On Mitigation of Active Eavesdropping Attack by Spoofing Relay

Jitendra K. Tugnait
Dept. of Electrical & Computer Eng.
Auburn University, Auburn, AL 36849, USA
Email: tugnajk@eng.auburn.edu

***Abstract*—We consider detection of spoofing relay attack in time-division duplex (TDD) multiple antenna systems where an adversary operating in a full-duplex mode, amplifies and forwards the training signal of the legitimate receiver. In TDD systems, the channel state information (CSI) can be acquired using reverse training. The spoofing relay attack contaminates the channel estimation phase. Consequently the beamformer designed using the contaminated channel estimate can lead to a significant information leakage to the attacking adversary. A recent approach proposed using the minimum description length (MDL) criterion to detect spoofing relay attack. In this paper we augment this approach with joint channel estimation and secure beamforming to mitigate the effects of pilot contamination by spoofing relay. The proposed mitigation approach is illustrated via simulations.**

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

I. 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 spoofing-relay eavesdropper Eve. Eve is equipped with a full-duplex terminal. 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. Operating in a full-duplex mode, Eve attacks the channel training phase by amplifying and forwarding Bob's signal (containing the same pilot sequence) to Alice with negligible time delay. 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 attack is called spoofing relay attack in [1].

When Eve has a half-duplex terminal, then Eve attacks the channel training phase by transmitting the same pilot sequence during the training phase, which also contaminates the channel estimation phase. This issue of pilot contamination attack was first noted in [2] who investigates enhancing eavesdropper's performance. Several approaches are discussed in [3], [4], [5], [6] for detection of the attack. In [5], the training signal is self-contaminated by Bob which results in signal subspace of dimension two in the presence of pilot contamination attack and of dimension one in its absence. In [5], the minimum description length (MDL) source enumeration method based on data correlation matrix is used for estimation of the signal subspace dimension, hence, for attack detection.

In [1] the problem of spoofing relay attack detection is not addressed, rather the focus is on optimizing spoofer's performance. In [7] is is shown that the basic idea of source enumeration used in [5] applies to spoofing relay attack detection without requiring self-contamination at Bob. Ref. [7] does not address the problem of attack mitigation. In this paper, we augment the approach of [7] with joint channel estimation and secure beamforming to mitigate the effects of pilot contamination by spoofing relay. Our set-up is different from the jamming scenarios considered in [8], [9] (and others). Here Eve's objective is to make Alice replace Alice-to-Bob channel with Alice-to-Eve channel, whereas both, pilot jamming of [8] and jamming of [9], aim to degrade overall system performance. None of [8], [9] considers spoofing relay.

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.

II. System Model and Background

We follow the system model of [1], i.e., there are single antennas at both Bob and Eve whereas the base station Alice has $N_r \geq 3$ antennas [7]. Let $s_t(n)$, $1 \leq n \leq T$, denote the training sequence of length T time samples. Consider a flat Rayleigh fading environment with Bob-to-Alice channel $\mathbf{h}_B = \sqrt{d_B}\,\tilde{\mathbf{h}}_B \in \mathbb{C}^{N_r}$, Eve-to-Alice channel $\mathbf{h}_E = \sqrt{d_E}\,\tilde{\mathbf{h}}_E \in \mathbb{C}^{N_r}$ and Bob-to-Eve scalar channel $\mathrm{g}_{BE} = \sqrt{d_{BE}}\tilde{\mathrm{g}}_{BE} \in \mathbb{C}$, where real scalars d_B, d_E and d_{BE} represent respective path loss attenuations, and $\tilde{\mathbf{h}}_B \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\tilde{\mathbf{h}}_E \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$ and $\tilde{\mathrm{g}}_{BE} \sim \mathcal{N}_c(0, 1)$ 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

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

This work was supported by NSF Grant ECCS-1651133.

978-1-5090-5932-4/17/$31.00 ©2017 IEEE

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 $|s_t(n)| = 1$).

The scalar signal received by Eve is

$$x_{BE}(n) = \sqrt{P_B}\, \mathrm{g}_{BE}\, s_t(n) + v_E(n) \tag{2}$$

where $v_E(n) \sim \mathcal{N}_c(0, \sigma_E^2)$ is the additive white Gaussian noise at Eve's receiver, independent of $\mathbf{v}(n)$. Suppose Eve acts as spoofing relay in full-duplex mode with simultaneous information reception and relaying [10], [1]. As in [1], assume simple amplify-and-forward relaying by Eve since it incurs the minimal processing delay. As demonstrated in [10], it is possible to design an amplify-and-forward relay with "zero" delay between reception and transmission. Denote the signal relayed by Eve as $x_{EA}(n)$ which in the presence of residual self-interference $v_{ri}(n)$ is given by

$$\begin{aligned} x_{EA}(n) &= x_{BE}(n) + v_{ri}(n) \\ &= \sqrt{P_B}\, \mathrm{g}_{BE}\, s_t(n) + v_E(n) + v_{ri}(n) \end{aligned} \tag{3}$$

where $\{v_{ri}(n)\}$ is modeled as additive zero-mean, complex white Gaussian independent of $\{v_E(n)\}$, with variance INR (residual interference to noise ratio) times the variance σ_E^2 of $v_E(n)$ [11], i.e., $\mathbb{E}\{|v_{ri}(n)|^2\} = \mathrm{INR} \times \sigma_E^2$. All reported methods for self-interference cancellation [11], [12], [10], [13] try to suppress the self-interference down to the thermal noise floor. The lowest value of INR is 1 (0dB), but is typically 5 or 10 dB, or even higher, depending upon the transmit power (in our case, P_E at the relay, the full-duplex transmitter) [11], [12], [13].

Under spoofing relay attack, the signal received at Alice is

$$\mathbf{x}(n) = \sqrt{P_B}\, \mathbf{h}_B s_t(n) + \sqrt{P_E}\, \mathbf{h}_E\, x_{EA}(n) + \mathbf{v}(n) \tag{4}$$

$$= \tilde{\mathbf{h}} s_t(n) + \sqrt{P_E}\, \mathbf{h}_E v_{EA}(n) + \mathbf{v}(n) \tag{5}$$

where $\tilde{\mathbf{h}} = \sqrt{P_B}\, \mathbf{h}_B + \sqrt{P_E P_B}\, \mathrm{g}_{BE}\, \mathbf{h}_E$, $v_{EA}(n) = v_E(n) + v_{ri}(n)$, $\mathbb{E}\{|v_{EA}(n)|^2\} = \sigma_{EA}^2 = \sigma_E^2(1 + \mathrm{INR})$. In case of Eve's attack, based on (5), Alice estimates $\tilde{\mathbf{h}}$ as Bob-to-Alice channel, instead of $\sqrt{P_B}\, \mathbf{h}_B$ based on (1).

Ref. [7] addresses the problem: how to detect Eve's spoofing attack based only on the knowledge of $s_t(n)$and $\mathbf{x}(n)$. In a binary statistical hypothesis testing problem framework, let $\mathcal{H}_0$ denote the null hypothesis that there is no spoofing relay attack, i.e., $\mathbf{x}(n)$ follows (1), and let $\mathcal{H}_1$ denote the alternative that Eve's attack is present, i.e., $\mathbf{x}(n)$ follows (5). Define the correlation matrix of measurements as $(i = 0, 1)$

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

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

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

where the expectation is w.r.t. noise with the channels fixed. Then we have $\mathbf{R}_{x,i} = \mathbf{R}_{s,i} + \sigma_v^2 \mathbf{I}_{N_r}$ for $i = 0, 1$. It is shown in [7] that $\mathrm{rank}(\mathbf{R}_{s,0}) = 1$, and $\mathrm{rank}(\mathbf{R}_{s,1}) = 2$ if $\sigma_{EA}^2 > 0$. If $\sigma_{EA}^2 = 0$, then $\mathrm{rank}(\mathbf{R}_{s,1}) = 1$. As in [5], [7] exploits the MDL estimator of the signal subspace dimension d ([15], [14]) based on the eigenvalues of the estimated data correlation matrix to detect if a pilot spoofing attack is present or not. Define the sample correlation matrix as

$$\widehat{\mathbf{R}}_x = T^{-1} \sum_{n=1}^{T} \mathbf{x}(n)\mathbf{x}^H(n). \tag{8}$$

Let the ordered eigenvalues of $\widehat{\mathbf{R}}_x$ be denoted by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{N_r}$. The MDL estimator of the signal subspace dimension d is given by [15], [14]

$$\widehat{d} = \arg \min_{1 \leq d \leq N_r - 1} \mathrm{MDL}(d) \tag{9}$$

where

$$\begin{aligned} \mathrm{MDL}(d) = &- \sum_{i=d+1}^{N_r} \ln(\lambda_i) + (N_r - d)\, \ln\left(\frac{1}{N_r - d} \sum_{i=d+1}^{N_r} \lambda_i \right) \\ &+ \frac{d(2N_r - d)\ln(T)}{2T}. \end{aligned} \tag{10}$$

If $\widehat{d} = 1$, there is no spoofing relay attack, and if $\widehat{d} > 1$, we have a spoofing relay attack.

Ref. [7] does not address attack mitigation. In this paper we do so.

III. Joint Channel Estimation

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

A. No Attack

If the MDL method indicates absence of any attack, Alice proceeds to initially estimate the channel using (1) under $\mathcal{H}_0$, knowledge of $\{s_t(n)\}$ and the least-squares method. This readily yields

$$\begin{aligned} \widehat{\mathbf{h}}_B &= \frac{\sqrt{P_B}}{T} \sum_{n=1}^{T} \mathbf{x}(n) s_t^*(n) \Big/ \left[\frac{P_B}{T} \sum_{n=1}^{T} |s_t(n)|^2 \right] \\ &= \frac{1}{T\sqrt{P_B}} \sum_{n=1}^{T} \mathbf{x}(n) s_t^*(n). \end{aligned} \tag{11}$$

B. Under Attack

1) Projection Orthogonal to Training: Stack P consecutive samples of ℓth component $x_\ell(n)$ of $\mathbf{x}(n)$ into a column:

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

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 $\check{\mathbf{v}}_{EA}(m) = [v_{EA}(1+(m-1)P)\ \cdots\ v_{EA}(P+(m-1)P)]^\top$. Then in the presence of the eavesdropper, we have

$$\begin{aligned} \mathbf{x}^\ell(m) = &\left(\sqrt{P_B}\, h_{B,\ell} + \sqrt{P_E P_B}\, \mathrm{g}_{BE}\, h_{E,\ell} \right) \check{\mathbf{s}}_t \\ &+ \sqrt{P_E}\, h_{E,\ell} \check{\mathbf{v}}_{EA}(m) + \mathbf{v}^\ell(m) \end{aligned}$$

where $h_{B,\ell}$ is the ℓth component of $\mathbf{h}_B$, and similarly for $h_{E,\ell}$. Let $\mathcal{P}_{\check{\mathbf{s}}_t}^{\perp}$ = projection orthogonal to the subspace spanned by

$\check{\mathbf{s}}_t$. Then $\mathcal{P}^{\perp}_{\check{\mathbf{s}}_t}\mathbf{x}^{\ell}(m)$ has no contribution from training $s_t(n)$. "Reshape" $\mathcal{P}^{\perp}_{\check{\mathbf{s}}_t}\mathbf{x}^{\ell}(m)$ into a row vector along time and put all components ℓs together. Then the so "projected" $\mathbf{x}(n)$ lacks $s_t(n)$ but has the effect of $\mathbf{h}_E$ and $v_{EA}(n)$ which can be used to estimate $\mathbf{h}_E$ 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 $m_1 \neq m_2$. Similarly, define the reduced dimension projected observations and contamination sequence, respectively,

$$\mathbf{x}^{\ell r}(m) := \mathbf{V}_1^H\mathbf{x}^{\ell}(m), \;\; \check{\mathbf{v}}^r_{EA}(m) := \mathbf{V}_1^H\check{v}_{EA}(m).$$

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

$$\mathbf{x}^{\ell r}(m) = \sqrt{P_E}\, h_{E,\ell}\check{\mathbf{v}}^r_{EA}(m) + \mathbf{v}^{\ell r}(m).$$

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

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

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

$$\tilde{\mathbf{x}}(n) = \sqrt{P_E}\,\mathbf{h}_E\tilde{v}_{EA}(n) + \tilde{\mathbf{v}}(n). \tag{12}$$

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 $\tilde{v}_{EA}(n)$ is zero-mean complex Gaussian with covariance $\mathbb{E}\{|\tilde{v}_{EN}(n)|^2\} = \sigma^2_{EA}$ (follows just as the properties of $\tilde{\mathbf{v}}(n)$).

2) Estimation of Eve's Channel: Consider (12) 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 (6),

$$\mathbf{R}_{\tilde{x}} = \frac{1}{T'}\sum_{n=1}^{T'}\mathbb{E}\{\tilde{\mathbf{x}}(n)\tilde{\mathbf{x}}^H(n)\} = \sigma^2_{EA}P_E\mathbf{h}_E\mathbf{h}_E^H + \sigma_v^2\mathbf{I}_{N_r}$$

where $\mathbb{E}\{|v_{EA}(n)|^2\} = \sigma^2_{EA} = \mathbb{E}\{|\tilde{v}_{EA}(n)|^2\}$. Hence we estimate $\mathbf{h}_E$ up to a complex constant as the unit norm eigenvector $\mathbf{u}_1$ corresponding to the largest eigenvalue of $\widehat{\mathbf{R}}_{\tilde{x}}$,

$$\widehat{\mathbf{R}}_{\tilde{x}} = \frac{1}{T'}\sum_{n=1}^{T'}\tilde{\mathbf{x}}(n)\tilde{\mathbf{x}}^H(n).$$

Since $\mathbf{h}_E \approx c\mathbf{u}_1$ for some complex c, we pick c to minimize $\frac{1}{T}\sum_{n=1}^{T}\|\mathbf{x}(n) - c\mathbf{u}_1 s_t(n)\|^2$, leading to the solution $\hat{c} = \frac{1}{T}\sum_{n=1}^{T}(\mathbf{u}_1^H\mathbf{x}(n))s_t^*(n)$, where c includes the contributions of P_E, P_B and g_{BE}. Then we have the estimate of $\mathbf{h}_E$ as

$$\hat{\mathbf{h}}_E = \hat{c}\mathbf{u}_1. \tag{13}$$

For large T, as $\widehat{\mathbf{R}}_{\tilde{x}} \to \mathbf{R}_{\tilde{x}}$, we have (for some θ)

$$\mathbf{u}_1 = e^{j\theta}\mathbf{h}_E/\|\mathbf{h}_E\| \tag{14}$$

and, therefore,

$$\lim_{T\to\infty}\hat{c} = \sqrt{P_B}\mathbf{u}_1^H\mathbf{h}_B + \sqrt{P_EP_B}\mathrm{g}_{BE}\mathbf{u}_1^H\mathbf{h}_E \tag{15}$$

$$= e^{-j\theta}\sqrt{P_B}\left(\mathbf{h}_E^H\mathbf{h}_B/\|\mathbf{h}_E\| + \sqrt{P_E}\mathrm{g}_{BE}\|\mathbf{h}_E\|\right). \tag{16}$$

Thus, for large T, we have

$$\hat{\mathbf{h}}_E \approx \sqrt{P_B}\left(\frac{\mathbf{h}_E^H\mathbf{h}_B}{\|\mathbf{h}_E\|^2} + \sqrt{P_E}\mathrm{g}_{BE}\right)\mathbf{h}_E. \tag{17}$$

As $N_r \to \infty$, $\mathbf{h}_E^H\mathbf{h}_B/\|\mathbf{h}_E\|^2 = (1/N_r)\mathbf{h}_E^H\mathbf{h}_B/((1/N_r)\mathbf{h}_E^H\mathbf{h}_E) \to 0$ with probability one since $\tilde{\mathbf{h}}_B \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, $\tilde{\mathbf{h}}_E \sim \mathcal{N}_c(0, \mathbf{I}_{N_r})$, and $\tilde{\mathbf{h}}_B$ and $\tilde{\mathbf{h}}_E$ are independent.

3) Estimation of Bob's Channel: Using $\mathbf{x}(n) = \left(\sqrt{P_B}\,\mathbf{h}_B + \sqrt{P_EP_B}\mathrm{g}_{BE}\,\mathbf{h}_E\right)s_t(n) + \sqrt{P_E}\,\mathbf{h}_E v_{EA}(n) + \mathbf{v}(n)$ under $\mathcal{H}_1$, we estimate the composite channel $\tilde{\mathbf{h}} := \sqrt{P_B}\,\mathbf{h}_B + \sqrt{P_EP_B}\mathrm{g}_{BE}\,\mathbf{h}_E$ using the training sequence $s_t(n)$ and least-squares, as

$$\hat{\tilde{\mathbf{h}}} = \frac{1}{T}\sum_{n=1}^{T}\mathbf{x}(n)s_t^*(n). \tag{18}$$

This an unbiased estimator of $\tilde{\mathbf{h}}$. Using (13), (17) and (18), we have the estimate of Bob's channel as

$$\hat{\mathbf{h}}_B = \left(\hat{\tilde{\mathbf{h}}} - \hat{\mathbf{h}}_E\right)/\sqrt{P_B} \overset{\text{large } T}{\approx} \mathbf{h}_B - \frac{\mathbf{h}_E^H\mathbf{h}_B}{\|\mathbf{h}_E\|^2}\mathbf{h}_E\,. \tag{19}$$

The second term in (19) tends to zero as $N_r \to \infty$.

IV. 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

$$x_B(n) = \sqrt{P_A}\mathbf{h}_B^{\top}\mathbf{w}\,s_A(n) + v_B(n) \tag{20}$$

$$x_{AE}(n) = \sqrt{P_A}\mathbf{h}_E^{\top}\mathbf{w}\,s_A(n) + v_E(n), \tag{21}$$

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 [16], [17], but instead uses the estimated channel to pick the optimum beamformer

$$\mathbf{w}_* = \widehat{\mathbf{h}}_B^*/\|\widehat{\mathbf{h}}_B\|. \tag{22}$$

The choice $\mathbf{w} = \mathbf{h}_B^*/\|\mathbf{h}_B\|$ maximizes the SNR at Bob since $|\mathbf{h}_B^\top \mathbf{w}| \leq \|\mathbf{h}_B\| \, \|\mathbf{w}\|$ 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

$$R_B = \log_2\left(1 + \mathrm{SNR}_B\right), \quad R_E = \log_2\left(1 + \mathrm{SNR}_E\right)$$

and the secrecy rate at Bob is

$$R_{B,sec} = \max\left(R_B - R_E, 0\right). \tag{23}$$

In the presence of Eve with channel $\mathbf{h}_E$, the beamformer $\mathbf{w}$ may be picked to maximize $R_{B,sec}$. By [18, 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

$$\left(\mathbf{I}_{N_r} + \mathbf{h}_B^*\mathbf{h}_B^\top/\sigma_B^2, \mathbf{I}_{N_r} + \mathbf{h}_E^*\mathbf{h}_E^\top/\sigma_E^2\right). \tag{24}$$

Under high SNR, the above solution approaches the solution to the optimization problem [18, 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

$$\mathbf{w}_* = \frac{\left(\mathbf{I}_{N_r} - \mathbf{h}_E^*\mathbf{h}_E^\top/\|\mathbf{h}_E\|^2\right)\mathbf{h}_B^*}{\|\left(\mathbf{I}_{N_r} - \mathbf{h}_E^*\mathbf{h}_E^\top/\|\mathbf{h}_E\|^2\right)\mathbf{h}_B^*\|}. \tag{25}$$

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 (25).

V. Simulation Example

We consider Rayleigh flat-fading channels with path losses $d_B = d_E = d_{BE} = 1$, noise powers $\sigma_v^2 = \sigma_E^2$, INR=5dB, and the training power budget P_B at Bob is such that $P_B/\sigma_v^2 =$ 10dB, and training power budget P_E at Eve is such that P_E/σ_v^2 varies from -30dB through 20dB. Bob and Eve have single antennas while Alice has $N_r = 4$ or 40 antennas. The training sequence was a periodic binary Hadamard sequence with period of 8, and of length $T = 32$ or 80. All results were averaged over 5000 Monte Carlo runs. Fig. 1 shows our detection probability P_d results under spoofing relay 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 (augmented with the generalized eigenvector of (24) with largest eigenvalue, or null placement along Eve, if Eve's presence is detected) as discussed in Sec. IV, are shown in Fig. 2, with the corresponding channel estimation MSE (mean-square error) $\|\widehat{\mathbf{h}}_E - \sqrt{P_B P_E}\mathrm{g}_{BE}\mathbf{h}_E\|^2/N_r$ and $\|\widehat{\mathbf{h}}_B - \mathbf{h}_B\|^2/N_r$ shown in Figs. 3 and 4, respectively, for Eve's and Bob's channels. If Eve's presence is not detected, we use (22). If Eve is detected, after joint channel estimation, we use the generalized eigenvector of (24) with largest eigenvalue, or suboptimal (25). In our simulations, we did not see any discernible difference

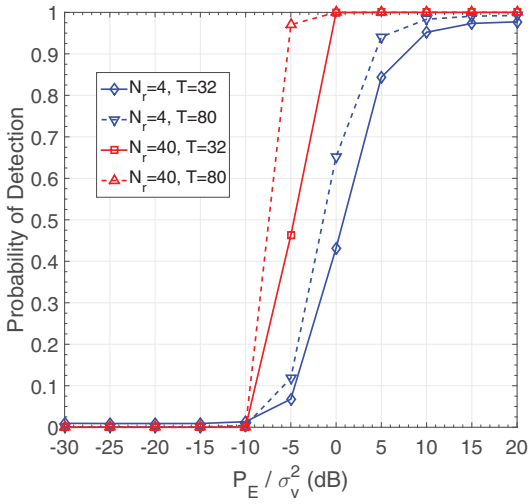

Fig. 1: Probability of spoofing relay attack detection as a function of Eve's power P_E relative to noise power σ_v^2 when Bob's power is fixed at $P_B/\sigma_v^2 = 10$dB, $\sigma_E^2 = \sigma_v^2$, INR=5dB.

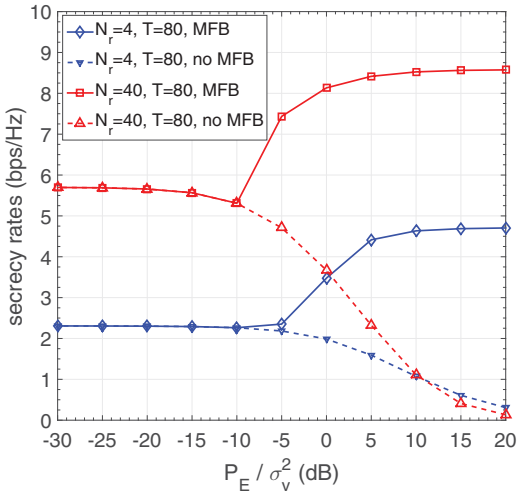

Fig. 2: Secrecy rate (bps/Hz) at Bob using the beamformers discussed in Sec. IV as a function of Eve's power P_E. All parameters as for Fig. 1. The label "MFB" refers to matched filter beamforming of Sec. IV; "no MFB" means ones uses (22) with Eve ignored in channel estimation. $P_A = 1$, $\sigma_B^2 = \sigma_E^2 = 0.1$

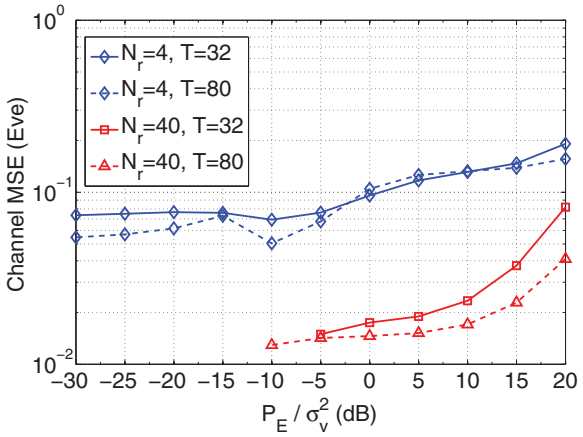

Fig. 3: Channel MSE $\|\widehat{\mathbf{h}}_E - \sqrt{P_B P_E}\mathrm{g}_{BE}\mathbf{h}_E\|^2/N_r$ for Eve's channel as a function of Eve's power P_E. All parameters as for Fig. 1.

between suboptimal (25) and optimal generalized eigenvector solution.

It is seen that secure beamforming yields an improved secrecy rate performance as a function of P_E when the relay spoofing attack "strong." Higher P_E allows better estimation of Eve's channel which, in turn, allows better null placement in Eve's direction as well as improved estimation of Bob's channel. When P_E is insignificant, Alice does not know Eve's channel and its beamformer operates as if it is not aware of Eve's existence.

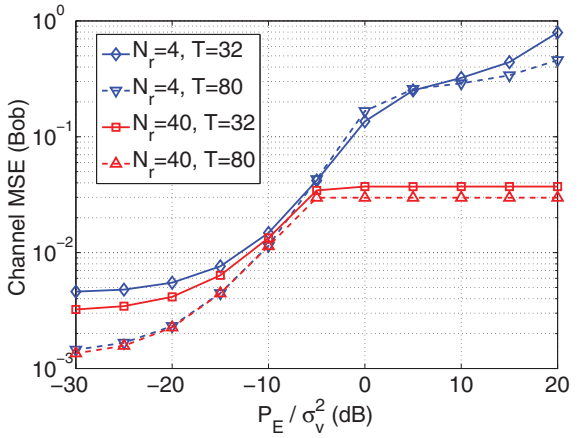

Fig. 4: Channel MSE $\|\widehat{\mathbf{h}}_B - \mathbf{h}_B\|^2/N_r$ for Bob's channel as a function of Eve's power P_E. All parameters as for Fig. 1.

VI. Conclusions

We considered mitigation of spoofing relay attack in a 3-node TDD multiple antenna systems where an adversary operating in a full-duplex mode, amplifies and forwards the training signal of the legitimate receiver. A novel approach to detection of spoofing relay attack was recently presented in [7] where attack mitigation was not addressed. In this paper we augmented the approach of [7] with joint channel estimation and secure beamforming to mitigate the effects of spoofing relay attack. The proposed approach was illustrated by numerical examples.

References

[1] Y. Zeng and R. Zhang, "Active eavesdropping via spoofing relay attack," in *Proc. IEEE Intern. Conf. Acoustics, Speech, Signal Proc.*, pp. 2159-2163, Shanghai, China, March 2016.

[2] 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.

[3] 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.

[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. Inf. Forensics Security*, vol. 10, no. 5, 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] 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.

[7] J.K. Tugnait, "Detection of active eavesdropping attack by spoofing relay in multiple antenna systems," *IEEE Wireless Communications Letters*, vol. 5, no. 5, pp. 460-463, Oct. 2016.

[8] 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.

[9] 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.

[10] D. Bharadia and S. Katti, "FastForward: Fast and constructive full duplex relays," in *Proc. ACM SIGCOMM'14*, Chicago, IL, Aug. 2014, pp. 1-12.

[11] V. Aggarwal, M. Duarte, A. Sabharwal and N.K. Shankaranarayanan, "Full- or half-duplex? A capacity analysis with bounded radio resources," in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sept. 2012, pp. 207-211.

[12] D. Bharadia, E. McMilin and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM'13*, Hong Kong, China, Aug. 2013, pp. 1-12.

[13] M. Duarte, A. Sabharwal, V. Aggarwal, R. Jana, K.K. Ramakrishnan, C.W. Rice and N.K. Shankaranarayanan, "Design and characterization of a full-duplex multiantenna system for WiFi networks," *IEEE Trans. Veh. Tech.*, vol. 63, no. 3, pp. 1160-1177, March 2014.

[14] 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 Proc.*, vol. 58, no. 1, pp. 452-457, Jan. 2010.

[15] 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.

[16] 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.

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

[18] 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.