ON MITIGATION OF PILOT SPOOFING ATTACK

Jitendra K. Tugnait

Department of Electrical & Computer Engineering
Auburn University, Auburn, AL 36849, USA
tugnajk@eng.auburn.edu

ABSTRACT

In a time-division duplex (TDD) multiple antenna system, the channel state information (CSI) can be estimated using reverse training. A pilot contamination (spoofing) attack occurs when during the training phase, an adversary also sends identical training (pilot) signal as that of the legitimate receiver. This contaminates channel estimation and alters the legitimate beamformimg design, facilitating eavesdropping. A recent approach proposed superimposing a random sequence on the training sequence at the legitimate receiver and then using the minimum description length (MDL) criterion to detect pilot contamination attack. In this paper we augment this approach with joint estimation of both legitimate receiver and eavesdropper channels, and secure beamforming, to mitigate the effects of pilot spoofing. The proposed mitigation approach is illustrated via simulations.

Index Terms— Physical layer security, pilot spoofing attack, active eavesdropping, secure beamforming.

1. INTRODUCTION

Consider a three-node time-division duplex (TDD) multiple antenna system, consisting of a multi-antenna base station Alice, a single antenna legitimate user Bob, and a single antenna eavesdropper Eve. Alice designs its transmit beamformer based upon its channel to Bob for improved performance. In a TDD system, the downlink and uplink channels can be assumed to be reciprocal. Therefore, Alice can acquire the channel state information (CSI) regarding Alice-to-Bob channel via reverse training during the uplink transmission. Bob sends pilot (training) signals to Alice during the training phase of the slotted TDD system. If Eve attacks the channel training phase by transmitting the same pilot sequence during the training phase, the CSI estimated by Alice then is a weighted sum of Bob-to-Alice and Eve-to-Alice CSIs. Consequently the beamformer designed on this basis will lead to a significant information leakage to Eve. This is an example of a pilot contamination attack [1, 2].

This issue of pilot contamination attack was first noted in [1] where the focus is on enhancing eavesdropper's performance. Several approaches are discussed in [2, 3, 4, 5] for detection of the attack assuming a TDMA uplink requiring separate time slots for each user Bob. In [6] an SDMA uplink was considered to allow for simultaneous transmission of training from Bobs.

Relation to Prior Work: Approaches of [3, 5] require a separate secure channel from Alice-to-Bob (two-way training) to work. We only need one-way reverse training in this paper. Refs. [2, 4, 6] deal only with attack detection, not its mitigation. In this paper we augment the approach of [4] with joint estimation of both legitimate receiver and eavesdropper channels, and secure beamforming, to mitigate the effects of pilot spoofing. Our set-up (and that of [2, 3, 4, 5, 6]) is different from the jamming scenarios considered in [7] (and others). Here Eve's objective is to make Alice replace Alice-to-Bob channel with Alice-to-Eve channel, whereas pilot jamming of [7] aims to degrade overall system performance.

Notation: Superscripts $(.)^*$, $(.)^\top$ and $(.)^H$ represent complex conjugate, transpose and complex conjugate transpose (Hermitian) operation, respectively, on a vector/matrix. The notation $\mathbb{E}\{.\}$ denotes the expectation operation, $\mathbb{C}$ the set of complex numbers, $\mathbf{I}_M$ an $M \times M$ identity matrix, $\mathbf{1}_{\{A\}}$ is the indicator function. The notation $\mathbf{x} \sim \mathcal{N}_c(\mathbf{m}, \Sigma)$ denotes a random vector $\mathbf{x}$ that is circularly symmetric complex Gaussian with mean $\mathbf{m}$ and covariance Σ.

2. SYSTEM MODEL AND BACKGROUND

We follow the system model of [2, 3, 5, 4]. Let $s_t(n)$, $1 \le n \le T$, denote the training sequence of length T time samples. Consider a flat Rayleigh fading environment with Bob-to-Alice channel denoted as $\mathbf{h}_B = \sqrt{d_B}\,\tilde{\mathbf{h}}_B \in \mathbb{C}^{N_r \times 1}$ and Eve-to-Alice channel denoted as $\mathbf{h}_E = \sqrt{d_E}\,\tilde{\mathbf{h}}_E \in \mathbb{C}^{N_r \times 1}$, where real scalars d_B and d_E represent respective path loss attenuations and $\tilde{\mathbf{h}}_B \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$ and $\tilde{\mathbf{h}}_E \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$ represent small-scale fading. Let P_B and P_E denote the average training power allocated by Bob and Eve, respectively. In the absence of any transmission from Eve, the received signal at Alice during the training phase is given by

$$\mathbf{y}(n) = \sqrt{P_B}\,\mathbf{h}_B s_t(n) + \mathbf{v}(n) \tag{1}$$

where additive noise $\mathbf{v}(n) \sim \mathcal{N}_c(0, \sigma_v^2 \mathbf{I}_{N_r})$ and we normalize $T^{-1}\sum_{n=1}^{T} |s_t(n)|^2 = 1$ (e.g., take $|s_t(n)| = 1$). When Eve also transmits (Eve's pilot contamination attack), the received signal at Alice during the training phase is

$$\mathbf{y}(n) = \left(\sqrt{P_B}\,\mathbf{h}_B + \sqrt{P_E}\,\mathbf{h}_E\right) s_t(n) + \mathbf{v}(n). \tag{2}$$

This work was supported by NSF Grant ECCS-1651133.

In case of Eve's attack, based on (2), Alice would estimate $\sqrt{P_B}\,\mathbf{h}_B + \sqrt{P_E}\,\mathbf{h}_E$ as Bob-to-Alice channel, instead of $\sqrt{P_B}\,\mathbf{h}_B$ based on (1).

How to detect Eve's attack based only on the knowledge of $s_t(n)$ and $\mathbf{y}(n)$, is addressed in [4] where a fraction β of the training power P_B at Bob is allocated to a scalar random sequence $s_B(n)$ (zero-mean, i.i.d., normalized to have $T^{-1}\sum_{n=1}^{T}|s_B(n)|^2 = 1$, finite alphabet: BPSK or QPSK, e.g.) to be transmitted by Bob along with (superimposed on) $s_t(n)$. That is, instead of $\sqrt{P_B}s_t(n)$, Bob transmits ($0 \le \beta < 1,\ \ n = 1, 2, \cdots, T$)

$$\tilde{s}_B(n) = \sqrt{P_B(1-\beta)}\, s_t(n) + \sqrt{P_B\beta}\, s_B(n). \tag{3}$$

The sequence $\{s_B(n)\}$ is unknown to Alice (and to Eve) and it can not be replicated in advance as it is a random sequence generated at Bob. However, Alice knows that such $\{s_B(n)\}$ is to be expected in $\mathbf{y}(n)$.

Now we have the following two hypotheses $\mathcal{H}_0$ (no attack) and $\mathcal{H}_1$ (attack present) for the received signal at Alice:

$$\begin{array}{ll} \mathcal{H}_0: & \mathbf{y}(n) = \mathbf{h}_B\tilde{s}_B(n) + \mathbf{v}(n) \\ \mathcal{H}_1: & \mathbf{y}(n) = \mathbf{h}_B\tilde{s}_B(n) + \sqrt{P_E}\,\mathbf{h}_E s_t(n) + \mathbf{v}(n). \end{array} \tag{4}$$

Define the correlation matrix of measurements as ($i = 0, 1$)

$$\mathbf{R}_{y,i} = T^{-1}\sum_{n=1}^{T}\mathbb{E}\left\{\mathbf{y}(n)\mathbf{y}^H(n)\,\middle|\,\mathcal{H}_i\right\} \tag{5}$$

and the correlation matrix of source signals as ($i = 0, 1$)

$$\mathbf{R}_{s,i} = T^{-1}\sum_{n=1}^{T}\mathbb{E}\left\{[\mathbf{y}(n)-\mathbf{v}(n)][\mathbf{y}(n)-\mathbf{v}(n)]^H\,\middle|\,\mathcal{H}_i\right\}. \tag{6}$$

Then we have

$$\mathbf{R}_{y,i} = \mathbf{R}_{s,i} + \sigma_v^2\mathbf{I}_{N_r},\ \ i = 0, 1. \tag{7}$$

It is shown in [4] that $\text{rank}(\mathbf{R}_{s,0}) = 1$ and $\text{rank}(\mathbf{R}_{s,1}) = 2$. Thus, introduction of $\{s_B(n)\}$ by Bob leads to signal subspace of rank 2 in the presence of Eve's attack. If $\beta = 0$, then $\text{rank}(\mathbf{R}_{s,1}) = 1$. [4] exploits the MDL estimator of the signal subspace dimension d ([8, 9, 10]) based on the eigenvalues of the estimated data correlation matrix to detect spoofing attack; it does not address attack mitigation. Note that if Eve also adds a random sequence to its pilot, $\text{rank}(\mathbf{R}_{s,1}) = 2$. The attack will be detected but our mitigation approach will not apply.

3. JOINT CHANNEL ESTIMATION

If the MDL method indicates presence of attack, Alice proceeds to jointly estimate the channels to Bob and Eve.

3.1. No Attack

If the MDL method indicates absence of any attack, Alice proceeds to initially estimate the channel using (4) under $\mathcal{H}_0$, knowledge of $\{s_t(n)\}$ and the least-squares method. This approach treats $\{s_B(n)\}$ as interference. An obvious solution is to perform iterative channel estimation via a linear minimum mean-square error (MMSE) equalizer to estimate and decode (quantize) self-contamination $s_B(n)$ and then use the decoded $s_B(n)$ in conjunction with $s_t(n)$ as pseudo-training. For details, see [4, Sec. IV].

3.2. Under Attack

3.2.1. Projection Orthogonal to Training

Stack P consecutive samples of ℓth component $y_\ell(n)$ of $\mathbf{y}(n)$ into a column:

$$\underbrace{y_\ell(1)\ \cdots\ y_\ell(P)}_{\mathbf{y}^\ell(1)}\ \underbrace{y_\ell(P+1)\ \cdots\ y_\ell(2P)}_{\mathbf{y}^\ell(2)}\cdots$$

Define $\mathbf{v}^\ell(m)$ from $v_\ell(n)$, the ℓth component $\mathbf{v}(n)$ in a similar fashion. Let $\check{\mathbf{s}}_t = [s_t(1)\ s_t(2)\ \cdots\ s_t(P)]^\top$ and $\check{\mathbf{s}}_B(m) = [s_B(1+(m-1)P)\ \cdots\ s_B(P+(m-1)P)]^\top$. Then in the presence of self-contamination and eavesdropper, we have

$$\begin{aligned}\mathbf{y}^\ell(m) = &\left(\sqrt{P_B(1-\beta)}\,h_{B,\ell} + \sqrt{P_E}\,h_{E,\ell}\right)\check{\mathbf{s}}_t \\ &+ \sqrt{P_B\beta}\,h_{B,\ell}\check{\mathbf{s}}_B(m) + \mathbf{v}^\ell(m)\end{aligned}$$

where $h_{B,\ell}$ is the ℓth component of $\mathbf{h}_B$, and similarly for $h_{E,\ell}$. Let $\mathcal{P}^\perp_{\check{\mathbf{s}}_t}$ = projection orthogonal to the subspace spanned by $\check{\mathbf{s}}_t$. Then $\mathcal{P}^\perp_{\check{\mathbf{s}}_t}\mathbf{y}^\ell(m)$ has no contribution from training $s_t(n)$. "Reshape" $\mathcal{P}^\perp_{\check{\mathbf{s}}_t}\mathbf{y}^\ell(m)$ into a row vector along time and put all components ℓs together. Then the so "projected" $\mathbf{y}(n)$ lacks $s_t(n)$ but has the effect of $\mathbf{h}_B$ and $s_B(n)$ which can be used to estimate $\mathbf{h}_B$ up to a scale factor via eigen-decomposition. We elaborate on this approach in what follows.

We have

$$\mathcal{P}^\perp_{\check{\mathbf{s}}_t} = \mathbf{I}_P - P^{-1}\check{\mathbf{s}}_t\check{\mathbf{s}}_t^H \in \mathbb{C}^{P\times P}$$

where we have used $\check{\mathbf{s}}_t^H\check{\mathbf{s}}_t = P$. Since $\text{rank}(\mathcal{P}^\perp_{\check{\mathbf{s}}_t}) = P-1$, its SVD is

$$\mathcal{P}^\perp_{\check{\mathbf{s}}_t} = \mathbf{U}_1\Sigma_1\mathbf{V}_1^H,\quad \mathbf{U}_1, \mathbf{V}_1 \in \mathbb{C}^{P\times(P-1)}$$

where Σ_1 is diagonal with positive singular values along its diagonal. Consider

$$\begin{aligned}\mathbb{E}\{[\mathcal{P}^\perp_{\check{\mathbf{s}}_t}\mathbf{v}^\ell(m)][\mathcal{P}^\perp_{\check{\mathbf{s}}_t}\mathbf{v}^\ell(m)]^H\} &= \mathbf{U}_1\Sigma_1\mathbf{V}_1^H(\sigma_v^2\mathbf{I}_P)\mathbf{V}_1\Sigma_1\mathbf{U}_1^H \\ &= \sigma_v^2\mathbf{U}_1\Sigma_1^2\mathbf{U}_1^H \in \mathbb{C}^{P\times P}\end{aligned}$$

Noting that $\Sigma_1^{-1}\mathbf{U}_1^H\mathcal{P}^\perp_{\check{\mathbf{s}}_t} = \mathbf{V}_1^H$, consider the reduced dimension

$$\mathbf{v}^{\ell r}(m) := \mathbf{V}_1^H\mathbf{v}^\ell(m) \in \mathbb{C}^{P-1}.$$

Then we have $\mathbb{E}\{\mathbf{v}^{\ell r}(m)(\mathbf{v}^{\ell r}(m))^H\} = \sigma_v^2\mathbf{I}_{P-1}$. Note that $\mathbf{v}^{\ell r}(m_1)$ and $\mathbf{v}^{\ell r}(m_2)$ are independent for $m_1 \ne m_2$. Similarly, define the reduced dimension projected observations and contamination sequence

$$\mathbf{y}^{\ell r}(m) := \mathbf{V}_1^H\mathbf{y}^\ell(m),\quad \check{\mathbf{s}}_B^r(m) := \mathbf{V}_1^H\check{\mathbf{s}}_B(m).$$

Then we have for $m = 1, 2, \cdots, T/P$,

$$\mathbf{y}^{\ell r}(m) = \sqrt{P_B \beta}\, h_{B,\ell} \check{\mathbf{s}}_B^r(m) + \mathbf{v}^{\ell r}(m).$$

Now reshape $\mathbf{y}^{\ell r}(m)$, $m = 1, \cdots, T/P$, with T/P an integer, into a row of scalars $\tilde{y}_\ell(n)$, $n = 1, 2, \cdots, (T/P)(P-1)$, using the correspondence

$$\underbrace{\tilde{y}_\ell(1) \ \cdots \ \tilde{y}_\ell(P-1)}_{\mathbf{y}^{\ell r}(1)} \ \underbrace{\tilde{y}_\ell(P) \ \cdots \ \tilde{y}_\ell(2(P-1))}_{\mathbf{y}^{\ell r}(2)} \cdots$$

Similarly define $\tilde{v}_\ell(n)$ from $\mathbf{v}^{\ell r}(m)$, $m = 1, \cdots, T/P$, and similarly construct $\tilde{s}_B(n)$ from $\check{\mathbf{s}}_B^r(m)$. Then $\tilde{\mathbf{y}}(n) \in \mathbb{C}^{N_r}$ with ℓth component $\tilde{y}_\ell(n)$, satisfies

$$\tilde{\mathbf{y}}(n) = \sqrt{P_B \beta}\, \mathbf{h}_B \tilde{s}_B(n) + \tilde{\mathbf{v}}(n). \tag{8}$$

In the above model $\{\tilde{\mathbf{v}}(n)\}$ is i.i.d. zero-mean complex Gaussian with covariance $\sigma_v^2 \mathbf{I}_{P-1}$ and similarly $\tilde{s}_B(n)$ is uncorrelated zero-mean sequence with $\mathbb{E}\{|\tilde{s}_B(n)|^2\}$ not a function of n (follows just as the properties of $\tilde{\mathbf{v}}(n)$).

3.2.2. Channel Estimation

Consider (8) with $n = 1, 2, \cdots, n_b(P-1)$, where $n_b = T/P$= an integer. Then with $n_b(P-1) =: T'$, as in (5),

$$\mathbf{R}_{\tilde{y}} = \frac{1}{T'} \sum_{n=1}^{T'} \mathbb{E}\{\tilde{\mathbf{y}}(n)\tilde{\mathbf{y}}^H(n)\} = \beta P_B \mathbf{h}_B \mathbf{h}_B^H + \sigma_v^2 \mathbf{I}_{N_r}$$

where $\mathbb{E}\{|s_B(n)|^2\} = 1 = \mathbb{E}\{|\tilde{s}_B(n)|^2\}$. Hence we estimate $\mathbf{h}_B$ up to a complex constant as the unit norm eigenvector $\mathbf{v}_1$ corresponding to the largest eigenvalue of $\widehat{\mathbf{R}}_{\tilde{y}} = (1/T') \sum_{n=1}^{T'} \tilde{\mathbf{y}}(n)\tilde{\mathbf{y}}^H(n)$. Since $\mathbf{h}_B \approx c\mathbf{v}_1$ for some complex c, we pick c to minimize

$$\frac{1}{T} \sum_{n=1}^{T} \|\mathbf{y}(n) - c\mathbf{v}_1 \sqrt{(1-\beta)P_B} s_t(n)\|^2,$$

leading to the solution

$$\hat{c} = \frac{1}{\sqrt{(1-\beta)P_B T}} \sum_{n=1}^{T} (\mathbf{v}_1^H \mathbf{y}(n)) s_t^*(n).$$

Then we have the estimate of $\mathbf{h}_B$ as

$$\hat{\mathbf{h}}_B = \hat{c}\mathbf{v}_1. \tag{9}$$

For "large" T, we have $\mathbf{v}_1 = \mathbf{h}_B/\|\mathbf{h}_B\|$ and

$$\lim_{T\to\infty} \hat{c} = \mathbf{v}_1^H \mathbf{h}_B + \sqrt{\frac{P_E}{P_B(1-\beta)}} \mathbf{v}_1^H \mathbf{h}_E.$$

Using $\mathbf{y}(n) = \left(\sqrt{P_B(1-\beta)}\, \mathbf{h}_B + \sqrt{P_E}\, \mathbf{h}_E\right) s_t(n) + \sqrt{P_B \beta}\, \mathbf{h}_B s_B(n) + \mathbf{v}(n)$ under $\mathcal{H}_1$, we estimate the composite channel $\mathbf{h}_c := \sqrt{P_B(1-\beta)}\, \mathbf{h}_B + \sqrt{P_E}\, \mathbf{h}_E$ using the training sequence $s_t(n)$ and least-squares, as

$$\hat{\mathbf{h}}_c = \frac{1}{T} \sum_{n=1}^{T} \mathbf{y}(n) s_t^*(n). \tag{10}$$

This an unbiased estimator of $\mathbf{h}_c$. Using (9) and (10), we have the estimate of Eve's channel (with unknown $\sqrt{P_E}$ part of the estimate) as

$$\hat{\mathbf{h}}_E = \hat{\mathbf{h}}_c - \sqrt{P_B(1-\beta)} \hat{\mathbf{h}}_B. \tag{11}$$

4. MATCHED FILTER BEAMFORMING

Let $\{s_A(n)\}$, $\mathbb{E}\{|s_A(n)|^2\} = 1$, denote the scalar information sequence of Alice intended for Bob, and let $\mathbf{w} \in \mathbb{C}^{N_r}$ denote the unit norm beamforming vector of Alice. Then Alice transmits $\sqrt{P_A}\mathbf{w}\, s_A(n)$ where P_A is the transmit power. The received signals at Bob and Eve are given, respectively, by

$$y_B(n) = \sqrt{P_A} \mathbf{h}_B^\top \mathbf{w}\, s_A(n) + v_B(n) \tag{12}$$

$$y_{AE}(n) = \sqrt{P_A} \mathbf{h}_E^\top \mathbf{w}\, s_A(n) + v_E(n), \tag{13}$$

where we have used channel reciprocity, $v_E(n) \sim \mathcal{N}_c(0, \sigma_E^2)$ and $v_B(n) \sim \mathcal{N}_c(0, \sigma_B^2)$ are additive white Gaussian noise at Eve's and Bob's receivers. For MF reception at Bob, Alice should pick $\mathbf{w}$ as $\mathbf{h}_B^*/\|\mathbf{h}_B\|$ if $\mathbf{h}_B$ is known [11, 12], but instead uses the estimated channel to pick

$$\mathbf{w}_* = \widehat{\mathbf{h}}_B^*/\|\widehat{\mathbf{h}}_B\|. \tag{14}$$

The choice $\mathbf{w} = \mathbf{h}_B^*/\|\mathbf{h}_B\|$ maximizes the SNR at Bob since $|\mathbf{h}_B^\top \mathbf{w}| \le \|\mathbf{h}_B\|\, \|\mathbf{w}\|$ with equality iff $\mathbf{w} = c\mathbf{h}_B^*$ for some constant c.

The SNRs at Bob and Eve, respectively, are $\mathrm{SNR}_B = P_A|\mathbf{h}_B^\top \mathbf{w}_*|^2/\sigma_B^2$, $\mathrm{SNR}_E = P_A|\mathbf{h}_E^\top \mathbf{w}_*|^2/\sigma_E^2$. If a Gaussian codebook is used for $\{s_A(n)\}$, the achievable rates at Bob and Eve, respectively, are $R_B = \log_2(1 + \mathrm{SNR}_B)$ and $R_E = \log_2(1 + \mathrm{SNR}_E)$ and the secrecy rate at Bob is

$$R_{B,sec} = \max(R_B - R_E, 0). \tag{15}$$

In the presence of Eve with channel $\mathbf{h}_E$, the beamformer $\mathbf{w}$ may be picked to maximize $R_{B,sec}$. By [13, Theorem 2], the optimal beamformer $\mathbf{w}_*$ is given by the (unit-norm) generalized eigenvector corresponding to the largest generalized eigenvalue of the matrix pair

$$\left(\mathbf{I}_{N_r} + \mathbf{h}_B^* \mathbf{h}_B^\top/\sigma_B^2,\ \mathbf{I}_{N_r} + \mathbf{h}_E^* \mathbf{h}_E^\top/\sigma_E^2\right). \tag{16}$$

Under high SNR, the above solution approaches the solution to the optimization problem [13, Cor. 1]

$$\max_{\mathbf{w}} \ |\mathbf{h}_B^\top \mathbf{w}| \quad \text{subject to } \mathbf{h}_E^\top \mathbf{w} = 0,\ \|\mathbf{w}\| = 1.$$

The solution to this optimization problem is given by

$$\mathbf{w}_* = \frac{\left(\mathbf{I}_{N_r} - \mathbf{h}_E^* \mathbf{h}_E^\top/\|\mathbf{h}_E\|^2\right) \mathbf{h}_B^*}{\|\left(\mathbf{I}_{N_r} - \mathbf{h}_E^* \mathbf{h}_E^\top/\|\mathbf{h}_E\|^2\right) \mathbf{h}_B^*\|}. \tag{17}$$

In practice, we replace $\mathbf{h}_B$ and $\mathbf{h}_E$ with their estimates. The constraint $\mathbf{h}_E^\top \mathbf{w} = 0$ implies that $\mathbf{w}$ lies in a subspace orthogonal to $\mathbf{h}_E^*$, i.e., for some $\mathbf{w}_0$, $\mathbf{w} = \mathcal{P}_{\mathbf{h}_E^*}^{\perp} \mathbf{w}_0 = \left(\mathbf{I}_{N_r} - \mathbf{h}_E^* \mathbf{h}_E^\top / \|\mathbf{h}_E\|^2\right) \mathbf{w}_0$. With $\tilde{\mathbf{h}}_B := (\mathcal{P}_{\mathbf{h}_E^*}^{\perp})^\top \mathbf{h}_B$, $|\tilde{\mathbf{h}}_B^\top \mathbf{w}_0|$ is maximized w.r.t. $\mathbf{w}_0$, $\|\mathbf{w}_0\| = 1$, by the solution in (17).

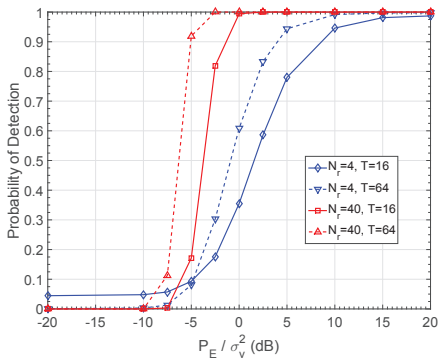

Fig. 1: Probability of attack detection as a function of Eve's power P_E relative to noise power σ_v^2 when Bob's power is fixed at $P_B/\sigma_v^2 = 10$dB, β=0.4 .

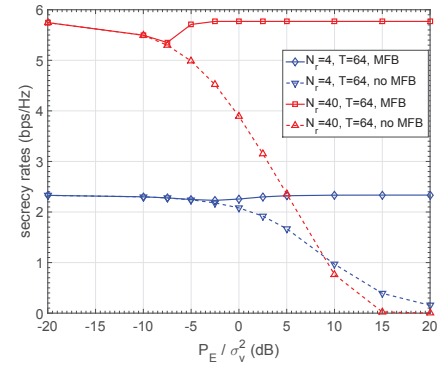

Fig. 2: Secrecy rate at Bob using the beamformers discussed in Sec. 4 as a function of Eve's power P_E. All parameters as for Fig. 1. The label "MFB" refers to matched filter beamforming of Sec. 4; "no MFB" means ones uses (14) with Eve ignored in channel estimation. $P_A = 1$, $\sigma_B^2 = \sigma_E^2 = 0.1$

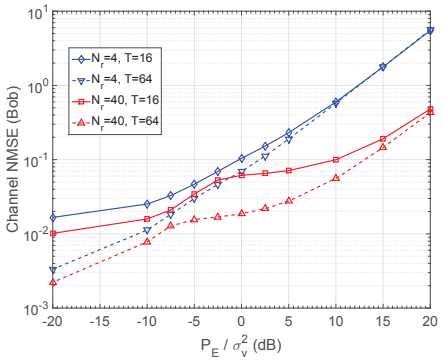

Fig. 3: Channel normalized MSE for Bob's channel as a function of Eve's power P_E. All parameters as for Fig. 1.

5. SIMULATION EXAMPLES

We consider Rayleigh flat-fading channels with path losses $d_B = d_E = 1$, noise power σ_v^2, training power budget P_B at Bob is such that $P_B/\sigma_v^2 = 10$dB, training power budget P_E at Eve is such that P_E/σ_v^2 varies from -20dB through 20dB, and fractional allocation β of training power at Bob to random sequence $s_B(n)$ is 0.4 . Bob and Eve have single antennas while Alice has $N_r = 4$ or 40 antennas. The training sequence is selected as periodic extension of a (binary) Hadamard sequence of length $P = 2^4 = 16$ and the random sequences $\{s_{B_i}(n)\}$ were i.i.d. QPSK. Fig. 1 shows our detection probability P_d results averaged over 5000 runs under pilot contamination attack for various parameter choices when $P_B/\sigma_v^2 = 10dB$. The performance improves with increasing T, N_r and Eve's power P_E.

The secrecy rate results of matched filter beamforming as discussed in Sec. 4 are shown in Fig. 2, with the corresponding normalized channel estimation MSE (mean-square error) $\|\widehat{\mathbf{h}}_B - \mathbf{h}_B\|^2/\|\mathbf{h}_B\|^2$ and $\|\widehat{\mathbf{h}}_E - \mathbf{h}_E\|^2/\|\mathbf{h}_E\|^2$ shown in Figs. 3 and 4, respectively, all averaged over 5000 runs. If Eve's presence is not detected, we use (14). If Eve is detected, after joint channel estimation, we use the generalized eigenvector of (16) with largest eigenvalue. In our simulations, we did not see any discernible difference between this solution and (17). It is seen from Fig. 2 that secure beamforming yields a secrecy rate performance as a function of P_E that is almost invariant to the presence/absence of pilot spoofing attack.

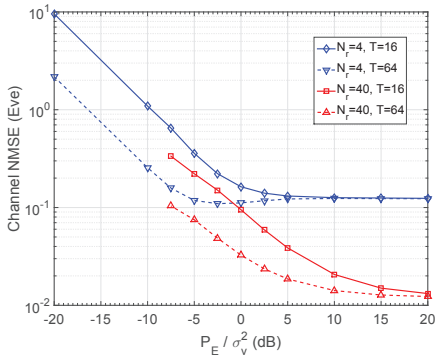

Fig. 4: Channel normalized MSE for Eve's channel as a function of Eve's power P_E. All parameters as for Fig. 1.

6. CONCLUSIONS

A novel approach to detection of pilot contamination attack in a 3-node TDD system was recently presented in [4] where attack mitigation was not addressed. In this paper In this paper we augmented the approach of [4] with joint (Bob and Eve) channel estimation and secure beamforming to mitigate the effects of pilot spoofing. The proposed approach was illustrated by numerical examples which show a secrecy rate performance that is almost invariant to the presence/absence of pilot spoofing attack.

7. REFERENCES

[1] X. Zhou, B. Maham and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 903-907, March 2012.

[2] D. Kapetanovic, G. Zheng, K-K. Wong and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. 2013 IEEE 24th Intern. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*, pp. 13-18, London, UK, Sept. 8-11, 2013.

[3] Q. Xiong, Y-C. Liang, K.H. Li and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Information Forensics & Security*, vol. 10, pp. 932-940, May 2015.

[4] J.K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems ," *IEEE Wireless Communications Letters*, vol. 4, No. 5, pp. 525-528, Oct. 2015.

[5] Q. Xiong, Y-C. Liang, K.H. Li and Y. Gong, "Secure transmission against pilot spoofing attack: A two-way training-based scheme," *IEEE Trans. Information Forensics & Security*, vol. 11, pp. 1017-1026, May 2016.

[6] J.K. Tugnait, "Detection of pilot contamination attack in TDD/SDMA systems," in *Proc. 2016 IEEE Intern. Conf. Acoustics, Speech & Signal Processing (ICASSP 2016)*, pp. 3576-3580, Shanghai, China, March 20-25, 2016.

[7] R. Miller and W. Trappe, "On the vulnerabilities of CSI in MIMO wireless communication systems," *IEEE Trans. Mobile Computing*, vol. 8, pp. 1386-1398, Aug. 2012.

[8] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Trans. Acoustics, Speech, Signal Proc.*, vol. 33, no. 2, pp. 387-392, April 1985.

[9] F. Haddadi, M. Malek-Mohammadi, M.M. Nayebi and M.R. Aref, "Statistical performance analysis of MDL source enumeration in array processing," *IEEE Trans. Signal Processing*, vol. 58, no. 1, pp. 452-457, Jan. 2010.

[10] B. Nadler, "Nonparametric detection of signals by information theoretic criteria: Performance analysis and an improved estimator," *IEEE Trans. Signal Processing*, vol. 58, no. 5, pp. 2746-2756, May 2010.

[11] L. Lu, G.Y. Li, A.L. Swindlehurst, A. Ashikhmin and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Proc.*, vol. 8, no. 5, pp. 742-758, Oct. 2014.

[12] T. Lo, "Maximal ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458-1461, Oct. 1999.

[13] A. Khisti and G. Wornell, "Secure transmission with multiple antennas - I: The MISOME wiretap channel," *IEEE Trans. Information Theory,* vol. 56, pp. 3088-3104, July 2010.