DETECTION OF PILOT SPOOFING ATTACK OVER FREQUENCY SELECTIVE CHANNELS

Jitendra K. Tugnait

Department of Electrical & Computer Engineering
Auburn University, Auburn, AL 36849, USA
tugnajk@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 precoder/beamformimg design, facilitating eavesdropping. Past approaches to pilot spoofing detection are limited to flat fading channels. In this paper we propose a novel approach for detection of pilot spoofing attack over frequency selective channels, with unknown channels and channel lengths, except that an upperbound on the number of channel taps is assumed to be known. The proposed approach is illustrated by numerical examples and they show the efficacy of the proposed approach. A method to estimate Bob's channel regardless of the spoofing attack, is also presented and illustrated via simulations.

Index Terms— Physical layer security, pilot spoofing attack, active eavesdropping, channel estimation.

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 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, synchronized with Bob's training. Then the CSI estimated by Alice 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 spoofing/contamination attack [1–3].

Several types of eavesdropping have been identified and analyzed in the literature [3]. In passive eavesdropping, the eavesdropper does not transmit any signal of its own, but tries to intercept confidential communication between a legitimate transmitter-receiver pair. In active eavesdropping, the eavesdropper also transmits a signal of its own. If the intent is to disrupt the legitimate operation, active eavesdropping attack is more appropriately termed as a jamming attack [4, 5]. Such jamming attacks may occur during the training phase (pilot jamming), as in [4–6], and/or in the data phase, as in [4, 5]. The objective of a jamming attack is to degrade the overall legitimate system performance. Distinct from pilot jamming is the pilot spoofing or pilot contamination attack [1, 3, 7], where the eavesdropper Eve sends synchronized, identical training (pilot) signal as that of the legitimate user Bob. In contrast, in a pilot jamming attack, Eve's signal is a different pilot or not noise-like signal [6]. Eve's objective in pilot spoofing is to deceive Alice into treating the Alice-to-Eve channel as Alice-to-Bob channel. This paper is concerned with pilot spoofing attack issues.

Relation to Prior Work: All prior works on pilot spoofing detection [2, 3, 7–12] deal with flat fading environments. The assumption of flat fading is fundamental to these cited papers, and their solutions will not work in frequency selective channels. In this paper we address frequency selective channels with unknown channels and channel lengths, except an upperbound on the number of channel taps is assumed to be known. In contrast, all prior works such as [2, 3, 7–12], assume that channels are 1-tap channels.

Notation: Superscripts $(.)^*$, $(.)^\top$ and $(.)^H$ represent complex conjugate, transpose and complex conjugate transpose 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, and $\rho(\mathbf{A})$ denotes the rank of $\mathbf{A}$. 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 an MISO (multiple-input single-output) system with a multi-antenna transmitter Alice equipped with N_r antennas, a single antenna legitimate user Bob, and an eavesdropper Eve. Eve's objective in pilot spoofing is to deceive Alice into treating the Alice-to-Eve channel as Alice-to-Bob channel. Hence, the number of antennas at Eve must be the same as the number of antennas at Bob. Therefore, in our model, Eve also has a single antenna. Such a system model has also been been investigated in [2, 7–9], except that instead of considering flat fading channels, we consider frequency selective channels. Let $s_t(n)$, $1 \le n \le T$, denote the training sequence of length T time samples. Bob-to-Alice frequency selective channel impulse response is denoted as $\{\mathbf{h}_{B\ell}\}_{\ell=0}^{L_B-1}$ ($\mathbf{h}_{B\ell} \in \mathcal{C}^{N_r}$, L_B is the Bob's channel length (number of taps)), and Eve-to-Alice channel is denoted as $\{\mathbf{h}_{E\ell}\}_{\ell=0}^{L_E-1}$ ($\mathbf{h}_{E\ell} \in \mathcal{C}^{N_r}$, L_E is the Eve's channel length), where the impulse responses include both large-scale and small-scale fading effects. 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

$$\mathbf{y}(n) = \sqrt{P_B} \sum_{\ell=0}^{L_B-1} \mathbf{h}_{B\ell} s_t(n-\ell) + \mathbf{v}(n) \in \mathcal{C}^{N_r} \qquad (1)$$

This work was supported by NSF Grant ECCS-1651133.

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 pilot, the received signal at Alice during the training phase is ($\bar{L} = \max(L_B, L_E)$)

$$\mathbf{y}(n) = \sum_{\ell=0}^{\bar{L}-1} \left(\sqrt{P_B}\,\mathbf{h}_{B\ell} + \sqrt{P_E}\,\mathbf{h}_{E\ell}\right) s_t(n-\ell) + \mathbf{v}(n) \quad (2)$$

where $\mathbf{h}_{B\ell} = 0$ for $\ell \geq L_B$ and $\mathbf{h}_{E\ell} = 0$ for $\ell \geq L_E$. In case of Eve's attack, based on (2), Alice would estimate $\sqrt{P_B}\,\mathbf{h}_{B\ell} + \sqrt{P_E}\,\mathbf{h}_{E\ell}$, $\ell = 0, 1, \cdots$, as Bob-to-Alice channel, instead of $\sqrt{P_B}\,\mathbf{h}_{B\ell}$ based on (1).

2.1. Self-contamination at Bob

How to detect Eve's attack based only on the knowledge of $s_t(n)$ and $\mathbf{y}(n)$, is addressed in [8] for flat fading channels, 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 ($0 \leq \beta < 1$, $n = 1, 2, \cdots, T$)

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

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 $\mathbf{y}(n)$. In this case, in the absence of any transmission from Eve, the received signal at Alice during the training phase is given by

$$\mathbf{y}(n) = \mathbf{x}_0(n) + \mathbf{v}(n), \quad (4)$$

where

$$\mathbf{x}_0(n) = \sum_{\ell=0}^{L_B-1} \mathbf{h}_{B\ell}\tilde{s}_B(n-\ell)\,. \quad (5)$$

When Eve also transmits, we have

$$\mathbf{y}(n) = \mathbf{x}_1(n) + \mathbf{v}(n) \quad (6)$$

where

$$\mathbf{x}_1(n) = \sum_{\ell=0}^{L_B-1} \mathbf{h}_{B\ell}\tilde{s}_B(n-\ell) + \sqrt{P_E}\sum_{\ell=0}^{L_E-1} \mathbf{h}_{E\ell}s_t(n-\ell). \quad (7)$$

In this paper we extend the self-contamination approach of [8] to apply to frequency selective channels. Let $L_m \geq \bar{L} = \max(L_B, L_E)$ and $T_m = T - L_m + 1$. We do not assume knowledge of L_B or L_E, but an upperbound L_m on them is assumed to be known to Alice. Define the $L_m \times T_m$ matrix

$$\mathbb{U} = \begin{bmatrix} s_t(L_m) & s_t(L_m+1) & \cdots & s_t(T) \\ s_t(L_m-1) & s_t(L_m) & \cdots & s_t(T-1) \\ \vdots & \vdots & \ddots & \vdots \\ s_t(1) & s_t(2) & \cdots & s_t(T-L_m+1) \end{bmatrix} \quad (8)$$

We assume that $\{s_t(n)\}$ is such that $\rho(\mathbb{U}) = L_m$. It then follows that $\rho(\mathbb{U}\mathbb{U}^H) = L_m$. This is the persistence of excitation condition of order L_m [13, Def. 10.1], which is necessary and sufficient for unique estimation of channel tap gains (for number of taps $\leq L_m$) using the method of least squares.

3. ATTACK DETECTION

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

$$\begin{array}{ll} \mathcal{H}_0: & \mathbf{y}(n) = \mathbf{x}_0(n) + \mathbf{v}(n) \\ \mathcal{H}_1: & \mathbf{y}(n) = \mathbf{x}_1(n) + \mathbf{v}(n) \end{array}, n = 1, 2, \cdots, T. \quad (9)$$

3.1. Signal Subspace Dimension

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

$$\mathbf{R}_{y,i} = T_m^{-1}\sum_{n=L_m}^{T} \mathbb{E}\left\{\mathbf{y}(n)\mathbf{y}^H(n)\,\middle|\,\mathcal{H}_i\right\} \quad (10)$$

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

$$\mathbf{R}_{x,i} = T_m^{-1}\sum_{n=L_m}^{T} \mathbb{E}\left\{\mathbf{x}_i(n)\mathbf{x}_i^H(n)\,\middle|\,\mathcal{H}_i\right\}. \quad (11)$$

Then we have $\mathbf{R}_{y,i} = \mathbf{R}_{x,i} + \sigma_v^2\mathbf{I}_{N_r}$, $i = 0, 1$.

If $s_t(n)$ is non-random, using (5), we obtain

$$\mathbf{R}_{x,0} = P_B\mathbf{H}_B\left[(1-\beta)\mathbf{R}_{tB} + \beta\sigma_B^2\mathbf{I}_{L_B}\right]\mathbf{H}_B^H \quad (12)$$

where $\sigma_B^2 = \mathbb{E}\{|s_B(n)|^2\}$,

$$\mathbf{H}_B = \left[\mathbf{h}_{B0}\ \cdots\ \mathbf{h}_{B(L_B-1)}\right] \in \mathbb{C}^{N_r \times L_B} \quad (13)$$

$$[\mathbf{R}_{tB}]_{ij} = (ij)\text{th element of } \mathbf{R}_{tB} \in \mathbb{C}^{L_B \times L_B} \quad (14)$$

$$= T_m^{-1}\sum_{n=L_m}^{T} s_t(n-i+1)s_t^*(n-j+1)\,. \quad (15)$$

Note that (12) also holds if $\{s_t(n)\}$ is random and independent of $\{s_B(n)\}$. Since $\rho(\mathbb{U}) = L_m$ (see (8)), $\rho(\mathbf{R}_{tB}) = L_B$. (If $\{s_t(n)\}$ is i.i.d. random, $\mathbf{R}_{tB} = \sigma_t^2\mathbf{I}_{L_B}$, where $\sigma_t^2 = \mathbb{E}\{|s_t(n)|^2\}$.) We also assume that

$$\mathbf{h}^{(B)} = \left[\mathbf{h}_{B0}^H\ \cdots\ \mathbf{h}_{B(L_B-1)}^H\right]^H \in \mathbb{C}^{N_r L_B} \quad (16)$$

is a realization of a continuous random vector with positive-definite covariance matrix, implying that $\rho(\mathbf{H}_B) = L_B$ w.p.1 if $N_r \geq L_B$. Therefore, $\rho(\mathbf{R}_{x,0}) = L_B$ w.p.1 if $N_r \geq L_B$.

Similarly, using (7), we obtain

$$\mathbf{R}_{x,1} = [\mathbf{H}_C\ \ \mathbf{H}_B]\begin{bmatrix} \mathbf{R}_{tC} & 0 \\ 0 & \beta\sigma_B^2\mathbf{I}_{L_B} \end{bmatrix}\begin{bmatrix} \mathbf{H}_C^H \\ \mathbf{H}_B^H \end{bmatrix} \quad (17)$$

where

$$\mathbf{H}_C = \left[\mathbf{h}_{C0}\ \cdots\ \mathbf{h}_{C(\bar{L}-1)}\right] \in \mathbb{C}^{N_r \times \bar{L}} \quad (18)$$

$$\mathbf{h}_{C\ell} = \sqrt{(1-\beta)P_B}\,\mathbf{h}_{B\ell} + \sqrt{P_E}\,\mathbf{h}_{E\ell} \quad (19)$$

$$[\mathbf{R}_{tC}]_{ij} = (ij)\text{th element of } \mathbf{R}_{tC} \in \mathbb{C}^{\bar{L} \times \bar{L}} \quad (20)$$

$$= T_m^{-1}\sum_{n=L_m}^{T} s_t(n-i+1)s_t^*(n-j+1)\,. \quad (21)$$

Since $\rho(\mathbb{U}) = L_m$, $\rho(\mathbf{R}_{tC}) = \bar{L}$. We assume that

$$\mathbf{h}^{(E)} = \left[\mathbf{h}_{E0}^H\ \cdots\ \mathbf{h}_{E(L_E-1)}^H\right]^H \in \mathbb{C}^{N_r L_E}$$

is a realization of a continuous random vector with positive-definite covariance matrix, and it is independent of $\mathbf{h}^{(B)}$. Therefore, $\rho([\mathbf{H}_C \quad \mathbf{H}_B]) = L_B + L_E$ w.p.1 if $N_r \geq L_B + L_E$. Therefore, $\rho(\mathbf{R}_{x,1}) = L_B + L_E$ w.p.1 if $N_r \geq L_B + L_E$.

Thus, the ranks of the signal correlation matrix under the two hypotheses are different. Alice does not know the true values of L_B and L_E, only an upperbound L_m on them. Lack of knowledge of L_B and L_E precludes use of the approach of [8] (also used in [11, 12]), which relies on the knowledge that $L_B = L_E = 1$, i.e., the channels are flat-fading (1-tap). We propose an alternative next.

3.2. Projection Orthogonal to Training

Stack T_m consecutive samples of kth component $y_k(n)$ of $\mathbf{y}(n)$ into a column:

$$\mathbf{y}^k = [y_k(L_m) \;\; y_k(L_m+1) \;\cdots\; y_k(T)]^\top \in \mathbb{C}^{T_m}$$

Define $\mathbf{v}^k$ from $v_k(n)$, the kth component $\mathbf{v}(n)$, in a similar fashion. For $i = 0, 1, \cdots, L_m - 1$, let

$$\begin{aligned}\check{\mathbf{s}}_t(i) =&[s_t(L_m - i) \;\; s_t(L_m + 1 - i) \;\cdots\; s_t(T - i)]^\top\\ \check{\mathbf{s}}_B(i) =&[s_B(L_m - i) \;\; s_B(L_m + 1 - i) \;\cdots\; s_B(T - i)]^\top .\end{aligned}$$

Then in the presence of eavesdropper, we have

$$\begin{aligned}\mathbf{y}^k =& \sum_{\ell=0}^{\bar{L}-1} \left(\sqrt{P_B(1-\beta)}\,[\mathbf{h}_{B\ell}]_k + \sqrt{P_E}\,[\mathbf{h}_{E\ell}]_k\right)\check{\mathbf{s}}_t(\ell)\\ &+ \sum_{\ell=0}^{L_B-1} \sqrt{P_B\beta}\,[\mathbf{h}_{B\ell}]_k \check{\mathbf{s}}_B(\ell) + \mathbf{v}^k\end{aligned}$$

where $[\mathbf{h}_{B\ell}]_k$ is the kth component of $\mathbf{h}_{B\ell}$, and similarly for $[\mathbf{h}_{E\ell}]_k$. Finally define

$$\check{\mathbf{S}} = [\check{\mathbf{s}}_t(0) \;\cdots\; \check{\mathbf{s}}_t(L_m - 1)] \in \mathbb{C}^{T_m \times L_m}. \tag{22}$$

The training is such that $\rho(\check{\mathbf{S}}) = \rho(\mathbb{U}) = L_m$. Let $\mathcal{P}_{\check{\mathbf{S}}}^{\perp}$ = projection orthogonal to the subspace spanned by the columns of $\check{\mathbf{S}}$. Then $\mathcal{P}_{\check{\mathbf{S}}}^{\perp}\mathbf{y}^k$ has no contribution from training $s_t(n)$. "Reshape" $\mathcal{P}_{\check{\mathbf{S}}}^{\perp}\mathbf{y}^k$ into a row vector along time and put all components ks together. Then the so "projected" $\mathbf{y}(n)$ lacks $s_t(n)$ but has the effect of $\mathbf{h}_{B\ell}$s and $s_B(n)$.

We have (EVD stands for eigenvalue decomposition)

$$\mathcal{P}_{\check{\mathbf{S}}}^{\perp} = \mathbf{I}_{T_m} - \check{\mathbf{S}}(\check{\mathbf{S}}^H\check{\mathbf{S}})^{-1}\check{\mathbf{S}}^H \in \mathbb{C}^{T_m \times T_m} \tag{23}$$

$$\stackrel{EVD}{=} \mathbf{U}_1\mathbf{\Sigma}_1\mathbf{U}_1^H, \;\; \mathbf{U}_1 \in \mathbb{C}^{T_m \times (T_m - L_m)} \tag{24}$$

where $\mathbf{\Sigma}_1$ is diagonal with $T_m - L_m$ positive eigenvalues along its diagonal and we have used the fact that $\rho(\check{\mathbf{S}}) = L_m$, hence the orthogonal subspace is of rank $T_m - L_m$. Consider the reduced dimension vectors of dimension $T_m - L_m$:

$$\begin{aligned}&\mathbf{y}^{kr} := \mathbf{U}_1^H\mathbf{y}^k, \;\; \mathbf{v}^{kr} := \mathbf{U}_1^H\mathbf{v}^k,\\ &\check{\mathbf{s}}_t^r(i) := \mathbf{U}_1^H\check{\mathbf{s}}_t(i), \;\; \check{\mathbf{s}}_B^r(i) := \mathbf{U}_1^H\check{\mathbf{s}}_B(i).\end{aligned} \tag{25}$$

Then we have $\mathbb{E}\{\mathbf{v}^{kr}(\mathbf{v}^{kr})^H\} = \sigma_v^2\mathbf{I}_{T_m - L_m}$. Since $\mathcal{P}_{\check{\mathbf{S}}}^{\perp}\check{\mathbf{S}} = 0$ implies $\mathbf{U}_1^H\check{\mathbf{S}} = 0$, i.e., $\mathbf{U}_1^H\check{\mathbf{s}}_t(\ell) = 0$ for $0 \leq \ell \leq L_m - 1$, we have

$$\mathbf{y}^{kr} = \sum_{\ell=0}^{L_B-1} \sqrt{P_B\beta}\,[\mathbf{h}_{B\ell}]_k \check{\mathbf{s}}_B^r(\ell) + \mathbf{v}^{kr}.$$

Now reshape $\mathbf{y}^{kr}$ into a row of scalars $\tilde{y}_k(n)$, $n = L_m, \cdots, T_m$, as ($T_m' = T_m - L_m = T - 2L_m + 1$)

$$\mathbf{y}^{kr} = [\tilde{y}_k(L_m) \;\; \tilde{y}_k(L_m+1) \;\cdots\; \tilde{y}_k(T_m)]^\top \in \mathbb{C}^{T_m'}$$

Similarly define $\tilde{v}_k(n)$ from $\mathbf{v}^{kr}$, and $\tilde{s}_B^{ri}(n)$ from $\check{\mathbf{s}}_B^r(i)$. Then $\tilde{\mathbf{y}}(n) \in \mathbb{C}^{N_r}$ with kth component $\tilde{y}_k(n)$, satisfies

$$\tilde{\mathbf{y}}(n) = \underbrace{\sqrt{P_B\beta}\sum_{\ell=0}^{L_B-1}\mathbf{h}_{B\ell}\tilde{s}_B^{r\ell}(n)}_{=\tilde{\mathbf{x}}(n)} + \tilde{\mathbf{v}}(n). \tag{26}$$

Since $\mathbb{E}\{\mathbf{v}^{kr}(\mathbf{v}^{kr})^H\} = \sigma_v^2\mathbf{I}_{T_m - L_m}$, it follows that $\{\tilde{v}_k(n)\}_{n=L_m}^{T_m}$ is a zero-mean, i.i.d.,complex-Gaussian sequence, and since (original) $\{\mathbf{v}(n)\}$ is spatially (i.e., componentwise) independent, in (26), $\{\tilde{\mathbf{v}}(n)\}$ is i.i.d. zero-mean complex Gaussian with covariance $\sigma_v^2\mathbf{I}_{N_r}$. Similarly $\tilde{s}_B^{r\ell}(n)$ is uncorrelated zero-mean sequence with $\mathbb{E}\{|\tilde{s}_B^{r\ell}(n)|^2\}$ not a function of n (follows just as the properties of $\tilde{\mathbf{v}}(n)$). Similar to (12), the correlation matrix of $\tilde{\mathbf{x}}(n)$ is given by

$$\mathbf{R}_{\tilde{x}} = \beta P_B\,\mathbf{H}_B\tilde{\mathbf{R}}_B\mathbf{H}_B^H \tag{27}$$

where $[\tilde{\mathbf{R}}_B]_{ij} = \frac{1}{T_m'}\sum_{n=L_m}^{T_m}\mathbb{E}\{\tilde{s}_B^{r(i-1)}(n)(\tilde{s}_B^{r(j-1)}(n))^*\}$. It can be shown that $\rho(\tilde{\mathbf{R}}_B) = L_B$, so that $\rho(\mathbf{R}_{\tilde{x}}) = L_B$ w.p.1.

3.3. Proposed Attack Detection Approach

In addition to (9), consider the nature of projected $\{\tilde{\mathbf{y}}(n)\}$ under the two hypotheses:

$$\begin{array}{ll}\mathcal{H}_0: & \tilde{\mathbf{y}}(n) = \tilde{\mathbf{x}}(n) + \tilde{\mathbf{v}}(n)\\ \mathcal{H}_1: & \tilde{\mathbf{y}}(n) = \tilde{\mathbf{x}}(n) + \tilde{\mathbf{v}}(n)\end{array}, n = L_m, L_m+1, \cdots, T_m. \tag{28}$$

We see that under $\mathcal{H}_0$, the signal subspace rank of both $\{\mathbf{y}(n)\}$ and $\{\tilde{\mathbf{y}}(n)\}$ is L_B, whereas under $\mathcal{H}_1$, the signal subspace rank of $\{\mathbf{y}(n)\}$ is $L_B + L_E$ while that of $\{\tilde{\mathbf{y}}(n)\}$ is L_B. Since the channel lengths L_B and L_E are not known, our proposed relies on estimating the signal subspace ranks of $\{\mathbf{y}(n)\}$ and $\{\tilde{\mathbf{y}}(n)\}$: if the two ranks are the same, there is no pilot spoofing, and if the two ranks are different, one declares presence of a pilot spoofing attack. In contrast, in the approach of [8] (also used in [11, 12]) applicable to flat fading channels, it is enough to check the signal subspace rank of $\{\mathbf{y}(n)\}$, which is 1 if there is no pilot spoofing, and is 2 in the presence of pilot spoofing.

We use two different approaches for estimation of signal subspace rank given observations of signals in white Gaussian noise: the minimum description length (MDL) source enumeration method ([14–16]), and the random matrix theory (RMT) based source enumeration approach of [17, 18].

3.4. Estimation of Bob's Channel

Regardless of the absence/presence of spoofer, we first estimate the channel $\mathbf{h}_{C\ell}$ (see (19)) with known input $s_t(n)$ and noisy output $\mathbf{y}(n)$ using the method of least-squares. The solution $\hat{\mathbf{h}}_{C\ell}$ satisfies ($k = 0, 1, \cdots, L_m - 1$)

$$\sum_{\ell=0}^{L_m-1} r_s(\ell,k)\hat{\mathbf{h}}_{C\ell} = \frac{1}{T_m}\sum_{n=L_m}^{T}\mathbf{y}(n)s_t^*(n-k),$$

where $r_s(\ell,k) = \frac{1}{T_m}\sum_{n=L_m}^{T} s_t(n-\ell)s_t^*(n-k)$. Remove the training contribution from the received signal to define

$$\check{\mathbf{y}}(n) = \mathbf{y}(n) - \sum_{\ell=0}^{L_m-1} \hat{\mathbf{h}}_{C\ell} s_t(n-\ell) \tag{29}$$

$$\approx \sqrt{\beta P_B} \sum_{\ell=0}^{L_B-1} \mathbf{h}_{B\ell} s_B(n-\ell) + \mathbf{v}(n). \tag{30}$$

Now using (30), we apply the blind approach of [19] (the SIMO case, equalizer length of 5 taps, delay of 2) to estimate $\mathbf{h}_{B\ell}$ as $\hat{\mathbf{h}}_{B\ell} = c\mathbf{h}_{B\ell}, \forall \ell$, up to a complex constant c. (Note that step 2 of Algorithm 1 of [19] was modified to extract "significant" principal eigenvectors of the data correlation matrix, instead of the number of principal eigenvectors stated in [19, Step 2, Alg. 1]. All eigenvalues smaller than $0.1\times$ the largest eigenvalue of the data correlation matrix in step 2 of Algorithm 1 of [19] were deemed to be insignificant, hence the corresponding eigenvectors were insignificant. The reason for this modification is the lack of knowledge of L_B in (30).) We will use a phase-insensitive mean-square error (MSE) measure to evaluate channel estimation errors; this has been used in [20] in a different context. If $\hat{\mathbf{h}}^{(B)}$ is an estimate of $\mathbf{h}^{(B)}$ (see (16)), both normalized to unit norm, phase-insensitive MSE in estimation of $\mathbf{h}^{(B)}$ is given by [20]

$$\min_{\theta\in[0,2\pi]} \|\mathbf{h}^{(B)} - e^{j\theta}\hat{\mathbf{h}}^{(B)}\|^2 = 2 - 2|\mathbf{h}^{(B)H}\hat{\mathbf{h}}^{(B)}|. \tag{31}$$

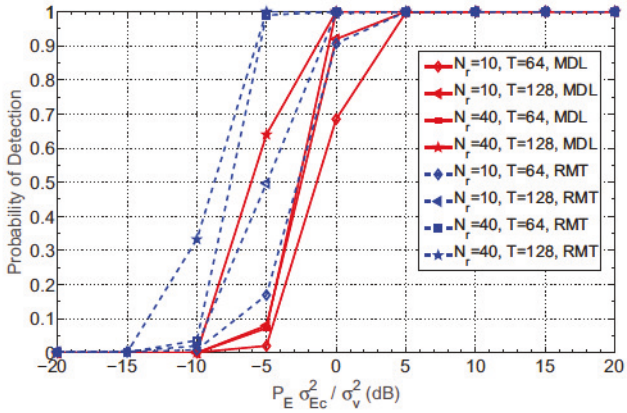

Fig. 1: Probability of attack detection as a function of Eve's power P_E relative to noise power σ_v^2 when Bob's power is fixed at $P_B\sigma_{Bc}^2/\sigma_v^2 = 10$dB, β=0.4 .

4. SIMULATION EXAMPLE

We consider frequency selective channels with $L_B = 3$, $L_E = 2$, both values unknown to Alice who uses the upperbound $L_m = 4$, $\mathbf{h}_{B\ell} \sim \mathcal{N}_c(0, \sigma_{Bc}^2\mathbf{I}_{N_r})$, $\mathbf{h}_{E\ell} \sim \mathcal{N}_c(0, \sigma_{Ec}^2\mathbf{I}_{N_r})$, both channels have independent tap gains, and noise power σ_v^2, training power budget P_B at Bob is such that $P_B\sigma_{Bc}^2/\sigma_v^2 = 10$dB, training power budget P_E at Eve is such that $P_E\sigma_{Ec}^2/\sigma_v^2$ 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 $N_r = 10$ or 40 antennas ($\geq 2L_m$). The training sequence is a random binary sequence with T =64 or 128, and the random sequence $\{s_B(n)\}$ is i.i.d. QPSK. Fig. 1 shows our detection probability P_d results averaged over 5000 runs for both MDL and RMT (designed for false-alarm rate of 0.001) approaches. The performance improves with increasing T, N_r and Eve's power P_E, and RMT outperforms MDL. Fig. 2 shows phase-insensitive MSE in Bob's channel estimation. The curves labeled "blind" are based on Sec. 3.4, and the curves labeled "naive" ignore Eve's presence and use an iterative method for channel estimation (estimate channel using only training, equalize and quantize self-contamination, and then redo with training-plus-estimated $s_B(n)$ as pseudo-training). The blind result is invariant to Eve's power, since it is applied after canceling training contribution, hence Eve's contribution. The naive results work well for low P_E (as exptected), but rapidly deteriorate with increasing P_E. The estimated Bob's channel can be used by Alice to implement a time-reversal matched-filter precoding [21] at Alice for transmission to Bob; this precoder does not need the knowledge of scaling ambiguity in estimating Bob's channel.

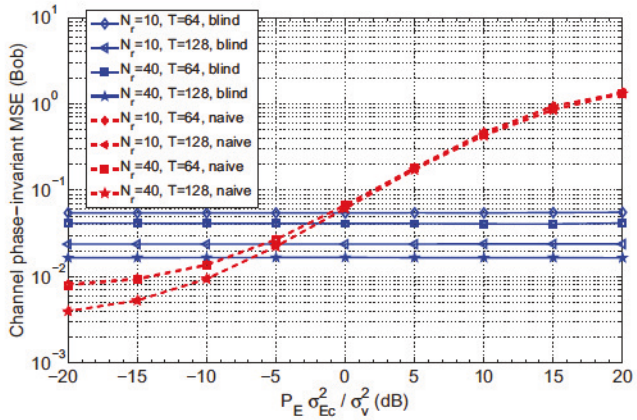

Fig. 2: Channel normalized MSE (31) for Bob's channel as a function of Eve's power P_E. All parameters as for Fig. 1.

5. CONCLUSIONS

A novel approach to detection of pilot spoofing/contamination attack in a 3-node TDD system (legitimate source-destination pair Alice and Bob, and spoofer Eve) was presented in [8] (and also used in [11, 12]) for flat fading channels, exploiting the fact that both Bob's and Eve's channels are one-tap channels. In this paper we extended the approach of [8] to frequency selective channels, with unknown channels and channel lengths, except that an upperbound on the number of channel taps is assumed to be known to Alice. The proposed approach was illustrated by numerical examples and they show the efficacy of the proposed approach. A method to estimate Bob's channel regardless of the spoofing attack, was also presented and illustrated via simulations.

6. 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] D. Kapetanovic, G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, No. 6, pp. 21-27, June 2015.

[4] 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.

[5] X. Chen, J. Chen, H. Zhang, Y. Zhang and C. Yuen, "On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI," *IEEE Trans. Veh. Tech.*, vol. 65, no. 10, pp. 8014-8024, Oct. 2016.

[6] T.T. Do, E. Björnson, E.J. Larsson and S.M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 210-223, Jan. 2018.

[7] 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.

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

[9] 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.

[10] 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.

[11] J.K. Tugnait, "On mitigation of pilot spoofing attack," in *Proc. 2016 IEEE Intern. Conf. Acoust., Speech Signal Process. (ICASSP 2017)*, New Orleans, Louisiana, March 5-9, 2017, pp. 2097-2101.

[12] J.K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, to appear (online Jan. 25, 2018).

[13] M. Verhaegen and V. Verdult, *Filtering and System Identification*. Cambridge, UK: Cambridge U. Press, 2007.

[14] 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.

[15] 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.

[16] 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.

[17] S. Kritchman and B. Nadler, "Determining the number of components in a factor model from limited noisy data," *Chem. Inst. Lab. Syst.*, vol. 94, pp. 19-32, 2008.

[18] S. Kritchman and B. Nadler, "Non-parametric detection of the number of signals: Hypothesis testing and random matrix theory," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 3930-3941, Oct. 2009.

[19] I. Kacha, K. Abed-Meraim and A. Belouchrani, "Fast adaptive blind MMSE equalizer for multichannel FIR systems," *EURASIP J. Applied Signal Process.*, vol. 2006, Article ID 14827, pages 1-17, 2006.

[20] D.J. Love and R.W. Heath, "Equal gain transmission in multiple-input multiple-output wireless systems," *IEEE Trans. Commun.*, vol. 51, no. 7, pp. 1102-1110, July 2003.

[21] T. Strohmer, M. Emami, J. Hansen, G. Papanicolaou and A.J. Paulraj, "Application of time-reversal with MMSE equalizer to UWB communications," in *Proc. IEEE Globecom 2004*, vol. 5, pp. 3123-3127, Nov. 2004.