DETECTION OF PILOT SPOOFING ATTACK IN MULTI-ANTENNA SYSTEMS VIA ENERGY-RATIO COMPARISON

Qi Xiong[†]*, Ying-Chang Liang*[‡]*, and Kwok Hung Li*[†] *and Yi Gong*[*]

[†]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
[‡]Institute for Infocomm Research, A*STAR, Singapore
[*]Department of Electrical and Electronic Engineering, South University of Science and Technology of China, China

ABSTRACT

We study a spoofing attack happened in the physical layer of a multiple-antenna system, where an adversary tries to spoof the transmitter by sending the identical pilot (training) signal as that of a legitimate receiver in the uplink channel estimation phase. This attack, named as pilot spoofing attack, could lead to a secrecy information leakage to the adversary and information rate decrease at the legitimate receiver. Due to the serious results caused by the pilot spoofing attack, we propose an energy-ratio detector (ERD) to protect the legitimate components. The ERD makes the decision by exploiting the asymmetry of the received signal strength (RSS) between the transmitter and the legitimate receiver when the system is under the pilot spoofing attack. Numerical results are presented to illustrate the effectiveness of our proposed detector.

***Index Terms*—** Pilot spoofing attack, physical layer security, active eavesdropping, energy-ratio detection

1. INTRODUCTION

Security is a fundamental concern in the design of a wireless network, especially when security-sensitive activities such as the financial trade are operated through the wireless medium. But the openness of the wireless medium allows the possibility of passive eavesdropping and active jamming by the adversaries. Conventional cryptographic method is one essential method to provide the security but facing rising challenges such as the increasing computation capability of the adversaries and the increasing complexity of the key management etc. In recent years, the physical layer security has drawn much attention, which intends to maximize the secrecy rate defined as the information rate difference between the legitimate channel and illegitimate channel [1]. With the multiple-antenna technology, a positive secrecy rate is generally available even when the eavesdropper's channel is stronger than the legitimate channel [2–4]. Except from the passive eavesdropping, the adversary could also choose the active jamming to jeopardize the transmission among the legitimate users [5].

The spoofing attack is an intelligent active attack which usually exists in the upper layers such as the network layer. For instance, an adversary can fake a legitimate node's identity and attack the management/control messages in a Wi-Fi network [6], in which the adversary could further filch more information from the users in the network. However, the spoofing attack could also happen in the physical layer. Consider a time-division duplex (TDD) communication system, a training phase is needed for the channel estimation by having the receiver transmit the assigned pilot signal to the transmitter via uplink channel. Due to the limited source of the pilot signals, these signals are generally repeatedly used and publicly known. Therefore, it creates the possibility for the adversary to spoof the transmitter in the channel estimation by broadcasting the identical pilot signal as the that of the legitimate receiver. While later in the downlink data transmission phase, the transmitter (equipped with multiple antennas) designs the beamforming vector, e.g., maximum-ratio transmission (MRT), based on the channel estimation which actually combines the legitimate channel and illegitimate channel. The pilot spoofing attack then may result in a information rate increase at the adversary and a information rate decrease at the legitimate receiver, which are unwanted to the communication system especially from the security perspective.

The pilot spoofing attack was initially observed in [7] where the authors concluded the problem from the pilot contamination phenomenon and named it as the pilot contamination attack. To our best knowledge, only a few works mentioned the detection of the pilot spoofing attack [8,9]. The main idea of the methods in [8, 9] is to introduce the randomness to the process of choosing the fundamentally redesigned pilot signals, so the adversary may not gain the pilot signal information. In this work, we propose an energy-ratio based detector that examines the asymmetry of the received signal's power levels at the transmitter and the legitimate receiver, which requires no change to the design of the pilot signals and a minor change to the channel estimation process. The detection process mainly contains two steps: 1) in the uplink phase, the transmitter estimates the channel based on the received pilot signals transmitted by the legitimate receiver, and computes the average received signal power level (denoted as Q_1); 2) in the downlink phase, the transmitter modulates Q_1

as data and broadcasts it in the downlink channel by MRT. The legitimate receiver then demodulates Q_1 and calculates the average received signal power level (denoted as Q_2). By comparing the energy ratio (Q_2/Q_1) with a given threshold γ, a detection result could be generated.

2. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a TDD communication system which consists of three components: one transmitter Alice equipped with M ($M \geq 2$) antennas, one single-antenna legitimate receiver Bob and one single-antenna eavesdropper Eve. The uplink and downlink channels are assumed to be reciprocal. We denote the channel between Alice and Bob as $\mathbf{h}_B = \sqrt{\rho_B}\tilde{\mathbf{h}}_B$ and the channel between Alice and Eve as $\mathbf{h}_E = \sqrt{\rho_E}\tilde{\mathbf{h}}_E$, respectively. Both $\mathbf{h}_B$ and $\mathbf{h}_E$ are assumed to be stationary in a given time slot and independent among different time slots. $\tilde{\mathbf{h}}_B \in \mathbb{C}^{M\times 1}$ and $\tilde{\mathbf{h}}_E \in \mathbb{C}^{M\times 1}$ are the small-scale fading coefficient vectors (e.g., multi-path effects), where each entry of $\tilde{\mathbf{h}}_B$ and $\tilde{\mathbf{h}}_E$ is independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian (CSCG) random variable with zero mean and unit variance. ρ_B and ρ_E represent the large-scale fading coefficients (e.g., path-loss). Next, we will succinctly introduce the process of pilot spoofing attack and the impact it may cause to Alice and Bob.

During the uplink training phase, Bob transmits the pilot signal (denoted as $x_p(n)$) to Alice, and the intelligent adversary also broadcasts the same pilot signal to spoof Alice. Therefore, the received signal at Alice is represented as

$$\mathbf{y}(n) = (\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)x_p(n) + \mathbf{u}(n), \tag{1}$$

where $n = 1, \cdots, N_1$ and N_1 is the sample number of pilot signal at Alice. $\mathbf{u}_n \in \mathbb{C}^{M\times 1}$ denotes the white noise vector at Alice and each element in $\mathbf{u}(n)$ is i.i.d. CSCG random variable with zero mean and variance σ^2, i.e., $\mathbf{u}(n) \sim \mathcal{CN}(0, \sigma^2\mathbf{I})$. $\mathcal{P}_B$ and $\mathcal{P}_E$ represent the power levels of sending the pilot signal at Bob and Eve, respectively.

Therefore, the channel estimation (denoted as $\hat{\mathbf{h}}_B$) by using least square (LS) method is given by

$$\hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E + \tilde{\epsilon}, \tag{2}$$

where $\tilde{\epsilon}$ is the estimation error. Then the design of beamforming vector $\mathbf{w}$ according to MRT becomes $\mathbf{w} = \hat{\mathbf{h}}_B/\|\hat{\mathbf{h}}_B\|$ and the received signals at Bob and Eve during downlink data transmission phase are

$$y_b(n) = \sqrt{\mathcal{P}_A}\mathbf{h}_B^H\mathbf{w}x_d(n) + v_b(n), \tag{3}$$

$$y_e(n) = \sqrt{\mathcal{P}_A}\mathbf{h}_E^H\mathbf{w}x_d(n) + v_e(n), \tag{4}$$

where $n = 1, \ldots, N_2$ and N_2 is the sample number of received signal at Bob/Eve. $\mathcal{P}_A$ is the power budget at Alice, where we let $\mathcal{P}_A = \mathcal{P}_B$ for simplicity. $v_b(n)$ and $v_e(n)$ are the white Gaussian noises at Bob and Eve, respectively, i.e., $v_b(n) \sim \mathcal{CN}(0, \sigma^2)$ and $v_e(n) \sim \mathcal{CN}(0, \sigma^2)$. The average signal-to-noise-ratios (SNRs) of $y_b(n)$ and $y_e(n)$ are

$$\text{SNR}_B = \frac{\mathcal{P}_A}{\sigma^2}|\mathbf{h}_B^H\mathbf{w}|^2, \tag{5}$$

$$\text{SNR}_E = \frac{\mathcal{P}_A}{\sigma^2}|\mathbf{h}_E^H\mathbf{w}|^2, \tag{6}$$

respectively.

According to the MRT property, the largest SNR_B is achieved when $\mathbf{w}$ is in the same direction of $\mathbf{h}_B$, e.g., $\mathbf{w} = \mathbf{h}_B/\|\mathbf{h}_B\|$. Given that $\mathbf{h}_B$ and $\mathbf{h}_E$ are independent, the channel estimate $\hat{\mathbf{h}}_B$ generally deviates from $\mathbf{h}_B$ when Alice and Bob are under the pilot spoofing attack. Especially if $\mathcal{P}_E$ is sufficiently large, $\mathbf{h}_E$ becomes the dominating component of $\hat{\mathbf{h}}_B$ and the SNR_E could even surpass the SNR_B. It then indicates that by conducting the pilot spoofing attack, the eavesdropper could gain a larger information rate and also diminish the data reception at the legitimate receiver, which is a great damage to the legal communication system.

3. ENERGY-RATIO DETECTOR

In this section, we propose the energy-ratio detector for helping the transmitter and legitimate receiver to detect the pilot spoofing attack. We define two hypothesises: H_0, denoting that there is no pilot spoofing attack; and H_1, denoting that the pilot spoofing attack happens. The process of ERD mainly divides into two phases: the uplink phase and the downlink phase.

3.1. The Uplink Phase

During the uplink phase, Alice estimates the channels based on the received pilot signals (denoted as $\mathbf{y}(n)$) via LS method:

$$H_0 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \tilde{\epsilon}, \tag{7}$$

$$H_1 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E + \tilde{\epsilon}. \tag{8}$$

Applying the maximum-ratio combining (MRC) to the received signals, we obtain

$$H_0\text{: } y_a(n) = \frac{\hat{\mathbf{h}}_B^H}{\|\hat{\mathbf{h}}_B\|}[\sqrt{\mathcal{P}_B}\mathbf{h}_B x_p(n) + \mathbf{u}(n)], \tag{9}$$

$$H_1\text{: } y_a(n) = \frac{\hat{\mathbf{h}}_B^H}{\|\hat{\mathbf{h}}_B\|}[(\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)x_p(n) + \mathbf{u}(n)]. \tag{10}$$

With $y_a(n)$, we are able to calculate the average power Q_1 of received signals, which is given by

$$Q_1 = \frac{1}{N_1}\sum_{n=1}^{N_1}|y_a(n)|^2. \tag{11}$$

When N_1 is sufficiently large, according to central limit theorem (CLT) [10], Q_1 can be viewed as a Gaussian random

variable, i.e., $Q_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$, where

$$H_0 : \mu_1 = \left| \frac{\hat{\mathbf{h}}_B^H \mathbf{h}_B}{\|\hat{\mathbf{h}}_B\|} \right|^2 \mathcal{P}_B + \sigma^2, \quad (12)$$

$$H_1 : \mu_1 = \left| \frac{\hat{\mathbf{h}}_B^H (\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)}{\|\hat{\mathbf{h}}_B\|} \right|^2 + \sigma^2, \quad (13)$$

and $\sigma_1^2 = \mu_1^2/N_1$ for both H_0 and H_1.

3.2. The Downlink Phase

In the downlink phase, Alice first modulates the value of Q_1 as the data signal ($x_d(n)$) and then transmits it to Bob by using MRT. Some redundant data may be need to reach the required sequence length N_2. We assume Bob could successfully demodulate the signal and obtain the value of Q_1. Therefore, the received signal $y_b(n)$ at Bob becomes

$$y_b(n) = \frac{\mathbf{h}_B^H \hat{\mathbf{h}}_B}{\|\hat{\mathbf{h}}_B\|} \sqrt{\mathcal{P}_A} x_q(n) + v_b(n), \quad (14)$$

and the average received signal power Q_2 is given by

$$Q_2 = \frac{1}{N_2} \sum_{n=1}^{N_2} |y_b(n)|^2. \quad (15)$$

According to CLT, Q_2 could be approximated as a Gaussian random variable as well, i.e., $Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2)$, in which

$$\mu_2 = \left| \frac{\mathbf{h}_B^H \hat{\mathbf{h}}_B}{\|\hat{\mathbf{h}}_B\|} \right|^2 \mathcal{P}_A + \sigma^2, \quad (16)$$

$$\sigma_2^2 = \frac{1}{N_2} \mu_2^2. \quad (17)$$

where for H_0 and H_1, μ_2 is different for the different $\hat{\mathbf{h}}_B$. With the information of Q_1 and Q_2, we design the test statistic as the ratio of Q_1 and Q_2, i.e., $T = Q_2/Q_1$. Next we derive the probability density function (PDF) of T under both H_0 and H_1.

Given the PDF of the ratio of two independent Gaussian random variables [11], we could obtain the PDF of T under H_0 first, which is

$$f_0(T) = \frac{(N_2 T + N_1)\sqrt{N_1 N_2}}{\sqrt{2\pi}(N_2 T^2 + N_1)^{\frac{3}{2}}} e^{\frac{1}{2}\left[\frac{(N_2 T + N_1)^2}{N_2 T^2 + N_1} - N_1 - N_2\right]} \left[2\Phi\left(\frac{N_2 T + N_1}{\sqrt{N_2 T^2 + N_1}}\right) - 1\right] + \frac{\sqrt{N_1 N_2}}{\pi(N_2 T^2 + N_1)} e^{-\frac{1}{2}(N_1 + N_2)}, \quad (18)$$

where $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}u^2} du$. As we can observe, $f_0(T)$ is not related to μ_1 or μ_2, which means it is also not related to the CSIs, i.e., $\mathbf{h}_B$ or $\mathbf{h}_E$. This is a great advantage as it indicates that given a required probability of false alarm (denoted as P_{fa}), the detection threshold γ can be derived for all possible channel conditions.

Furthermore, the PDF of T under H_1 is given by

$$f_1(T) = \frac{\sqrt{N_1 N_2} b(T) c(T)}{\sqrt{2\pi}\mu_1 \mu_2 a^3(T)} \left[2\Phi\left(\frac{b(T)}{a(T)}\right) - 1\right] + \frac{\sqrt{N_1 N_2}}{a^2(T)\pi\mu_1\mu_2} e^{-\frac{1}{2}(N_1 + N_2)}, \quad (19)$$

where

$$a(T) = \sqrt{\frac{N_2 T^2}{\mu_2^2} + \frac{N_1}{\mu_1^2}}, \quad (20)$$

$$b(T) = \frac{N_2 T}{\mu_2} + \frac{N_1}{\mu_1}, \quad (21)$$

$$c(T) = e^{\frac{1}{2}\left[\frac{b^2(T)}{a^2(T)} - N_1 - N_2\right]}. \quad (22)$$

Note that $f_1(T)$ is dependent on the channel realizations of $\mathbf{h}_B$ and $\mathbf{h}_E$.

Thus, the detection threshold γ could be derived from a given probability of false alarm P_{fa}:

$$P_{fa} = Pr(T < \gamma | H_0; \mathbf{h}_B, \mathbf{h}_E) = Pr(T < \gamma | H_0) = \int_{-\infty}^{\gamma} f_0(x) dx. \quad (23)$$

The probability of detection then could be expressed as

$$P_d = Pr(T < \gamma | H_1; \mathbf{h}_B, \mathbf{h}_E) = \int_{-\infty}^{\gamma} f_1(x) dx. \quad (24)$$

Since the CSI of $\mathbf{h}_B$ and $\mathbf{h}_E$ are unavailable, the ergodic probability of detection $\bar{P}_d$ is achieved as

$$\bar{P}_d = E_{\mathbf{h}_B, \mathbf{h}_E}\left[Pr(T < \gamma | H_1)\right] = E_{\mathbf{h}_B, \mathbf{h}_E}\left[\int_{-\infty}^{\gamma} f_1(x)\right]. \quad (25)$$

The expressions of $f_0(T)$ and $f_1(T)$ are complicated so the closed-form of γ and $\bar{P}_d$ are generally intractable. However, with the mathematical software, e.g., MatLab, (25) can be solved efficiently by numerical methods.

Next, we intends to obtain simplified results by considering a special case that Alice is equipped with a large number of antennas, i.e., $M \to \infty$. We then have $Q_1 = \|\hat{\mathbf{h}}_B\|^2$, and T has a Gaussian distribution with certain mean and variance. Due to the space limit, the derived threshold γ_0 and the detection probability P_d are directly given below.

$$\gamma_0 = \left[\frac{\Phi^{-1}(P_{fa})}{\sqrt{N_2}} + 1\right] \mu_{T0}, \quad (26)$$

$$P_d = \Phi\left(\frac{\sqrt{N_2}(\gamma_0 - \mu_{T1})}{\mu_{T1}}\right), \quad (27)$$

where $\mu_{T0} = \frac{\mathcal{P}_B M \beta_B + \sigma^2}{\mathcal{P}_B M \beta_B + \frac{M\sigma^2}{N_1}}$ and $\mu_{T1} = \frac{\mathcal{P}_B M \beta_B + \sigma^2}{\mathcal{P}_B M \beta_B + \mathcal{P}_E M \beta_E + \frac{M\sigma^2}{N_1}}$ are the mean values of T under H_0 and H_1, respectively. We can see by utilizing larger power to conduct the pilot spoofing attack, i.e., $\mathcal{P}_E$ is large, Eve becomes even more vulnerable to our ERD.

4. NUMERICAL RESULTS

Numerical results are presented to show ERD's performance under different sample numbers and different power levels of Eve. The simulation results are obtained by 100000 times of transmission experiments. $\mathcal{P}_A = \mathcal{P}_B = 10$ dB and the antenna's number M is 4. We normalize the noise power as 1, i.e., $\sigma^2 = 1$. Without loss of generality, the large scale fading coefficients are set to be one, e.g., $\beta_B = \beta_E = 1$.

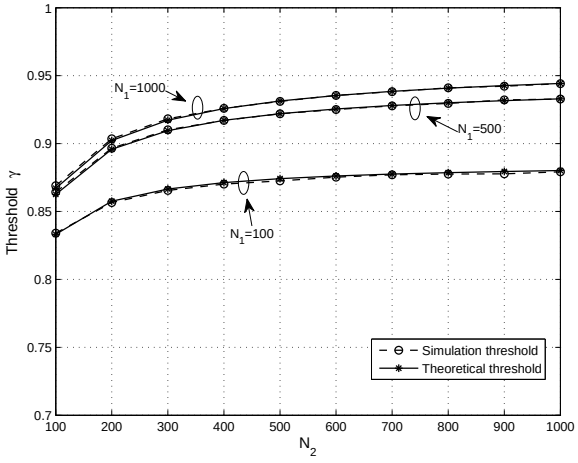

Fig. 1. Thresholds obtained by theoretical analysis and simulation results. $P_{fa} = 0.1, M = 4$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

The thresholds obtained by using simulations and our theoretical analysis at (23) are shown in Fig. 1 when given the required P_{fa} equals 0.1. We can observe that the simulation thresholds are overlapping with these derived from (23) for large sample number situation, e.g., $N_1 = N_2 = 1000$, and small sample number situation, e.g., $N_1 = N_2 = 100$. The latter situation is close to a practical system set-up where the sample numbers are usually of several hundreds. Moreover, it can be seen that with even larger N_1 and N_2, the variance of the test statistic T becomes smaller, which leads the threshold approaching one. Therefore, the overlapping results can validate our theoretical analysis.

In Fig. 2, the detection performance of our proposed ERD is shown under different requirements of P_{fa} ($P_{fa} = 0.1, 0.01$) and different power budgets at Eve ($\mathcal{P}_E$ from -10 dB to 15 dB). For the theoretical results, the detection probability is obtained based on (25) by utilizing the theoretical threshold derived from (23). Two specific cases of sample number are considered: $N_1 = N_2 = 1000$ and $N_1 = N_2 = 100$.

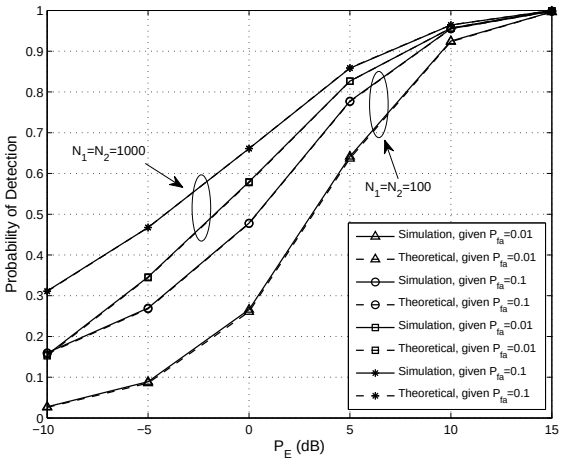

Fig. 2. The probability of detection (P_d) versus different given probability of false alarm (P_{fa}) under $N_1 = N_2 = 1000$ and $N_1 = N_2 = 100$. $M = 4$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

It can be observed that with a larger $\mathcal{P}_E$, a higher required P_{fa} or larger sample numbers, the eavesdropper faces a higher possibility to be detected. In order to make the ergodic secrecy rate to be zero, the eavesdropper usually needs to spend equal power as that of Bob. In that case, e.g., $\mathcal{P}_E = 10$ dB, the ERD's detection probability approaches one for both large N_1, N_2 case and small N_1, N_2 case. Furthermore, our simulations also compute the actual probability of false alarm P_{fa} based on the theoretical threshold derived from (23). When required P_{fa} equals 0.1 and 0.01, the actual P_{fa} become 0.0999, 0.0096 under $N_1 = N_2 = 1000$, and 0.0988, 0.0087 under $N_1 = N_2 = 100$, respectively. It shows the actual P_{fa} levels are all smaller than the required values, which satisfies the demand of the system.

5. CONCLUSION

In this paper, we have studied an active spoofing problem in the physical layer of a wireless multiple-antenna system, i.e., pilot spoofing attack. We proposed the ERD to detect such attack. The ERD is working based on exploiting the asymmetry of received signals' power levels at Alice and Eve if there exists the pilot spoofing attack. The closed form of the statistic's PDFs under H_0 and H_1 have been obtained. Our detector did not require to change the design of current pilot signal and drastically redesign the process of current channel estimation process. Future study may include the achievable secrecy rate optimization after the detection.

6. REFERENCES

[1] A. Wyner, "The wire-tap channel," Bell Syst. Tech. J., Vol.54, No.8, pp. 1355-1387, Oct. 1975.

[2] Q. Xiong, Y. Gong, Y. C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357-360, Aug. 2014.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas. Part II: The MIMOME wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 56, no. 11, pp. 5515 5532, Nov. 2010.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 57, no. 8, pp. 4961 4972, Aug. 2011.

[5] A. Mukherjee and A. L. Swindlehurst, "Jamming Games in the MIMO Wiretap Channel With an Active Eavesdropper," *IEEE Trans. Signal Process*, vol. 61, no. 1, pp. 82 - 91, Jan. 2013.

[6] L. Xiao, A. Reznik, W. Trappe, C. X. Ye, Y. Shah, L. J. Greenstein and N. B. Mandayam, "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. GLOBECOM*, 2010.

[7] X. Y. Zhou, B. Maham and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903-907, Mar. 2012.

[8] D. Kapetanovi, G. Zheng, K. K. Wong and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. PIMRC*, Sept. 2013.

[9] J. J. Yang, S. L. Xie, X. Y. Zhou, R. Yu, Y. Zhang, "A semiblind two-way training method for discriminatory channel estimation in MIMO systems," available at http://arxiv.org/abs/1405.4626v1 .

[10] Y.-C. Liang, Y. H. Zeng, E. Peh, A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[11] D. V. Hinkley, "On the ratio of two correlated normal random variables". Biometrika 56 (3): 635 - 639, Dec. 1969.