Pilot Contamination for Active Eavesdropping

Xiangyun Zhou, *Member, IEEE*, Behrouz Maham, *Member, IEEE*, and Are Hjørungnes

***Abstract*—Existing studies on physical layer security often assume the availability of perfect channel state information (CSI) and overlook the importance of channel training needed for obtaining the CSI. In this letter, we discuss how an active eavesdropper can attack the training phase in wireless communication to improve its eavesdropping performance. We derive a new security attack from the pilot contamination phenomenon, which targets at systems using reverse training to obtain the CSI at the transmitter for precoder design. This attack changes the precoder used by the legitimate transmitter in a controlled manner to strengthen the signal reception at the eavesdropper during data transmission. Furthermore, we discuss an efficient use of the transmission energy of an advanced full-duplex eavesdropper to simultaneously achieve a satisfactory eavesdropping performance whilst degrading the detection performance of the legitimate receiver.**

***Index Terms*—Physical layer security, active eavesdropper, channel estimation, pilot contamination.**

I. Introduction

Recently, a significant effort has been made on physical layer security to prevent message eavesdropping by a malicious user. Many studies have taken an information-theoretic approach to compute the achievable rate with perfect secrecy [1]. However, the channel knowledge assumptions and coding complexity needed for achieving perfect secrecy may not always be possible. Departing from the information-theoretic framework, the studies on physical layer security enhancements have also been carried out from a signal processing perspective oriented towards more practical designs. For example, the precoding design of multi-antenna transmission was considered in [2–4] to weaken the signal reception at the eavesdropper or lower the probability of interception.

While various secure transmission schemes are under rapid development, increasingly powerful adversaries also bring in new security attacks. One important example is an active eavesdropper, which acts as either (both) a jammer or (and) a classical eavesdropper in a half-duplex (full-duplex) mode. The decision between jamming and eavesdropping for a half-duplex eavesdropper was studied in [5, 6]. A quasi full-duplex case was considered in [7] where a multi-antenna eavesdropper partitioned its antenna array into eavesdropping and jamming sub-arrays. In this work, we look for new designs of an active eavesdropper from a practical viewpoint.

Manuscirpt received July 7, 2011, revised October 17, 2011, accepted December 21, 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. B. S. Rajan.

X. Zhou is with the Research School of Engineering, The Australian National University, ACT 0200, Australia (Email: xiangyun.zhou@anu.edu.au). B. Maham is with the School of Electrical and Computer Engineering, College of Engineering, University of Tehran (Email: b.maham@ece.ut.ac.ir). A. Hjørungnes (deceased) was with UNIK - University Graduate Center, University of Oslo, Norway. This work was supported by the Australian Research Council's Discovery Projects funding scheme (project no. DP110102548) and the Research Council of Norway through the project 197565/V30.

One major assumption in the literature of physical layer security is the perfect knowledge of the legitimate user's channel state information (CSI). While a few exceptions can be found in [8–10] which incorporated channel uncertainty in the secure transmission design, they did not consider the *training phase* needed for obtaining the (imperfect) CSI. In this letter, we show that the inclusion of the training phase in practical communication systems creates an exciting opportunity for the eavesdropper to develop smart attacks. Specifically, we derive a new security attack based on the *pilot contamination* phenomenon. Pilot contamination was first discussed in [11] in multi-cell systems (without security considerations), where simultaneous uplink training with correlated pilot signals in different cells causes undesirable correlation between the precoding vectors designed at the base stations in those cells. In this work, we show that this undesirable phenomenon can indeed be utilized by an active eavesdropper to improve its eavesdropping performance.

The pilot contamination attack targets at systems in which the transmitter designs its precoder based on the estimates of the legitimate link's CSI and the estimation is done by having the receiver send pilot signals to facilitate the channel estimation at the transmitter, *i.e.*, reverse training. The reverse training scheme requires channel reciprocity which holds in time-division duplex (TDD) systems [11, 12]. During the reverse training phase, the active eavesdropper also sends the same pilot signals to fool the transmitter about the correct channel to be estimated. As a result, the transmitter incorrectly designs the precoder which will benefit the signal reception at the eavesdropper during data transmission. Compared with the active eavesdropper designs in [5–7] where the transmitted signal from the eavesdropper is random jamming noise with the purpose of degrading the signal reception at the legitimate receiver, the pilot contamination attack transmits deterministic signals with the purpose of improving the signal reception at the eavesdropper.

Notation: Boldface letters denote vectors. $[\cdot]^*$ and $[\cdot]^T$ denote complex conjugate and transpose, respectively. $\|\cdot\|$ denotes the Euclidean norm. $\mathbb{E}\{\cdot\}$ is the expectation operator.

II. System Model

We consider message transmissions from a legitimate transmitter, Alice, to an intended receiver, Bob, in the presence of an eavesdropper, Eve. We assume that channel reciprocity holds. Alice is equipped with N_A antennas where $N_A > 1$, while both Bob and Eve have a single antenna (for transmission or reception), *i.e.*, $N_B = N_E = 1$. The wireless channels between the three communicating terminals experience large-scale path loss as well as small-scale fading. The channel parameters are shown in Fig. 1. For instance, the channel

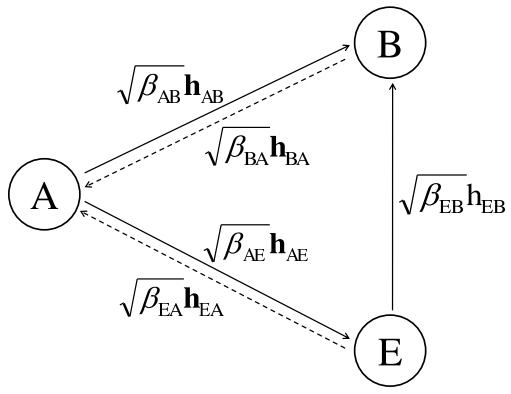

Fig. 1. The parameters of the wireless communication channels between Alice (A), Bob (B), and Eve (E). Alice is equipped with multiple antennas, while both Bob and Eve have a single antenna for transmission or reception.

from Alice to Bob is modeled as $\sqrt{\beta_{AB}}\boldsymbol{h}_{AB}$, where β_{AB} denotes the path loss attenuation and $\boldsymbol{h}_{AB}$ is the fading gain. The channel from Bob to Alice is denoted as $\sqrt{\beta_{BA}}\boldsymbol{h}_{BA}$, where $\boldsymbol{h}_{BA} = \boldsymbol{h}_{AB}^T$ due to channel reciprocity and β_{BA} is not necessarily equal to β_{AB}. Similarly, we denote the channels from Alice to Eve and from Eve to Alice as $\sqrt{\beta_{AE}}\boldsymbol{h}_{AE}$ and $\sqrt{\beta_{EA}}\boldsymbol{h}_{EA}$, respectively, and the channel from Eve to Bob as $\sqrt{\beta_{EB}}h_{EB}$, where h_{EB} is a scalar. Note that $\boldsymbol{h}_{EA} = \boldsymbol{h}_{AE}^T$ due to channel reciprocity. The channel gains $\boldsymbol{h}_{AB}$ and $\boldsymbol{h}_{AE}$ are $1 \times N_A$ row vectors, while $\boldsymbol{h}_{BA}$ and $\boldsymbol{h}_{EA}$ are $N_A \times 1$ column vectors. We model the entries in all channel gains as independent and identically distributed (i.i.d.) zero-mean complex Gaussian random variables with unit variance. We also assume that the path loss attenuations are constant and known to all terminals. Nevertheless, the channel fading gains are unknown to all terminals at the start of the communication.

A. Secure Transmission versus Classical Eavesdropping

We consider block-wise transmissions in which the channel fading gains are assumed to be constant during one transmission block of L symbols and change to some independent values in the next block. For a message transmission from Alice, the received signal at Bob, ignoring possible jamming noise from Eve, is given by

$$y_B = \sqrt{\mathcal{P}_A\beta_{AB}}\boldsymbol{h}_{AB}\boldsymbol{w}x_d + n_B, \quad (1)$$

where x_d is the normalized message symbol with unit variance, $\mathcal{P}_A$ denotes the power of the message symbol, $\boldsymbol{w}$ is the $N_A \times 1$ beamforming vector, and n_B is the zero-mean complex Gaussian receiver noise at Bob with variance σ_B^2. Similarly, the received signal at Eve is given by

$$y_E = \sqrt{\mathcal{P}_A\beta_{AE}}\boldsymbol{h}_{AE}\boldsymbol{w}x_d + n_E, \quad (2)$$

where n_E is the zero-mean complex Gaussian receiver noise at Eve with variance σ_E^2.

From the legitimate user's viewpoint, the goal is to provide reliable communication between Alice and Bob, at the same time preventing message eavesdropping by Eve. From (2), we see that the effective channel fading gain for Eve is given by $\boldsymbol{h}_{AE}\boldsymbol{w}$, which is unknown to Eve. However, Eve can rely on blind detection techniques if $\boldsymbol{h}_{AE}\boldsymbol{w}$ is fixed over a sufficiently long period of time. This is true for the conventional beamforming transmission where a fixed $\boldsymbol{w}$ is used and hence, $\boldsymbol{h}_{AE}\boldsymbol{w}$ is fixed over the entire transmission block. To overcome this problem, the authors in [4] proposed a randomized beamforming design. This design requires the knowledge of $\boldsymbol{h}_{AB}$ to be obtained at Alice but completely unknown to Eve. This can be realized using reverse training, *i.e.*, having Bob send pilot signals to allow the channel estimation at Alice. Denote the estimate of $\boldsymbol{h}_{AB}$ as $\hat{\boldsymbol{h}}_{AB}$. Alice randomly generates $\boldsymbol{w}$ for *each* data symbol transmission with only one constraint given by $\hat{\boldsymbol{h}}_{AB}\boldsymbol{w} = \|\hat{\boldsymbol{h}}_{AB}\|$. The received signal at Bob can then be rewritten as

$$y_B = \sqrt{\mathcal{P}_A\beta_{AB}}\|\hat{\boldsymbol{h}}_{AB}\|x_d + \sqrt{\mathcal{P}_A\beta_{AB}}\tilde{\boldsymbol{h}}_{AB}\boldsymbol{w}x_d + n_B, \quad (3)$$

where $\tilde{\boldsymbol{h}}_{AB} = \boldsymbol{h}_{AB} - \hat{\boldsymbol{h}}_{AB}$ denotes the channel estimation error. Note that the second term in (3) is generally non-Gaussian and is uncorrelated with the first term in (3) if the linear minimum mean square error (LMMSE) criterion is used for channel estimation. The detection of x_d is possible since the coefficient in the first term of (3) takes a constant positive value over the current transmission block, *i.e.*, $\sqrt{\mathcal{P}_A\beta_{AB}}\|\hat{\boldsymbol{h}}_{AB}\|$, even if $\hat{\boldsymbol{h}}_{AB}$ is unknown to Bob. On the other hand, the effective channel fading gain for Eve, $\boldsymbol{h}_{AE}\boldsymbol{w}$, is random for each symbol transmission. As the results shown in [4], Eve cannot do any better than a guessing-based exhaustive search for data detection and her bit error rate (BER) stays around 0.5.

With the randomized beamforming design in [4], it seems hopeless for Eve to intercept the message anymore. However, our discussion has overlooked the importance of the reverse training phase. In the remainder of this letter, we show how an active eavesdropper can increase its chance of message eavesdropping by attacking the reverse training phase in a controlled manner.

III. The Pilot Contamination Attack

In this section, we describe the pilot contamination attack, which is available when the reverse training sequence used by Alice and Bob is also known by Eve. Since the training sequence is fixed and repeatedly used over time, it can be easily obtained by Eve. This creates an opportunity for an active eavesdropper to make a controlled impact on the channel estimation at Alice. Specifically, Eve transmits the pilots at the same time as Bob transmits during the reverse training phase. This makes Alice's estimate of her outgoing channel to Bob also align with her outgoing channel to Eve. The impact of the pilot contamination attack is twofold: it reduces the accuracy of Alice's estimate of her outgoing channel to Bob; and more importantly it helps the data detection at Eve by infecting the beamforming design at Alice. Note that an important assumption made here is the synchronization of transmissions from Bob and Eve. In order to synchronize with Bob, Eve needs to estimate the propagation delays between all the terminals using their location information and obtain any timing information by utilizing the signal exchange between

Alice and Bob during the transmitter-receiver synchronization. The details on when and how accurate synchronization is achievable are beyond the scope of this work.

For block-wise transmissions, each block of L symbols consists of a reverse training phase and a data transmission phase. We assume that only one pilot symbol is transmitted, followed by $L-1$ data symbol transmissions. The extension to multiple pilot symbols is straightforward. In what follows, we discuss the training and data transmission in detail. We consider that Eve operates in a full-duplex mode, so that she can also transmit jamming signal to Bob whilst listening to the data transmission from Alice. For simplicity, we assume no self-interference between the transmit and receive antenna at Eve.[1] As discussed later, the half-duplex mode is a special case of the full-duplex mode.

Reverse Training Phase: During the reverse training phase, both Bob and Eve transmit the pilot and the received signal at Alice is given by

$$\boldsymbol{y}_A = \sqrt{\mathcal{P}_B \beta_{BA}}\boldsymbol{h}_{BA} x_p + \sqrt{\mathcal{P}_{Ep}\beta_{EA}}\boldsymbol{h}_{EA} x_p + \boldsymbol{n}_A, \quad (4)$$

where x_p is the normalized pilot symbol with unit variance, $\boldsymbol{n}_A$ is the receiver noise vector at Alice having zero-mean complex Gaussian entries with variance σ_A^2. In addition, $\mathcal{P}_B$ denotes the training power at Bob and $\mathcal{P}_{Ep}$ denotes the pilot contamination power at Eve. Assuming Alice knows Bob's training power and has accurately obtained the variance of the received signal $\boldsymbol{y}_A$, she applies the LMMSE method to estimate $\boldsymbol{h}_{AB}$, given by [13]

$$\begin{aligned}\hat{\boldsymbol{h}}_{AB} &= \hat{\boldsymbol{h}}_{BA}^T \\ &= \sqrt{\mathcal{P}_B\beta_{BA}}x_p^*(\mathcal{P}_B\beta_{BA} + \mathcal{P}_{Ep}\beta_{EA} + \sigma_A^2)^{-1}\boldsymbol{y}_A^T, \quad (5)\end{aligned}$$

which is also directly related to the LMMSE estimate of $\boldsymbol{h}_{AE}$ as

$$\hat{\boldsymbol{h}}_{AE} = \sqrt{\frac{\mathcal{P}_{Ep}\beta_{EA}}{\mathcal{P}_B\beta_{BA}}}\hat{\boldsymbol{h}}_{AB}. \quad (6)$$

Beamforming Design: Treating $\hat{\boldsymbol{h}}_{AB}$ as the true channel gain, Alice designs the beamforming vector $\boldsymbol{w}$ for data transmission. For both the conventional beamforming and the randomized beamforming described in Section II-A, we have $\hat{\boldsymbol{h}}_{AB}\boldsymbol{w} = \|\hat{\boldsymbol{h}}_{AB}\|$. One major difference between the two beamforming designs is the long-term average power of $\boldsymbol{w}$ defined as $\sigma_w^2 = \mathbb{E}\{\|\boldsymbol{w}\|^2\}$: $\sigma_w^2 = 1$ for the conventional beamforming and $\sigma_w^2 > 1$ for the randomized beamforming [4].

Data Transmission Phase: During the data transmission phase, Alice transmits $L-1$ data symbols while both Bob and Eve perform detection. In addition, Eve also transmits jamming signals to degrade Bob's detection performance. For simplicity, we consider binary phase shift keying (BPSK) modulation, hence $x_d = \pm 1$. For each symbol transmission, the received signal at Bob is given by

$$\begin{aligned}y_B &= \sqrt{\mathcal{P}_A\beta_{AB}}\boldsymbol{h}_{AB}\boldsymbol{w}x_d + \sqrt{\mathcal{P}_{Ed}\beta_{EB}}h_{EB}v + n_B, \\ &= \sqrt{\mathcal{P}_A\beta_{AB}}\|\hat{\boldsymbol{h}}_{AB}\|x_d + \sqrt{\mathcal{P}_A\beta_{AB}}\tilde{\boldsymbol{h}}_{AB}\boldsymbol{w}x_d \\ &\quad + \sqrt{\mathcal{P}_{Ed}\beta_{EB}}h_{EB}v + n_B, \quad (7)\end{aligned}$$

where v denotes the jamming noise symbol with unit variance and $\mathcal{P}_{Ed}$ denotes the jamming power. We assume that the jamming noise has the same distribution as the receiver noise. As mentioned earlier, the second term in (7) is non-Gaussian and uncorrelated with the first term.

Although $\|\hat{\boldsymbol{h}}_{AB}\|$ is unknown to Bob, the detection of the BPSK modulated symbol x_d can be easily done by observing the sign of the real part of y_B, *i.e.*, $\Re\{y_B\}$. Hence, the average error performance is closely related to the average post-processing SNR given by

$$\text{SNR}_B = \frac{2\mathcal{P}_A\beta_{AB}\mathbb{E}\{\|\hat{\boldsymbol{h}}_{AB}\|^2\}}{\mathcal{P}_A\beta_{AB}\mathbb{E}\{\|\tilde{\boldsymbol{h}}_{AB}\boldsymbol{w}\|^2\} + \mathcal{P}_{Ed}\beta_{EB} + \sigma_B^2}. \quad (8)$$

Using some basic properties of the LMMSE estimator and the fact that $\boldsymbol{h}_{AB}$ has Gaussian entries with unit variance, the expectations $\mathbb{E}\{\|\hat{\boldsymbol{h}}_{AB}\|^2\}$ and $\mathbb{E}\{\|\tilde{\boldsymbol{h}}_{AB}\boldsymbol{w}\|^2\}$ can be easily computed (derivations omitted for brevity), and SNR_B can then be further expressed as in (11) at the top of the next page.

At the same time, the received signal at Eve is given by (2) and can be rewritten as

$$\begin{aligned}y_E &= \sqrt{\mathcal{P}_A\beta_{AE}}\hat{\boldsymbol{h}}_{AE}\boldsymbol{w}x_d + \sqrt{\mathcal{P}_A\beta_{AE}}\tilde{\boldsymbol{h}}_{AE}\boldsymbol{w}x_d + n_E, \\ &= \sqrt{\mathcal{P}_A\beta_{AE}}\sqrt{\frac{\mathcal{P}_{Ep}\beta_{EA}}{\mathcal{P}_B\beta_{BA}}}\|\hat{\boldsymbol{h}}_{AB}\|x_d \\ &\quad + \sqrt{\mathcal{P}_A\beta_{AE}}\tilde{\boldsymbol{h}}_{AE}\boldsymbol{w}x_d + n_E, \quad (9)\end{aligned}$$

where we have defined $\tilde{\boldsymbol{h}}_{AE} = \boldsymbol{h}_{AE} - \hat{\boldsymbol{h}}_{AE}$ and used (6) to express $\hat{\boldsymbol{h}}_{AE}$ in terms of $\hat{\boldsymbol{h}}_{AB}$. We see that the coefficient of x_d in the first term of (9) takes a constant positive value over the entire transmission block, even if the randomized beamforming scheme is used by Alice. In other words, pilot contamination has made randomized beamforming ineffective. Similar to Bob, the detection at Eve is done by observing the sign of $\Re\{y_E\}$. The average post-processing SNR at Eve is given by

$$\text{SNR}_E = \frac{2\mathcal{P}_A\beta_{AE}\frac{\mathcal{P}_{Ep}\beta_{EA}}{\mathcal{P}_B\beta_{BA}}\mathbb{E}\{\|\hat{\boldsymbol{h}}_{AB}\|^2\}}{\mathcal{P}_A\beta_{AE}\mathbb{E}\{\|\tilde{\boldsymbol{h}}_{AE}\boldsymbol{w}\|^2\} + \sigma_E^2}. \quad (10)$$

By evaluating the expectations $\mathbb{E}\{\|\hat{\boldsymbol{h}}_{AB}\|^2\}$ and $\mathbb{E}\{\|\tilde{\boldsymbol{h}}_{AE}\boldsymbol{w}\|^2\}$, we can further express SNR_E as in (12) at the top of the next page.

From (11) and (12), we expect that Eve can simultaneously eavesdrop the transmitted messages and destroy the legitimate communication link if the pilot contamination power $\mathcal{P}_{Ep}$ is sufficiently high.

A. Optimizing Energy Allocation

In the following, we further discuss an efficient use of the transmission energy of the full-duplex eavesdropper. From the

[1] As we will describe, Eve transmits pilot signals during the reverse training phase. This allows her to measure the wireless channel gain between the transmit and receive antenna. Hence, the self-interference in the data transmission phase is known by Eve in principle. Any unknown residual self-interference due to other practical imperfections is beyond the scope of this work.

$$\text{SNR}_B = \frac{2\mathcal{P}_A\mathcal{P}_B\beta_{AB}\beta_{BA}N_A}{\mathcal{P}_A\beta_{AB}\sigma_w^2(\mathcal{P}_{Ep}\beta_{EA}+\sigma_A^2)+(\mathcal{P}_{Ed}\beta_{EB}+\sigma_B^2)(\mathcal{P}_B\beta_{BA}+\mathcal{P}_{Ep}\beta_{EA}+\sigma_A^2)}. \quad (11)$$

$$\text{SNR}_E = \frac{2\mathcal{P}_A\mathcal{P}_{Ep}\beta_{AE}\beta_{EA}N_A}{\mathcal{P}_A\beta_{AE}\sigma_w^2(\mathcal{P}_B\beta_{BA}+\sigma_A^2)+\sigma_E^2(\mathcal{P}_B\beta_{BA}+\mathcal{P}_{Ep}\beta_{EA}+\sigma_A^2)}. \quad (12)$$

viewpoint of the active eavesdropper design, it is desirable to optimally allocate the available energy budget in attacking the legitimate user's communication, so that the eavesdropper can enjoy a satisfactory detection performance while the legitimate receiver's detection is severely degraded. We assume that Eve has a total energy budget for each transmission block, given by $\mathcal{E}_E$, which is allocated among pilot contamination (during the reverse training phase) and jamming (during the data transmission phase). In other words, we have $\mathcal{P}_{Ep}+\mathcal{P}_{Ed}(L-1)=\mathcal{E}_E$. Note that this energy constraint can also be interpreted as an average power constraint given by $\mathcal{E}_E/L$. Denote the ratio of total energy allocated to pilot contamination as ϕ, we have the following relationships:

$$\mathcal{P}_{Ep}=\phi\mathcal{E}_E, \qquad \mathcal{P}_{Ed}=\frac{(1-\phi)\mathcal{E}_E}{L-1}. \quad (13)$$

We consider the scenario that Eve's primary design objective is to meet a target SNR_E which gives a satisfactory eavesdropping performance. On top of that, Eve also tries to minimize SNR_B to degrade Bob's detection performance. The optimization problem can then be formulated as

$$\arg\min_{\phi} \ \text{SNR}_B, \qquad \text{s.t. } \text{SNR}_E \geq \rho, \quad (14)$$

where ρ denotes the minimum required value of SNR_E.

Note that the constraint of $\text{SNR}_E \geq \rho$ may not be satisfied if ρ is too large. Since $\phi \in [0,1]$, the maximum feasible value of SNR_E is reached by setting $\phi=1$, which should not be smaller than ρ. Hence, solving $\text{SNR}_E=\rho$ with $\phi=1$ gives the maximum feasible value of ρ as

$$\rho_{\max}=\frac{2\mathcal{P}_A\beta_{AE}\beta_{EA}N_A\mathcal{E}_E}{(\mathcal{P}_B\beta_{BA}+\sigma_A^2)(\mathcal{P}_A\beta_{AE}\sigma_w^2+\sigma_E^2)+\beta_{EA}\sigma_E^2\mathcal{E}_E}. \quad (15)$$

Clearly if Eve has a larger energy budget, a higher $\rho_{\max}$ is feasible. Nevertheless, $\rho_{\max}$ is bounded from above by $2\mathcal{P}_A\beta_{AE}N_A/\sigma_E^2$ as $\mathcal{E}_E\to\infty$.

Assuming $\rho \leq \rho_{\max}$, we can find the feasible range of ϕ that satisfies $\text{SNR}_E \geq \rho$ as $\phi \in [\phi_{\min}, 1]$ where

$$\phi_{\min}=\frac{\rho(\mathcal{P}_B\beta_{BA}+\sigma_A^2)(\mathcal{P}_A\beta_{AE}\sigma_w^2+\sigma_E^2)}{(2\mathcal{P}_A\beta_{AE}\beta_{EA}N_A-\rho\beta_{EA}\sigma_E^2)\mathcal{E}_E}. \quad (16)$$

That is to say, any choice of $\phi \in [\phi_{\min}, 1]$ will give Eve the required eavesdropping performance.

Next, Eve chooses the optimal ϕ from $[\phi_{\min}, 1]$ to minimize SNR_B by solving $\arg\max_\phi \text{SNR}_B^{-1}$. Substituting (13) into (11), it can be shown that SNR_B^{-1} is concave in ϕ. Hence, the optimal energy allocation strategy is obtained by letting the first derivative of SNR_B^{-1} w.r.t. ϕ be zero and the solution is given by

$$\phi^*=\begin{cases} 1, & \text{if } \mathcal{E}_E<\kappa, \\ \phi_{\min}, & \text{if } \frac{\mathcal{E}_E+\kappa}{2\mathcal{E}_E}<\phi_{\min}, \\ \frac{\mathcal{E}_E+\kappa}{2\mathcal{E}_E}, & \text{otherwise}, \end{cases} \quad (17)$$

where

$$\kappa=\frac{\beta_{AB}\beta_{EA}\mathcal{P}_A(L-1)\sigma_w^2+\beta_{EA}(L-1)\sigma_B^2-\beta_{EB}\sigma_A^2-\beta_{BA}\beta_{EB}\mathcal{P}_B}{\beta_{EA}\beta_{EB}}. \quad (18)$$

Note that the solution in (17) requires the knowledge of the system parameters, such as the transmit powers, the path loss attenuations and the receiver noise variances, which are usually assumed to be known by the eavesdropper in the literature of physical layer security. By knowing the locations of Alice and Bob, and the path loss exponent of the wireless channel, the transmit powers from Alice and Bob, as well as the path loss attenuations between the three terminals can be obtained by Eve through measurements. In case Eve does not know the receiver noise variances at Alice and Bob, she may choose to ignore the receiver noise, which gives a reasonably accurate approximation in the moderate to high SNR regime.

Remark: When Eve is located much closer to Alice than to Bob, we have $\beta_{EA}/\beta_{EB} \gg 1$. In this scenario, one may expect that Eve should choose $\phi=1$, *i.e.*, allocating all the energy to pilot contamination, since the received pilot contamination signal at Alice would be much stronger compared to the received jamming signal at Bob. From the optimal solution in (17), we know that $\phi^*=1$ requires $\mathcal{E}_E \leq \kappa$. From (18), we have $\kappa \approx (L-1)(\beta_{AB}\mathcal{P}_A\sigma_w^2+\sigma_B^2)/\beta_{EB}$ which is independent of the ratio of β_{EA}/β_{EB}. Therefore, as long as Eve's energy budget is above (the finite value of) κ, it is never optimal to concentrate all energy to pilot contamination even if $\beta_{EA}/\beta_{EB}\to\infty$. A similar result can be found for the opposite case where Eve is located much closer to Bob than to Alice. Hence, we conclude that it is always wise for Eve to transmit in both phases when she has a good energy budget at hand.

B. Half-Duplex Eavesdropper

In what follows, we briefly discuss the case of a half-duplex eavesdropper, which is indeed a special scenario of the full-duplex case.

Pure Pilot Contamination: In this case, Eve performs the pilot contamination attack during the reverse training phase and acts as a receiver during the data transmission phase. This is the special case of $\mathcal{P}_{Ed}=0$ or $\phi=1$ in previous subsections. To achieve a target minimum value of SNR_E given by ρ, the minimum required pilot contamination power is found as

$$\mathcal{P}_{Ep,\min}=\frac{\rho(\mathcal{P}_B\beta_{BA}+\sigma_A^2)(\mathcal{P}_A\beta_{AE}\sigma_w^2+\sigma_E^2)}{2\mathcal{P}_A\beta_{AE}\beta_{EA}N_A-\rho\beta_{EA}\sigma_E^2}. \quad (19)$$

Pure Jamming: When Eve is not able to achieve a satisfactory data detection performance, she can choose to act

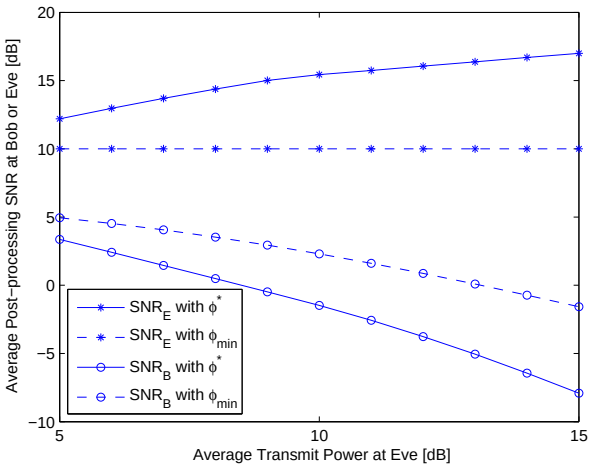

Fig. 2. The average post-processing SNR at Bob or Eve versus the average transmit power at Eve. The required minimum SNR_E is set to 10 dB. The solid lines show SNR_B and SNR_E achieved with the optimal energy allocation ϕ^* given in (17). The dashed lines show SNR_B and SNR_E achieved with $\phi_{\min}$ given in (16). The other system parameters are: $N_A = 4$, $L = 10$, $\mathcal{P}_A = \mathcal{P}_B = 10$ dB, $\sigma_A^2 = \sigma_B^2 = \sigma_E^2 = \sigma_w^2 = 1$, $\beta_{AB} = \beta_{BA} = \beta_{AE} = \beta_{EA} = \beta_{EB} = 1$.

as a pure jammer and aim to minimize SNR_B by optimally allocating her energy among the reverse training phase and the data transmission phase. The knowledge of the pilots is not required and random noise can be used in this case. The optimal value of ϕ is given by

$$\phi^* = \begin{cases} 1, & \text{if } \mathcal{E}_E < \kappa, \\ 0, & \text{if } \mathcal{E}_E < -\kappa, \\ \frac{\mathcal{E}_E + \kappa}{2\mathcal{E}_E}, & \text{otherwise}, \end{cases} \tag{20}$$

which is obtained by letting $\phi_{\min} = 0$ in (17) and κ is given in (18).

IV. Numerical Results

Now, we present numerical results to illustrate the benefits obtained by Eve from the pilot contamination attack. Fig. 2 shows the average post-processing SNRs at Bob and Eve, *i.e.*, SNR_B and SNR_E, during data transmission. The full-duplex mode is considered in which Eve uses different power levels for pilot contamination and jamming. The primary goal of Eve is to meet a minimum SNR_E of 10 dB. Results are shown for Eve's average power budget $\mathcal{E}_E/L$ ranging from 5 dB to 15 dB. We see that Eve is able to simultaneously achieve the required SNR for herself and make Bob suffer from a relatively low SNR. The values of SNR_B and SNR_E strongly depend on the energy allocation parameter ϕ. We include the SNR results for the case of minimum pilot contamination energy allocation, *i.e.*, $\phi_{\min}$ in (16), and the case of optimal energy allocation, *i.e.*, ϕ^* in (17). It is clear from Fig. 2 that the optimal energy allocation not only reduces SNR_B but also achieves a better SNR_E compared to the case of using minimum energy for pilot contamination.

V. Attack Detection and Countermeasures

In this work, we showed the detrimental effect of the pilot contamination attack on the secrecy performance. It is therefore important for the legitimate user to detect such an attack and design countermeasures. The detection of the pilot contamination attack may be achieved by transmitting a sufficiently long pilot sequence in the reverse training phase and analyzing the variance of the received signal at Alice after normalizing it by the pilot sequence. If the variance is close to that of the receiver noise, it indicates that the pilot contamination attack may have been used by Eve. In order to make this attack ineffective, blind channel estimation can be used by Alice based on the data transmission from Bob, assuming two-way communications.

References

[1] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conf. on Inform. Sciences and Syst. (CISS)*, Baltimore, MD, Mar. 2007, pp. 905–910.

[2] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. on Acoustic, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[3] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Processing*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[4] X. Li, M. Chen, and E. P. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," in *Proc. IEEE SPAWC*, New York, NY, Jun. 2005, pp. 811–815.

[5] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast fading channels: A block-Markov Wyner secrecy encoding scheme," submitted to *IEEE Trans. Inf. Theory*. Available at http://arxiv.org/abs/1002.1313.

[6] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," submitted to *IEEE Trans. Inf. Theory*. Available at http://arxiv.org/abs/1011.5274.

[7] ——, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Asilomar Conf. on Signals, Syst., and Computers*, Pacific Grove, CA, Nov. 2011.

[8] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Tech.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[10] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Processing*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[11] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.

[12] T. L. Marzetta, "How much training is required for multiuser MIMO?" in *Proc. Asilomar Conference on Signals, Systems and Computers (ACSSC)*, Pacific Grove, CA, Oct. 2006, pp. 359–363.

[13] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ: Prentice Hall, 1993.