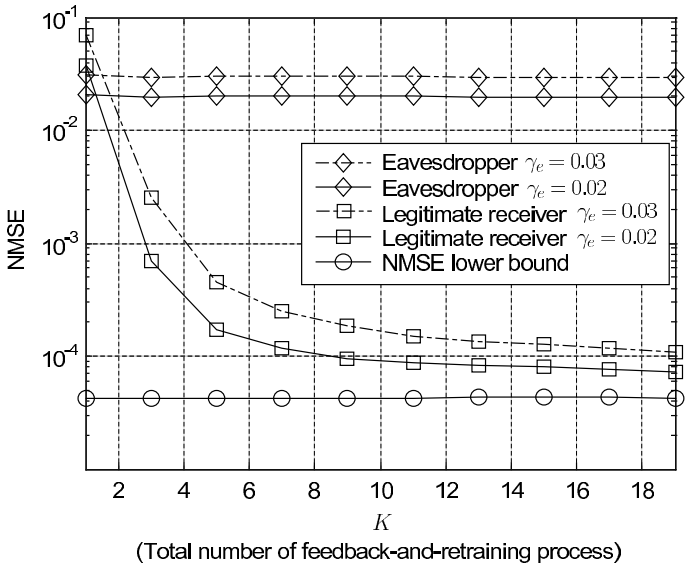

Figure 5. Simulation results of NMSE performance when multiple feedback-and-retraining processes are performed in Phase 2 for $\mathrm{SNR_r} = 25$ dB and $\mathrm{SNR_e} = 45$ dB.

REFERENCES

[1] C. E. Landwehr and D. M. Goldschlag, "Secure issues in networks with internet access," *Proc. IEEE*, vol. 85, pp. 2034–2051, Dec. 1997.

[2] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Communs. the ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.

[3] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME wiretap channel," submitted to *IEEE Trans. Inform. Theory*, 2008.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE ISIT*, Toronto, ON, Canada, July 6-11, 2008, pp. 524–528.

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

[7] T. F. Wong and B. Park, "Training sequence optimization in MIMO systems with colored interference," *IEEE Trans. Commun.*, vol. 52, no. 11, pp. 1939–1947, Nov. 2004.

[8] Y.-L. Liang, Y.-S. Wang, T.-H. Chang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy using artificial noise," in *Proc. IEEE ISIT*, Souel, Korea, June 28-July 3, 2009, pp. 2351–2355.

[9] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ: Prentice Hall International, 1993.

[10] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optim. Eng.*, vol. 8, pp. 67–127, April 2007.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.