This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2715814, IEEE Wireless Communications Letters

Detection and Identification of Spoofed Pilots in TDD/SDMA Systems

Jitendra K. Tugnait

***Abstract*—In a time-division duplex (TDD) multiple antenna system, the channel state information (CSI) can be estimated using reverse training. A pilot spoofing attack occurs when during the training phase, an adversary (spoofer) also sends identical training (pilot) signal as that of the legitimate receiver. This contaminates channel estimation and alters the legitimate precoder design, facilitating eavesdropping. A recent approach proposed superimposing a random sequence on the training sequence at the legitimate receivers, and then using the minimum description length (MDL) criterion to detect pilot spoofing attack via source enumeration. In this letter, we extend this approach by exploiting temporal subspace properties of the pilot signals in conjunction with the MDL criterion, to determine which pilots are contaminated by a spoofer, and which ones are free of spoofing attack. The identification performance is illustrated via simulations.**

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

I. Introduction

Consider a TDD system with space-division multiple access (SDMA) uplink and downlink. The system has a base station Alice, with N_r antennas, and K legitimate single antenna users, named Bob 1, Bob 2, $\cdots$, (Bobs), and $J \leq K$ single antenna spoofers (active eavesdroppers), named Eve 1, Eve 2, $\cdots$, (Eves). Based on her channel to Bobs, Alice designs her transmit beamformer/precoder for improved performance. Since the downlink and uplink channels are reciprocal in a TDD system, Alice acquires her CSI to Bob i via training from Bob i to Alice. In a publicly known protocol with known pilot sequences, an Eve can transmit the same pilot sequence during the training phase, thereby biasing the CSI estimated by Alice. The precoder designed by Alice based on corrupted CSI could lead to a significant information leakage to Eve. This phenomenon, i.e., Eve's transmission of a pilot signal concurrently with Bob's pilot, is called pilot contamination attack in [1], [2], and a pilot spoofing attack in [3].

In [1] the focus is on enhancing Eve's performance. Approaches discussed in [2]–[4] for detection of the attack assume a single legitimate user Bob and a single eavesdropper (ED) Eve. In [5] an SDMA uplink was considered to allow for simultaneous transmission of training from multiple Bobs. The approach of [5], using an extension of the self-contamination approach of [4], detects the presence a spoofing attack but does not determine which pilots are being spoofed. In this letter we provide a method to do so for the set-up of [5].

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, and $\delta_{i,j}$ equals 1 for $i = j$, 0 for $i \neq j$. 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. The abbreviations i.i.d. and w.p.1 stand for independent and identically distributed and with probability one, respectively.

J.K. Tugnait is with the Department of Electrical & Computer Engineering, Auburn University, Auburn, AL 36849, USA. Email: tugnajk@eng.auburn.edu

This work was supported by NSF Grant ECCS-1651133.

II. System Model and Background

Consider a flat Rayleigh fading environment with Bob i-to-Alice channel denoted as $\mathbf{h}_{B_i} \in \mathbb{C}^{N_r}$ and Eve i-to-Alice channel denoted as $\mathbf{h}_{E_i} \in \mathbb{C}^{N_r}$, 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; they also include path losses. In the absence of any transmission from any Eve, Alice receives

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

where additive noise $\mathbf{v}(n) \sim \mathcal{N}_c(0, \sigma_v^2 \mathbf{I}_{N_r})$, $s_{t,i}(n)$, $1 \leq n \leq T$, denotes the training sequence of the ith Bob, and the training sequences are periodic with period P and orthogonal satisfying $P^{-1}\sum_{n=1}^{P} s_{t,i}(n) s^*_{t,j}(n) = \delta_{i,j}$. Let $\mathcal{E} \subseteq [1, K]$, with $|\mathcal{E}| = J$, denote the set of active EDs. When Eves also transmit (Eve's pilot spoofing attack), Alice receives

$$\mathbf{y}(n) = \sum_{i=1}^{K} \tilde{\mathbf{h}}_i s_{t,i}(n) + \mathbf{v}(n) \tag{2}$$

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 (2), Alice will estimate $\mathbf{h}_i$ as Bob i-to-Alice channel, instead of $\sqrt{P_{B_i}}\, \mathbf{h}_{B_i}$.

In [5] a fraction β of the training power P_{B_i} at Bob i is allocated to a scalar random sequence $\{s_{B_i}(n)\}$ to be transmitted by Bob along with $s_{t,i}(n)$; it can be the information sequence of Bob i. It is assumed in [5] 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 (binary phase-shift keying) or QPSK (quadrature PSK), e.g. Thus, instead of $\sqrt{P_{B_i}} s_{t,i}(n)$, Bob i transmits ($0 \leq \beta < 1, \;\; n = 1, 2, \cdots, T$)

$$\tilde{s}_{B_i}(n) = \sqrt{P_{B_i}(1-\beta)}\, s_{t,i}(n) + \sqrt{P_{B_i}\beta}\, s_{B_i}(n). \tag{3}$$

The sequences $\{s_{B_i}(n)\}$ are unknown to Alice (and to Eves) and they can not be replicated in advance. For the received signal at Alice, we have two hypotheses $\mathcal{H}_0$ (no attack) and $\mathcal{H}_1$ (attack present). Under $\mathcal{H}_0$,

$$\mathbf{y}(n) = \sum_{i=1}^{K} \mathbf{h}_{B_i} \tilde{s}_{B_i}(n) + \mathbf{v}(n), \tag{4}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2715814, IEEE Wireless Communications Letters

and under $\mathcal{H}_1$,

$$\mathbf{y}(n) = \sum_{i=1}^{K} \left[\mathbf{h}_{B_i}\tilde{s}_{B_i}(n) + \sqrt{P_{E_i}}\,\mathbf{h}_{E_i}s_{t,i}(n)\mathbf{1}_{\{i\in\mathcal{E}\}}\right] + \mathbf{v}(n). \quad (5)$$

Define $\mathbf{R}_{y,j} = T^{-1}\sum_{n=1}^{T}\mathbb{E}\left\{\mathbf{y}(n)\mathbf{y}^H(n)\,\middle|\,\mathcal{H}_j\right\}$ where j=0 or 1, and further define $\mathbf{R}_{s,j} = T^{-1}\sum_{n=1}^{T}\mathbb{E}\left\{[\mathbf{y}(n)-\mathbf{v}(n)][\mathbf{y}(n)-\mathbf{v}(n)]^H\,\middle|\,\mathcal{H}_j\right\}$. Then we have $\mathbf{R}_{y,j} = \mathbf{R}_{s,j} + \sigma_v^2\mathbf{I}_{N_r}$, $j = 0, 1$. It is shown in [5] that $\text{rank}(\mathbf{R}_{s,0}) = K$ w.p.1 for $N_r \geq K$, and $\text{rank}(\mathbf{R}_{s,1}) = J + K$ w.p.1 for $N_r \geq J + K$. Thus, introduction of $\{s_{B_i}(n)\}$ by K legitimate users Bobs leads to signal subspace of rank $J + K$ in the presence of Eves' attack. If $\beta = 0$, then $\text{rank}(\mathbf{R}_{s,1}) = K$. Define the sample correlation matrix of T observations as $\widehat{\mathbf{R}}_y = T^{-1}\sum_{n=1}^{T}\mathbf{y}(n)\mathbf{y}^H(n)$. Let the ordered eigenvalues of $\widehat{\mathbf{R}}_y$ be denoted by $\nu_1 \geq \nu_2 \geq \cdots \geq \nu_{N_r}$. The MDL estimator $\widehat{d}$ of the signal subspace dimension d is given by [5], [6]

$$\widehat{d} = \arg\min_{1\leq d\leq N_r-1} \text{MDL}(d), \quad (6)$$

$$\text{MDL}(d) = -\sum_{i=d+1}^{N_r}\ln(\nu_i) + (N_r - d)\,\ln\Big(\frac{1}{N_r-d}\sum_{i=d+1}^{N_r}\nu_i\Big) + \frac{d(2N_r-d)\ln(T)}{2T}. \quad (7)$$

If $\widehat{d} = K$, declare no attack, and if $\widehat{d} > K$, we have a pilot spoofing attack.

III. Spoofed Pilot Identification

If the MDL method indicates presence of attack, Alice proceeds to identification of spoofed pilots. Stack P consecutive samples of ℓth component $y_\ell(n)$ of $\mathbf{y}(n)$ into a column:

$$\underbrace{y_\ell(1)\ \cdots\ y_\ell(P)}_{\mathbf{y}^\ell(1)}\ \underbrace{y_\ell(P+1)\ \cdots\ y_\ell(2P)}_{\mathbf{y}^\ell(2)}\cdots \quad (8)$$

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

$$\mathbf{y}^\ell(m) = \sum_{i=1}^{K} h_{i\ell}^{(1)}\check{\mathbf{s}}_{t,i} + \sum_{i=1}^{K} h_{i\ell}^{(2)}\check{\mathbf{s}}_{B_i}(m) + \mathbf{v}^\ell(m) \quad (9)$$

where $h_{i\ell}^{(1)} = \sqrt{P_{B_i}(1-\beta)}\,h_{B_i,\ell} + \sqrt{P_{E_i}}\,h_{E_i,\ell}\mathbf{1}_{\{i\in\mathcal{E}\}}$, $h_{i\ell}^{(2)} = \sqrt{P_{B_i}\beta}\,h_{B_i,\ell}$. Thus, $\mathbf{y}^\ell(m)$ lies in a subspace spanned by pilots $\check{\mathbf{s}}_{t,i}$ and random vectors $\check{\mathbf{s}}_{B_i}(m)$. Let $\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}$ denote the projection orthogonal to the subspace spanned by $\check{\mathbf{s}}_{t,k}$. Then $\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}\mathbf{y}^\ell(m)$ has no contribution from kth training $s_{t,k}(n)$. Reshape $\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}\mathbf{y}^\ell(m)$ into a row vector along time and put all components ℓs together. Then the so projected $\mathbf{y}(n)$ lacks $s_{t,k}(n)$. If the ED using $s_{t,k}(n)$ exists, projected signal subspace rank drops by 1. If no ED uses $s_{t,k}(n)$, projected signal subspace rank is unchanged due to the presence of self-contamination. We use this fact to iteratively test each training sequence for pilot contamination from ED.

We have

$$\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}} = \mathbf{I}_P - P^{-1}\check{\mathbf{s}}_{t,k}\check{\mathbf{s}}^H_{t,k} \in \mathbb{C}^{P\times P} \quad (10)$$

where we have used $\check{\mathbf{s}}^H_{t,k}\check{\mathbf{s}}_{t,k} = P$. Since $\text{rank}(\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}) = P-1$, its singular value decomposition (SVD) is

$$\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}} = \mathbf{U}_1\Sigma_1\mathbf{V}_1^H, \quad \mathbf{U}_1, \mathbf{V}_1 \in \mathbb{C}^{P\times(P-1)}, \quad (11)$$

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

$$\mathbb{E}\{[\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}\mathbf{v}^\ell(m)][\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}}\mathbf{v}^\ell(m)]^H\} = \mathbf{U}_1\Sigma_1\mathbf{V}_1^H(\sigma_v^2\mathbf{I}_P)\mathbf{V}_1\Sigma_1\mathbf{U}_1^H = \sigma_v^2\mathbf{U}_1\Sigma_1^2\mathbf{U}_1^H \in \mathbb{C}^{P\times P} \quad (12)$$

Noting that $\Sigma_1^{-1}\mathbf{U}_1^H\mathcal{P}^\perp_{\check{\mathbf{s}}_{t,k}} = \mathbf{V}_1^H$, consider the reduced dimension projected noise $\mathbf{v}^{\ell r}_{(k)}(m) := \mathbf{V}_1^H\mathbf{v}^\ell(m) \in \mathbb{C}^{P-1}$. Then we have $\mathbb{E}\{\mathbf{v}^{\ell r}_{(k)}(m)(\mathbf{v}^{\ell r}_{(k)}(m))^H\} = \sigma_v^2\mathbf{I}_{P-1}$. Note that $\mathbf{v}^{\ell r}_{(k)}(m_1)$ and $\mathbf{v}^{\ell r}_{(k)}(m_2)$ are independent for $m_1 \neq m_2$. Similarly, define the reduced dimension projected observations, pilots and contaminating sequences $\mathbf{y}^{\ell r}_{(k)}(m) := \mathbf{V}_1^H\mathbf{y}^\ell(m)$, $\check{\mathbf{s}}_{(k)t,i} := \mathbf{V}_1^H\check{\mathbf{s}}_{t,i}$, $\check{\mathbf{s}}_{(k)B_i}(m) := \mathbf{V}_1^H\check{\mathbf{s}}_{B_i}(m)$. Then we have, for $m = 1, 2, \cdots, T/P$, $\mathbf{y}^{\ell r}_{(k)}(m)$

$$= \sum_{i=1,\,i\neq k}^{K} h_{i\ell}^{(1)}\check{\mathbf{s}}_{(k)t,i} + \sum_{i=1}^{K} h_{i\ell}^{(2)}\check{\mathbf{s}}_{(k)B_i}(m) + \mathbf{v}^{\ell r}_{(k)}(m). \quad (13)$$

Now reshape $\mathbf{y}^{\ell r}_{(k)}(m)$, $m = 1, \cdots, T/P$, with T/P an integer, into a row a scalars $\tilde{y}_{(k)\ell}(n)$, $n = 1, 2, \cdots, (T/P)P'$, $P' = P-1$, using the correspondence

$$\underbrace{\tilde{y}_{(k)\ell}(1)\ \cdots\ \tilde{y}_{(k)\ell}(P')}_{\mathbf{y}^{\ell r}_{(k)}(1)}\ \underbrace{\tilde{y}_{(k)\ell}(P)\ \cdots\ \tilde{y}_{(k)\ell}(2P')}_{\mathbf{y}^{\ell r}_{(k)}(2)}\cdots \quad (14)$$

Similarly define $\tilde{v}_{(k)\ell}(n)$ from $\mathbf{v}^{\ell r}_{(k)}(m)$. Also let $\check{\mathbf{s}}_{(k)t,i} = [\tilde{s}_{(k)t,i}(1)\ \tilde{s}_{(k)t,i}(2)\ \cdots\ \tilde{s}_{(k)t,i}(P-1)]^\top \in \mathbb{C}^{P-1}$ and let $\tilde{s}_{(k)t,i}(n)$ be periodic extension of $\tilde{s}_{(k)t,i}(n)$, $n = 1, 2, \cdots, P'$, with period $P' = P-1$. Similarly construct $\tilde{s}_{(k)B_i}(n)$ from $\check{\mathbf{s}}_{(k)B_i}(m)$ except that unlike pilot signals, we do not have periodicity. Then $\tilde{\mathbf{y}}_{(k)}(n) \in \mathbb{C}^{N_r}$ with ℓth component $\tilde{y}_{(k)\ell}(n)$, satisfies

$$\tilde{\mathbf{y}}_{(k)}(n) = \sum_{\substack{i=1\\ i\neq k}}^{K}\mathbf{h}_i^{(1)})\tilde{s}_{(k)t,i}(n) + \sum_{i=1}^{K}\mathbf{h}_i^{(2)}\tilde{s}_{(k)B_i}(n) + \tilde{\mathbf{v}}_{(k)}(n) \quad (15)$$

where $\mathbf{h}_i^{(1)} = \sqrt{P_{B_i}(1-\beta)}\,\mathbf{h}_{B_i} + \sqrt{P_{E_i}}\,\mathbf{h}_{E_i}\mathbf{1}_{\{i\in\mathcal{E}\}}$, and $\mathbf{h}_i^{(2)} = \sqrt{P_{B_i}\beta}\,\mathbf{h}_{B_i}$. In the above model $\{\tilde{\mathbf{v}}_{(k)}(n)\}$ is i.i.d. zero-mean complex Gaussian with covariance $\sigma_v^2\mathbf{I}_{P-1}$ and similarly $\tilde{s}_{(k)B_i}(n)$ is uncorrelated zero-mean sequence with $\mathbb{E}\{|\tilde{s}_{(k)B_i}(n)|^2\}$ not a function of n (follows just as the properties of $\tilde{\mathbf{v}}_{(k)}(n)$).

With the above set-up we can invoke the results of [5] reviewed earlier, to conclude that the signal subspace rank for the model (15) equals $K + J$ for test pilot $s_{t,k}(n)$ if there is no ED using $s_{t,k}(n)$, and it equals $K + J - 1$ for test pilot $s_{t,k}(n)$ if there is an ED using $s_{t,k}(n)$. In (15), for $i \neq k$, $\mathbf{h}_i^{(1)}\tilde{s}_{(k)t,i}(n) + \mathbf{h}_i^{(2)}\tilde{s}_{(k)B_i}(n)$ makes up a signal subspace of dimension 2 (i.e., its correlation matrix is of dimension 2), if

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2715814, IEEE Wireless Communications Letters

$i \in \mathcal{E}$, and the signal subspace is of dimension 1 if $i \notin \mathcal{E}$. In the latter case, we have $\mathbf{h}_i^{(1)}\tilde{s}_{(k)t,i}(n) + \mathbf{h}_i^{(2)}\tilde{s}_{(k)B_i}(n) = \sqrt{P_{B_i}}\mathbf{h}_{B_i}(\sqrt{(1-\beta)}\tilde{s}_{(k)t,i}(n) + \sqrt{\beta}\tilde{s}_{(k)B_i}(n))$, which is of dimension 1. The projected pilots $\tilde{s}_{(k)t,i}(n)$ are no longer orthogonal to each other but the signal subspace rank is unaffected. Similar comments hold for the projected self-contamination $\tilde{s}_{(k)B_i}(n)$.

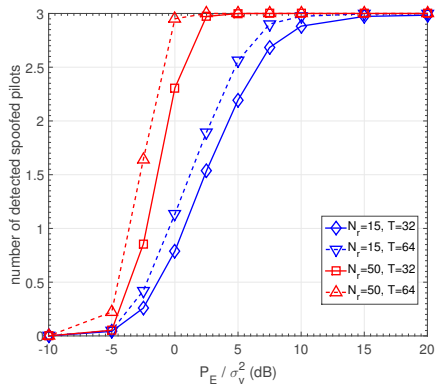

Fig. 1. Total number of detected spoofed pilots as a function of Eve's power P_E (=P_{E_j} $\forall j$) relative to noise power σ_v^2 when Bob's power is fixed at P_{B_i}/σ_v^2 = 10dB $\forall i$: K=6= number of legitimate users, J=3= number of spoofed pilots, β=0.2 .

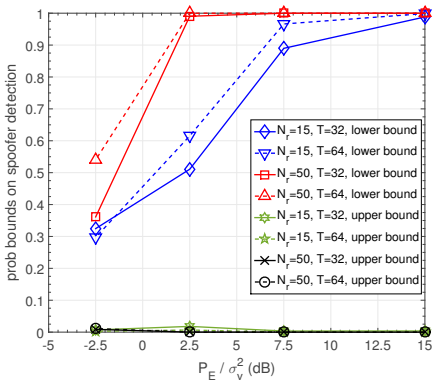

Fig. 2. Lower bound on the probability of correctly identifying a spoofed pilot, and upper bound on the probability of incorrectly classifying an unspoofed pilot as spoofed. All parameters as for Fig. 1.

Iterative Identification: Our iterative spoofed pilot identification procedure is summarized below.

(i) *Given*: Known number of legitimate users K, their pilot sequences, and observations $\mathbf{y}(n)$, $n = 1, 2, \cdots, T$, $T = Pn_b$, for some integer $n_b \geq 1$.

(ii) Apply the MDL criterion as in (7) to estimate $\hat{d}_{total}$, total number of sources; this exploits spatial subspace properties of signals, i.e., rank of $\mathbf{R}_{s,1}$. If $\hat{d}_{total} \leq K$, there are no EDs, hence quit; else continue.

(iii) Set $\hat{d}_E = 0$. For $k = 1, 2, \cdots, K$, do:

Using the kth pilot sequence and the projection operator $\mathcal{P}^{\perp}_{\tilde{\mathbf{s}}_{t,k}}$, generate the reduced length sequence $\tilde{\mathbf{y}}_{(k)}(n)$ satisfying (15). This exploits temporal subspace properties of pilots. Apply MDL criterion to the projected data $\tilde{\mathbf{y}}_{(k)}(n)$, $n = 1, 2, \cdots, n_b(P-1)$. Let the estimated number of sources be $\hat{d}_k$. If $\hat{d}_k < \hat{d}_{total}$, increment $\hat{d}_E$ by one; the kth pilot is spoofed by an ED. If $\hat{d}_k < \hat{d}_{total}$, store the MDL cost MDL($\hat{d}_k$), which equals minimized negative log-likelihood (with a penalty term) [6].

(iv) If $\hat{d}_E \leq \hat{d}_{total} - K$, quit. We have $\hat{d}_E$ spoofed pilots whose identities are given by the values of k for which $\hat{d}_k < \hat{d}_{total}$ in step (iii) above. If $\hat{d}_E > \hat{d}_{total} - K$, select $\hat{d}_{total} - K$ spoofed pilots out of the $\hat{d}_E$ candidates, that lead to the least $\hat{d}_{total} - K$ MDL costs MDL($\hat{d}_k$) out of the $\hat{d}_E$ MDL costs stored in step (iii) above.

The rationale for item (iv) is as follows. Assuming that $\hat{d}_{total}$ is accurate (i.e., equals $K + J$), one must have $\hat{d}_E \leq \hat{d}_{total} - K$. If it turns out that $\hat{d}_E > \hat{d}_{total} - K$, one must discard $\hat{d}_E - \hat{d}_{total} - K$ pilots from the pool of estimated spoofed pilots. We use the negative log-likelihood interpretation of MDL costs to "order" the $\hat{d}_E$ spoofed pilot candidates.

Performance: Let d_0 and λ_{d_0} denote the true values of d and ν_{d_0} in (6) and (7). Then, by [7], the probability of correctly detecting the true value of d is given by $P(\widehat{d} = d_0) \approx 1 - Q(-\bar{\mu}(T)/\bar{\sigma}(T))$ as $T \to \infty$, where $Q(z) = (1/\sqrt{2\pi})\int_z^\infty exp(-x^2/2)\,dx$, $\bar{\sigma}^2(T) = (1/T)[1 + (1/(N_r - d_0))](N_r - d_0)^2\bar{\lambda}^2/[\bar{\lambda} + N_r - d_0 + 1]^2$, $\bar{\lambda} = (\lambda_{d_0}/\sigma_v^2) - 1$, $\bar{\mu}(T) = -\ln(1+\bar{\lambda}) - \ln(1 + \frac{N_r - d_0}{\bar{\lambda}T} - \frac{d_0 - 1}{T}) + (1/T) - (N_r - d_0)\ln(1 - \frac{1+\bar{\lambda}}{\bar{\lambda}T} - \frac{d_0-1}{T}) + (N_r - d_0 + 1)\ln(1 + \frac{\bar{\lambda}}{N_r - d_0 + 1}(1 - \frac{d_0-1}{T}) - \frac{d_0-1}{T}) - \frac{1}{2(N_r - d_0 + 1)T}\frac{(1+\bar{\lambda})^2 + N_r - d_0}{(1+(\bar{\lambda}/(N_r - d_0 + 1)))^2} - (N_r - d_0 + 0.5)\ln(T)/T$. We also have $\lim_{T\to\infty} P(\widehat{d} = d_0) = 1$ and $\lim_{T\to\infty} Q(-\bar{\mu}(T)/\bar{\sigma}(T)) = 0$ [7]. Let d_{k0} denote the true value of d_k in the kth iteration in step (iii) of the proposed iterative identification method. Then the probability P_{iter} that the iterative method correctly identifies the spoofed pilots is

$$P_{iter} = P(\cap_{k=1}^K \{\widehat{d}_k = d_{k0}\}) = 1 - P(\cup_{k=1}^K \{\widehat{d}_k \neq d_{k0}\})$$
$$\geq 1 - \sum_{k=1}^K P(\widehat{d}_k \neq d_{k0}) = 1 - \sum_{k=1}^K Q(-\bar{\mu}_k(T')/\bar{\sigma}_k(T')) \quad (16)$$

where $T' = n_b(P-1)$, and $\bar{\mu}_k(T')$ and $\bar{\sigma}_k(T')$ are defined just as $\bar{\mu}(T)$ and $\bar{\sigma}(T)$ with d_0 and $\bar{\lambda}$ replaced with d_{k0} and $\bar{\lambda}_k = (\lambda_{d_{k0}}/\sigma_v^2) - 1$, respectively. Thus, $\lim_{T\to\infty} P_{iter} = 1$.

IV. Simulation Example

We consider $\mathbf{h}_{B_i} \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\mathbf{h}_{E_i} \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\forall i$, K=6= number of legitimate users, and J=3= number of spoofed pilots. The training power budget P_{B_i} at Bob i and noise power σ_v^2 are such that P_{B_i}/σ_v^2 = 10dB $\forall i$, training power budget P_{E_j} at Eve j is such that P_{E_j}/σ_v^2 varies from $-$10dB through 20dB and is the same $\forall j$, and fractional allocation β of training power at Bob i to power of random sequence $s_{B_i}(n)$ is 0.2 . Bobs and Eves have single antennas while Alice has N_r = 15 or 50 antennas. The training sequences are selected as periodic extensions of orthogonal (binary) Hadamard sequences of length P = 16 and the random sequences $\{s_{B_i}(n)\}$ were i.i.d. QPSK. Fig. 1 shows the total number of detected spoofed pilots, averaged over 5000 runs, under pilot spoofing attack, for various parameter choices when $P_{B_i}/\sigma_v^2 = 10dB$ $\forall i$. The performance improves with increasing T, N_r, and P_E. Performance of the proposed iterative method is shown in Fig. 2, which shows the minimum (over 3 spoofed pilots) of the probability of correctly identifying a spoofed pilot (labeled "lower bound"), and the maximum

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2715814, IEEE Wireless Communications Letters

(over 3 unspoofed pilots) of the probability of incorrectly mis-identifying an unspoofed pilot as spoofed (labeled "upper bound").

After having identified spoofed pilots, we also estimated Bob i-to-Alice channel, only for those Bobs whose pilots were identified as not spoofed. An iterative method as proposed in [5] was used: first carry out pilot-based least-squares channel estimation for selected Bobs, then use a linear MMSE equalizer based on estimated channels to estimate and decode (quantize) self-contamination $s_{B_i}(n)$ for selected Bobs, and finally, use the decoded $s_{B_i}(n)$ in conjunction with training $s_{t,i}(n)$ as pseudo-training to obtain the final channel estimates. For details, please refer to [5]. Suppose $\hat{K} \leq K$ denotes the number of Bobs identified as unspoofed by the proposed approach. Let columns of $\mathbf{H}_0 \in \mathbb{C}^{N_r \times \hat{K}}$ contain the true Bob-to-Alice channels for unspoofed Bobs, and let $\widehat{\mathbf{H}}_0$ denote the estimate of $\mathbf{H}_0$ obtained by the method of [5]. We define channel normalized mean-square error (CNMSE) as $\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2 / \|\mathbf{H}_0\|_F^2$. Channel estimation results in terms of CNMSE, averaged over 5000 runs, are shown in Figs. 3, 4 and 5. Fig. 3 is based on Bobs that were identified as unspoofed by the proposed approach, hence include mis-identified results. For Fig. 4, the identities of unspoofed Bobs were known a priori whereas the results of Fig. 5 are based on the assumption that there is no spoofing present (therefore, $\hat{K} = K$). Since Fig. 5 ignores spoofing, the results therein are the worst. Since for Fig. 4, one knows exactly which pilots are unspoofed, the results therein are the best of the three figures. With increasing N_r and T, correct identification of spoofed pilots improves, resulting in improved performance depicted in Fig. 3. At lower Eve power levels, mis-identification of spoofed pilots increases, resulting in poorer performance in Fig. 3 compared to that in Fig. 4. Mis-identification of spoofed pilots explains why CNMSE is lower at $P_E/\sigma_v^2 = 0dB$ compared to $P_E/\sigma_v^2 = -2.5dB$ in Fig. 3 for $N_r = 50$, $T = 64$; see also identification results in Fig. 2. Finally, the effect of spoofing on channel estimation is "small" at very low Eve power levels, even though spoofed pilots are not detected.

V. Conclusion

A novel approach to detection of pilot spoofing attack in TDD/SDMA systems was recently presented in [5]. In this letter we extended [5] by exploiting certain subspace properties of the pilot signals in conjunction with the MDL criterion, to determine which pilots are spoofed by an active ED, and which ones are free of active ED attack. What to do regarding spoofed pilots is left for future research. For the case of single Bob and Eve, some results are in [8], [9].

References

[1] X. Zhou, B. Maham and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, 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. IEEE PIMRC*, London, UK, Sept. 2013, pp. 13-18.

[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. Inf. Forensics Security*, vol. 10, no. 5, pp. 932-940, May 2015.

[4] 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.

[5] J.K. Tugnait, "Detection of pilot contamination attack in TDD/SDMA systems," in *Proc. 2016 IEEE Int. Conf. Acous. Speech Signal Proc.*, Shanghai, China, March 2016, pp. 3576-3580.

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

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

[8] 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. Inf. Forensics Security*, vol. 11, pp. 1017-1026, May 2016.

[9] J.K. Tugnait, "On mitigation of pilot spoofing attack," in *Proc. 2017 IEEE Int. Conf. Acous. Speech Signal Proc.*, New Orleans, March 2017.

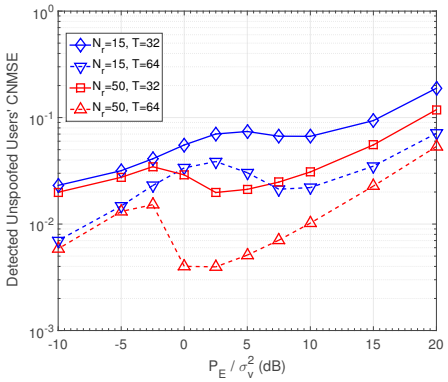

Fig. 3. Normalized channel MSE (CNMSE) $\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2 / \|\mathbf{H}_0\|_F^2$ for channels identified to be spoofing free. All parameters as for Fig. 1.

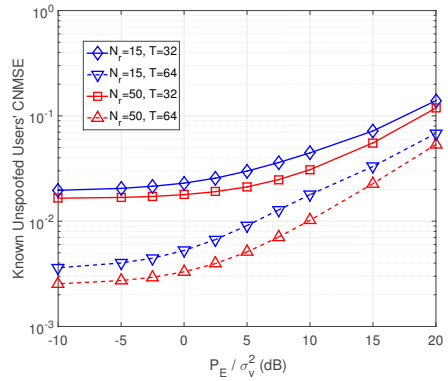

Fig. 4. Normalized channel MSE (CNMSE) $\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2 / \|\mathbf{H}_0\|_F^2$ for channels known to be spoofing free. All parameters as for Fig. 1.

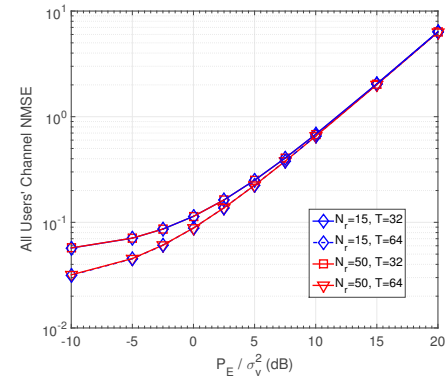

Fig. 5. Normalized channel MSE (CNMSE) $\|\widehat{\mathbf{H}}_0 - \mathbf{H}_0\|_F^2 / \|\mathbf{H}_0\|_F^2$ under the assumption that there is no spoofing at all. All parameters as for Fig. 1.