DETECTION OF PILOT CONTAMINATION ATTACK IN T.D.D./S.D.M.A. SYSTEMS

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 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 precoder design, facilitating eavesdropping. We investigate superimposing a random sequence on the training sequence at the legitimate receivers and then using source enumeration methods to detect pilot contamination attack. The proposed method extends an existing TDD/TDMA uplink approach to TDD/SDMA uplink scenario. The detection performance is illustrated via simulations.

Index Terms— Physical layer security, pilot contamination attack, active eavesdropping, source enumeration.

1. INTRODUCTION

Broadcast nature of wireless networks makes them vulnerable to malicious attacks aimed at disrupting their operation, such as pilot contamination attacks [1], [2], where the eavesdropper actively disrupts the channel state information (CSI) training process so as to neutralize beamformer/precoder design. In physical layer security methods, full or partial knowledge of the CSI of the legitimate system is required [3]. This knowledge is typically acquired by channel estimation during the training phase before the information signal transmission. In a time-division duplex (TDD) multiple antenna system, the CSI can be acquired using reverse training.

Consider a TDD system with SDMA (space-division multiple access) uplink and downlink, with a base station Alice, equipped with N_r antennas, and several single antenna users (to be called Bobs: Bob 1, Bob 2, $\cdots$). Alice designs its transmit beamformer/precoder based upon its channel to Bobs for improved performance. For a TDD system, the downlink and uplink channels can be assumed to be reciprocal so that Alice can learn its CSI to Bobs via Bobs' training of Alice. Therefore, each Bob sends its unique pilot (training) signal to Alice during the training phase of the slotted TDD system. If a publicly known protocol is used where the pilot sequences are publicly known, a malicious single-antenna terminal (eavesdropper) Eve can transmit the same pilot sequence during the training phase, thereby biasing the CSI estimated by Alice. In turn, the precoder designed on this basis could lead to a significant information leakage to Eve.

Relation to Prior Work: This issue of pilot contamination attack was first noted in [1] who investigates enhancing eavesdropper's performance. A diverse set of approaches are discussed in [2, 4, 5] for detection of the attack assuming a TDMA (time-division multiple access) uplink requiring separate time slots for each usr Bob. In this paper we consider SDMA uplink to allow for simultaneous transmission of training from Bobs.

Contributions: We extend the TDD/TDMA uplink approach of [5] to TDD/SDMA uplink scenario. The training sequences of various legitimate users are selected to be orthogonal. The proposed approach is analyzed and illustrated via simulations.

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

We consider K_B single antenna legitimate users ("Bobs"), with $s_{t,i}(n)$, $1 \le n \le T$, denoting the scalar training sequence of the ith user, of length T time samples. Suppose there are $K_E \le K_B$ potential single antenna eavesdroppers. An eavesdropper will try to spoof a legitimate user by transmitting the user's training sequence; that is, in our model, each potential eavesdropper is associated with a legitimate user in that the former uses the latter's training signal. Consider a flat Rayleigh fading environment with Bob i-to-Alice channel denoted as $\mathbf{h}_{B_i} \in \mathbb{C}^{N_r \times 1}$ and Eve i-to-Alice channel denoted as $\mathbf{h}_{E_i} \in \mathbb{C}^{N_r \times 1}$, where $\mathbf{h}_{B_i} \sim \mathcal{N}_c(0, \sigma^2_{B_i}\mathbf{I}_{N_r})$ and $\mathbf{h}_{E_i} \sim \mathcal{N}_c(0, \sigma^2_{E_i}\mathbf{I}_{N_r})$ represent fading. Let P_{B_i} and P_{E_i} denote the average training power allocated by Bob i and Eve i, respectively. In the absence of any transmission from any Eve, the received signal at Alice during the training phase is given by

$$\mathbf{y}(n) = \sum_{i=1}^{K_B} \sqrt{P_{B_i}}\, \mathbf{h}_{B_i} s_{t,i}(n) + \mathbf{v}(n) \qquad (1)$$

where additive noise $\mathbf{v}(n) \sim \mathcal{N}_c(0, \sigma_v^2 \mathbf{I}_{N_r})$ and the training sequences are periodic with period P and orthogonal satisfying

$$P^{-1} \sum_{n=1}^{P} s_{t,i}(n) s_{t,j}^*(n) = \delta_{i,j} = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases} \tag{2}$$

Let $\mathcal{E} \subseteq [1, K_B]$ denote the set of active eavesdroppers. When Eves also transmit (Eve's pilot contamination attack), the received signal at Alice during the training phase is

$$\begin{aligned} \mathbf{y}(n) &= \sum_{i=1}^{K_B} \left(\sqrt{P_{B_i}}\, \mathbf{h}_{B_i} + \sqrt{P_{E_i}}\, \mathbf{h}_{E_i} \mathbf{1}_{\{i \in \mathcal{E}\}} \right) s_{t,i}(n) + \mathbf{v}(n) \\ &= \sum_{i=1}^{K_B} \tilde{\mathbf{h}}_i s_{t,i}(n) + \mathbf{v}(n) \end{aligned} \tag{3}$$

where $\tilde{\mathbf{h}}_i = \sqrt{P_{B_i}}\, \mathbf{h}_{B_i} + \sqrt{P_{E_i}}\, \mathbf{h}_{E_i} \mathbf{1}_{\{i \in \mathcal{E}\}}$. In case of Eve's attack, based on (3), Alice would estimate $\tilde{\mathbf{h}}_i$ as Bob i-to-Alice channel, instead of $\sqrt{P_{B_i}}\, \mathbf{h}_{B_i}$ based on (1).

The problem addressed in this paper is: how to detect Eves' attack based only on the knowledge of $s_{t,i}(n)$ and $\mathbf{y}(n)$.

3. SELF-CONTAMINATION AT BOBS

Our proposed solution to the detection problem is to perform source enumeration using the information theoretic minimum description length (MDL) algorithm [6, 7, 8]. We propose to allocate a fraction β of the training power P_{B_i} at Bob i to a scalar random sequence $\{s_{B_i}(n)\}$ to be transmitted by Bob along with (superimposed on) $s_{t,i}(n)$; it can be the information sequence of Bob i. We assume that $\{s_{B_i}(n)\}$s are mutually independent random sequences, zero-mean, i.i.d., normalized to have $T^{-1} \sum_{n=1}^{T} |s_{B_i}(n)|^2 = 1$, finite alphabet: BPSK or QPSK, e.g. Thus, instead of $\sqrt{P_{B_i}} s_{t,i}(n)$, Bob i transmits ($0 \leq \beta < 1, \;\; n = 1, 2, \cdots, T$)

$$\tilde{s}_{B_i}(n) = \sqrt{P_{B_i}(1-\beta)}\, s_{t,i}(n) + \sqrt{P_{B_i}\beta}\, s_{B_i}(n). \tag{4}$$

The sequences $\{s_{B_i}(n)\}$ are unknown to Alice (and to Eves) and it can not be replicated in advance as they are random sequences generated at Bobs. However, Alice knows that such $\{s_{B_i}(n)\}$ is to be expected in $\mathbf{y}(n)$.

Now we have the following two hypotheses in a binary statistical hypothesis testing problem framework, for the received signal at Alice with $\mathcal{H}_0$ denoting the null hypothesis that there is no attack, and $\mathcal{H}_1$ denoting the alternative that at least one of the eavesdroppers attack is present:

$$\begin{aligned} \mathcal{H}_0 \; : \quad & \mathbf{y}(n) = \textstyle\sum_{i=1}^{K_B} \mathbf{h}_{B_i} \tilde{s}_{B_i}(n) + \mathbf{v}(n) \\ \mathcal{H}_1 \; : \quad & \mathbf{y}(n) = \textstyle\sum_{i=1}^{K_B} \left[\mathbf{h}_{B_i} \tilde{s}_{B_i}(n) \right. \\ & \qquad \left. + \sqrt{P_{E_i}}\, \mathbf{h}_{E_i} s_{t,i}(n) \mathbf{1}_{\{i \in \mathcal{E}\}} \right] + \mathbf{v}(n). \end{aligned} \tag{5}$$

We will model the sequences $\{s_{t,i}(n)\}$ and $\{s_{B,i}(n)\}$ as deterministic signals for source enumeration discussed later [7]. Then under $\mathcal{H}_0$, $\mathbf{y}(n) \sim \mathcal{N}_c(\sum_{i=1}^{K_B} \mathbf{h}_{B_i} \tilde{s}_{B_i}(n), \sigma_v^2 \mathbf{I}_{N_r})$, and under $\mathcal{H}_1$, $\mathbf{y}(n) \sim \mathcal{N}_c(\sum_{i=1}^{K_B} \left[\mathbf{h}_{B_i} \tilde{s}_{B_i}(n) + \sqrt{P_{E_i}}\, \mathbf{h}_{E_i} s_{t,i}(n) \mathbf{1}_{\{i \in \mathcal{E}\}} \right], \sigma_v^2 \mathbf{I}_{N_r})$.

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

$$\mathbf{R}_{y,\ell} = T^{-1} \sum_{n=1}^{T} \mathbb{E} \left\{ \mathbf{y}(n) \mathbf{y}^H(n) \,\middle|\, \mathcal{H}_\ell \right\} \tag{6}$$

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

$$\mathbf{R}_{s,\ell} = T^{-1} \sum_{n=1}^{T} \mathbb{E} \left\{ [\mathbf{y}(n) - \mathbf{v}(n)][\mathbf{y}(n) - \mathbf{v}(n)]^H \,\middle|\, \mathcal{H}_\ell \right\}. \tag{7}$$

Then we have

$$\mathbf{R}_{y,\ell} = \mathbf{R}_{s,\ell} + \sigma_v^2 \mathbf{I}_{N_r}, \quad \ell = 0, 1. \tag{8}$$

In addition to (2), the following two relations hold w.p.1 and in mean-square (m.s.) for "large" T:

$$\lim_{T \to \infty} T^{-1} \sum_{n=1}^{T} s_{B_i}(n) s_{B_j}^*(n) = \delta_{i,j}, \tag{9}$$

$$\lim_{T \to \infty} T^{-1} \sum_{n=1}^{T} s_{B_i}(n) s_{t,j}^*(n) = 0. \tag{10}$$

Define

$$\mathbf{H}_0 = \left[\mathbf{h}_{B_1} \; \mathbf{h}_{B_2} \; \cdots \; \mathbf{h}_{B_{K_B}} \right] \in \mathbb{C}^{N_r \times K_B} \tag{11}$$

$$\tilde{\mathbf{s}}_B(n) = \left[\tilde{s}_{B_1}(n) \; \tilde{s}_{B_2}(n) \; \cdots \; \tilde{s}_{B_{K_B}}(n) \right]^\top \in \mathbb{C}^{K_B \times 1} \tag{12}$$

Then under $\mathcal{H}_0$, $\mathbf{y}(n) = \mathbf{H}_0 \tilde{\mathbf{s}}_B(n) + \mathbf{v}(n)$ and

$$\mathbf{R}_{s,0} = \mathbf{H}_0 \mathbf{D}_0 \mathbf{H}_0^H, \quad \mathbf{D}_0 \in \mathbb{C}^{K_B \times K_B}, \tag{13}$$

where, using (2), (9) and (10), for "large" T

$$\left[\mathbf{D}_0 \right]_{ij} = T^{-1} \sum_{n=1}^{T} \tilde{s}_{B_i}(n) \tilde{s}_{B_j}^*(n) \approx \sqrt{P_{B_i} P_{B_j}}\, \delta_{i,j}. \tag{14}$$

Thus, $\text{rank}(\mathbf{R}_{s,0}) = K_B$ w.p.1 for $N_r \geq K_B$ since $\text{rank}(\mathbf{H}_0) = K_B$ w.p.1.

Now consider the hypothesis $\mathcal{H}_1$. Suppose that $|\mathcal{E}| = K_E$= number of eavesdroppers. Without loss of generality, let us reindex the user identities such that first K_E users are targeted by the eavesdroppers and the remaining $K_B - K_E \geq 0$ are not. That is, under $\mathcal{H}_1$, $\mathbf{y}(n) = \sum_{i=1}^{K_E} \left(\mathbf{h}_{B_i} \tilde{s}_{B_i}(n) + \sqrt{P_{E_i}}\, \mathbf{h}_{E_i} s_{t,i}(n) \right)$
$+ \sum_{i=K_E+1}^{K_B} \mathbf{h}_{B_i} \tilde{s}_{B_i}(n) + \mathbf{v}(n)$. Define

$$\begin{aligned} \tilde{\mathbf{s}}(n) = \big[& s_{t,1}(n) \; s_{B_1}(n) \; \cdots \; s_{t,K_E}(n) \; s_{B_{K_E}}(n) \; \cdots \\ & \tilde{s}_{B_{K_E+1}}(n) \; \cdots \; \tilde{s}_{B_{K_B}}(n) \big]^\top \in \mathbb{C}^{(K_E+K_B) \times 1} \end{aligned} \tag{15}$$

$$\mathbf{g}_i = \begin{cases} \sqrt{P_{B_\ell}(1-\beta)} \mathbf{h}_{B_\ell} & \\ \quad + \sqrt{P_{E_\ell}} \mathbf{h}_{E_\ell}, & i = 2\ell - 1, \; \ell \in [K_E] \\ \sqrt{P_{B_\ell} \beta} \mathbf{h}_{B_\ell} & i = 2\ell, \; \ell \in [K_E] \\ \mathbf{h}_{B_\ell} & i > 2K_E, \; \ell = i - 2K_E \end{cases} \tag{16}$$

$$\mathbf{H}_1 = \big[\mathbf{g}_1\ \mathbf{g}_2\ \cdots\ \mathbf{g}_{K_E+K_B}\big] \in \mathbb{C}^{N_r\times(K_E+K_B)}. \quad (17)$$

Then under $\mathcal{H}_1$, we have

$$\mathbf{R}_{s,1} = \mathbf{H}_1\Big(T^{-1}\sum_{n=1}^{T}\mathbf{s}(n)\mathbf{s}^H(n)\Big)\mathbf{H}_1^H = \mathbf{H}_1\mathbf{D}_1\mathbf{H}_1^H \quad (18)$$

where

$$\big[\mathbf{D}_1\big]_{ij} \approx \begin{cases} 0 & i\neq j \\ 1 & i=j\le 2K_E \\ P_{B_i} & i=j>2K_E \end{cases} \quad (19)$$

Therefore, rank$(\mathbf{R}_{s,1}) = K_E+K_B$ w.p.1 for $N_r \ge K_E+K_B$ since rank$(\mathbf{H}_1) = K_E+K_B$ w.p.1.

Thus, introduction of $\{s_{B_i}(n)\}$ by K_B legitimate users Bobs (as opposed to pilot contamination by Eve) leads to signal subspace of rank K_E+K_B in the presence of Eves' attack. If $\beta = 0$, then rank$(\mathbf{R}_{s,1}) = K_B$. Let the ordered (in decreasing magnitude) nonzero eigenvalues of $\mathbf{R}_{s,0}$ and $\mathbf{R}_{s,1}$ be denoted as $\lambda_{1,0} \ge \lambda_{2,0} \ge \cdots \ge \lambda_{K_B,0} > 0$ and $\lambda_{1,1} \ge \lambda_{2,1} \ge \cdots \ge \lambda_{K_B+K_E,1} > 0$, respectively. Then the N_r eigenvalues of $\mathbf{R}_{y,i}$ are

$$(\lambda_{1,0}+\sigma_v^2,\cdots,\lambda_{K_B,0}+\sigma_v^2,\sigma_v^2,\cdots,\sigma_v^2) \text{ for } i=0 \quad (20)$$

$$(\lambda_{1,1}+\sigma_v^2,\cdots,\lambda_{K_B+K_E,1}+\sigma_v^2,\sigma_v^2,\cdots,\sigma_v^2) \text{ for } i=1. \quad (21)$$

One can distinguish between the two hypotheses using the MDL criterion [6, 7, 8] for estimation of the signal subspace dimension d (i.e., rank d) provided that $N_r > d$ (number of sensors greater than number of sources). Since $d = K_B$ or K_B+K_E, we need $N_r \ge 2(K_B+K_E)+1$ for the MDL estimator of d [6, 7, 8]. The MDL estimator is discussed next.

3.1. MDL Source Enumeration for Attack Detection

Define the sample correlation matrix of T observations as

$$\widehat{\mathbf{R}}_y = T^{-1}\sum_{n=1}^{T}\mathbf{y}(n)\mathbf{y}^H(n). \quad (22)$$

Let the ordered eigenvalues of $\widehat{\mathbf{R}}_y$ be denoted by $\ell_1 \ge \ell_2 \ge \cdots \ge \ell_{N_r}$. The MDL estimator of the signal subspace dimension d is given by [6, 7, 8]

$$\widehat{d} = \arg\min_{1\le d\le N_r-1}\mathrm{MDL}(d) \quad (23)$$

where

$$\mathrm{MDL}(d) = -\sum_{i=d+1}^{N_r}\ln(\ell_i) + (N_r-d)\ln\left(\frac{1}{N_r-d}\sum_{i=d+1}^{N_r}\ell_i\right) + \frac{d(2N_r-d)\ln(T)}{2T}. \quad (24)$$

We reformulate the hypotheses (5) as

$$\begin{array}{ll}\mathcal{H}_0: & \mathrm{rank}(\mathbf{R}_{s,0}) = d = K_B \\ \mathcal{H}_1: & \mathrm{rank}(\mathbf{R}_{s,1}) = d > K_B\end{array} \quad (25)$$

but instead of solving it in the traditional detection theoretic sense (maximize probability of detection subject to an upper-bound on the probability of false alarm), we use the MDL method to determine d, the signal subspace dimension. Following (25), if $\widehat{d} = K_B$, declare no attack, and if $\widehat{d} > K_B$, we have a pilot contamination attack. The MDL method needs no threshold calculation.

4. ITERATIVE CHANNEL ESTIMATION

If the MDL method indicates absence of any attack, Alice proceeds to initially estimate the channel using (5) under $\mathcal{H}_0$, knowledge of $\{s_{t,i}(n)\}$, $i = 1,2,\cdots,K_B$, and the least-squares method. Define K_B-column vectors

$$\mathbf{s}_t(n) = \sqrt{1-\beta}\big[\sqrt{P_{B_1}}s_{t,1}(n)\ \cdots\ \sqrt{P_{B_{K_B}}}s_{t,K_B}(n)\big]^\top \quad (26)$$

$$\mathbf{s}_B(n) = \sqrt{\beta}\big[\sqrt{P_{B_1}}s_{B_1}(n)\ \cdots\ \sqrt{P_{B_{K_B}}}s_{B_{K_B}}(n)\big]^\top \quad (27)$$

With $\mathbf{s}_t(n)$ as the vector training sequence, we estimate $\mathbf{H}_0$ (see (11)) to minimize $\frac{1}{T}\sum_{n=1}^{T}\|\mathbf{y}(n)-\mathbf{H}_0\mathbf{s}_t(n)\|^2$ resulting in the estimate

$$\widehat{\mathbf{H}}_0 = \left[\frac{1}{T}\sum_{n=1}^{T}\mathbf{y}(n)\mathbf{s}_t^H(n)\right]\left[\frac{1}{T}\sum_{n=1}^{T}\mathbf{s}_t(n)\mathbf{s}_t^H(n)\right]^{-1} \approx \left[\frac{1}{(1-\beta)T}\sum_{n=1}^{T}\mathbf{y}(n)\mathbf{s}_t^H(n)\right]\Gamma_{P_B}^{-1} \quad (28)$$

where $\Gamma_{P_B} = \mathrm{diag}\{P_{B_1},\cdots,P_{B_{K_B}}\}$, a $K_B\times K_B$ diagonal matrix. This approach treats $\{\mathbf{s}_B(n)\}$ as interference which may lead to poor estimate for larger values of β. 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 $\mathbf{s}_B(n)$ and then use the decoded $\mathbf{s}_B(n)$ in conjunction with $\mathbf{s}_t(n)$ as pseudo-training. The linear MMSE equalizer $\mathbf{H}_{eq} \in \mathbb{C}^{K_B\times N_r}$ to estimate $\tilde{\mathbf{s}}_B(n)$ (see (12)) as $\hat{\tilde{\mathbf{s}}}_B(n)$ is given by (after replacing $\mathbf{H}_0$ with $\widehat{\mathbf{H}}_0$)

$$\mathbf{H}_{eq} = \Gamma_{P_B}\widehat{\mathbf{H}}_0^H\left[\widehat{\mathbf{H}}_0\mathbf{D}_0\widehat{\mathbf{H}}_0^H + \sigma_v^2\mathbf{I}_{N_r}\right]^{-1}. \quad (29)$$

Then we have $\hat{\tilde{\mathbf{s}}}_B(n) = \mathbf{H}_{eq}\mathbf{y}(n)$. Removing the known contribution of $\mathbf{s}_t(n)$, set $\check{\mathbf{s}}_B(n) = \hat{\tilde{\mathbf{s}}}_B(n) - \mathbf{s}_t(n)$ and then quantize $(\beta\Gamma_{P_B})^{-0.5}\check{\mathbf{s}}_B(n)$ (and premultiply with $(\beta\Gamma_{P_B})^{0.5}$) to get the finite-alphabet decoded estimate $\hat{\mathbf{s}}_{Bq}(n)$ of $\mathbf{s}_B(n)$. The pseudo-training sequence $\{\tilde{\mathbf{s}}_{Bq}(n),\ n = 1,2,\cdots T\}$ is then given by $\tilde{\mathbf{s}}_{Bq}(n) = \mathbf{s}_t(n) + \hat{\mathbf{s}}_{Bq}(n)$. Using this pseudo-training we re-do the channel estimate as

$$\widehat{\mathbf{H}}_0 = \left[\frac{1}{T}\sum_{n=1}^{T}\mathbf{y}(n)\tilde{\mathbf{s}}_{Bq}^H(n)\right]\left[\frac{1}{T}\sum_{n=1}^{T}\tilde{\mathbf{s}}_{Bq}(n)\tilde{\mathbf{s}}_{Bq}^H(n)\right]^{-1} \quad (30)$$

Information Sequence Detection: If the sequences $\{s_{B_i}(n)\}$ are the information sequences of legitimate users $i = 1, 2, \cdots, K_B$, then we use the channel estimate (30) back in (29) to design an updated equalizer and then use it to get the finite-alphabet decoded estimate of $\{s_{B_i}(n)\}$.

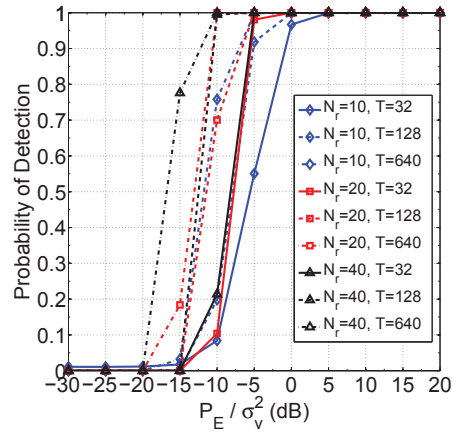

Fig. 1: Probability of attack detection as a function of Eve's power P_E (=P_{E_j} $\forall j$) relative to noise power σ_v^2 when Bob's power is fixed at $P_{B_i}/\sigma_v^2 = 10$dB $\forall i$: K_B=6= # of legitimate users, K_E=2= # of eavesdroppers, β=0.9 implying 10% of power in T symbols is for training and 90% for data.

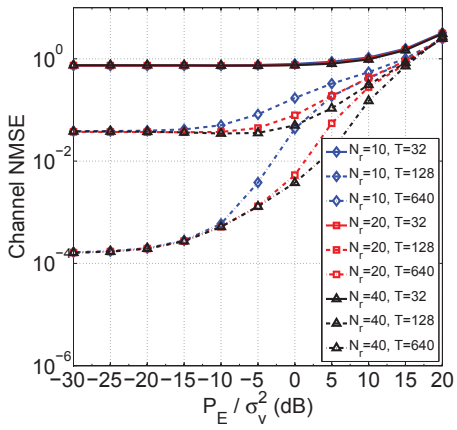

Fig. 2: Channel normalized MSE ($\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2/\|\mathbf{H}_0\|_F^2$, under the conditions of Fig. 1, where $\mathbf{H}_0$ as in (11), $\widehat{\mathbf{H}}_0$ as in (30)). Channel estimation is performed even if eavesdroppers are detected. β=0.9 implying 10% of power in T symbols is for training and 90% for data.

5. SIMULATION EXAMPLES

We consider $\mathbf{h}_{B_i} \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\mathbf{h}_{E_i} \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\forall i$, noise power σ_v^2, K_B=6= number of legitimate users, K_E=2= number of eavesdroppers, training power budget P_{B_i} at Bob i is such that $P_{B_i}/\sigma_v^2 = 10$dB $\forall i$, training power budget P_{E_j} at Eve j is such that P_{E_j}/σ_v^2 varies from -30dB through 20dB and is the same $\forall j$, and fractional allocation β of training power at Bob i to random sequence $s_{B_i}(n)$ is 0.9 . Bobs and Eves have single antennas while Alice has $N_r = 10$, 20 or 40 antennas. The training sequences are selected as periodic extensions of orthogonal (binary) Hadamard sequences of length $P = 2^5 = 32$ 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 $P_{B_i}/\sigma_v^2 = 10dB$ $\forall i$. The performance improves with increasing training sequence length T, number of receive antennas N_r and Eve's power P_E. The false-alarm rate P_{fa} was 0.0098 for $N_r = 10$, $T = 32$, and < 0.001 for all other parameter choices shown in Fig. 1. It is seen that the algorithm can detect "weak" eavesdroppers.

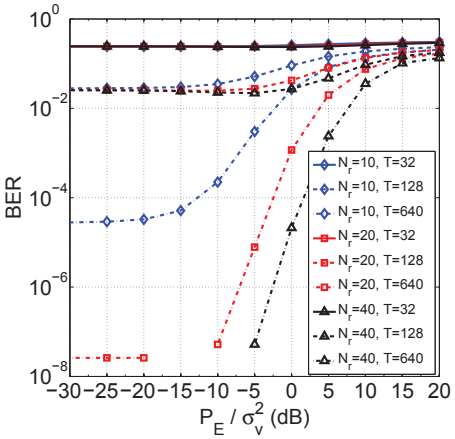

Fig. 3: Bit error rate averaged over all users, for QPSK superimposed information sequences, under the conditions of Fig. 2. β=0.9 implying 10% of power in T symbols is for training and 90% for data.

Channel estimation results in terms of normalized MSE $\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2/\|\mathbf{H}_0\|_F^2$, averaged over 5000 runs, are shown in Fig. 2 for the case of active attack (all parameters as for Fig. 1), where we used the iterative estimator (30). The performance improves with increasing superimposed training sequence length T and decreasing Eve's power P_E. From Figs. 1 and 2 we see that as eavesdropper's transmit power decreases, it is harder to detect its presence but correspondingly, channel MSE improves. The bit error rate (BER) results are shown in Fig. 3, averaged over 5000 runs, when information sequences are used as superimposed random self-contamination sequences. All other all parameters as for Fig. 2. The performance improves with increasing training sequence length T, increasing N_r, and decreasing Eve's power P_E.

6. CONCLUSIONS

We presented a novel approach to detection of pilot contamination attack in TDD/SDMA systems by extending the TDD/TDMA uplink approach of [5]. The proposed method was illustrated via simulations. The question of what alternative strategy or protocol should be employed once an attack is detected, was not addressed in this paper.

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] Y.-W. Hong, P.-C. Lan and C-C. Jay Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Proc. Mag.*, vol. 30, Issue 5, pp. 29-40, Sept. 2013.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.